Universität Siegen

Fakultät III: Wirtschaftswissenschaften, Wirtschaftsinformatik
und Wirtschaftsrecht

Bachelorthesis

Thema: Empirische Untersuchung der Eignung betrieblicher Authentifikationsverfahren und möglicher neuer Techniken in ausgewählten Organisationen

---

Vorgelegt von Marius Müller
Matrikelnummer 904025
Studiengang Wirtschaftsinformatik

Abgabedatum: 11. März 2015

Erstprüfer: Dr. Lars Fischer
Zweitprüfer: Dr. Markus Rohde

Inhaltsverzeichnis

Plagiatserklärung

Ich versichere, dass ich die vorliegende Arbeit selbständig angefertigt und keine anderen als die angegebenen Hilfsmittel benutzt habe.
Alle Stellen, die dem Wortlaut oder dem Sinn nach anderen Werken entnommen sind, habe ich in jedem einzelnen Fall unter genauer Angabe der Quelle (einschließlich des World Wide Web sowie anderer elektronischer Datensammlungen) deutlich als Entlehnung kenntlich gemacht. Dies gilt auch für angefügte Zeichnungen, bildliche Darstellungen, Skizzen und dergleichen.
Ich nehme zur Kenntnis, dass die nachgewiesene Unterlassung der Herkunftsangabe als versuchte Täuschung bzw. als Plagiat gewertet und mit Maßnahmen bis hin zur Aberkennung des akademischen Grades geahndet wird.

. . . .
(Ort, Datum) Unterschrift des Verfassers

Abkürzungsverzeichnis

IT	Informationstechnik
VPN	Virtual Private Network
OTP	One Time Password
CR	Challenge Response
PIN	Persönliche Identifikationsnummer
TAN	Transaktionsnummer
CA	Certification Authority
WOT	Web Of Trust
SSO	Single Sign-On
BSI	Bundesamt für Sicherheit in der Informationstechnik
ISMS	Informationssicherheitsmanagementsystem
ISO	International Organization for Standardization
IEC	International Electrotechnical Commission
SSL	Secure Socket Layer
DEW	Deutsche Edelstahlwerke
G.I.B	Gesellschaft für Information und Bildung

Tabellenverzeichnis

1 Einleitung

1.1 Motivation

In der heutigen Zeit, die häufig auch als digitales Zeitalter (vgl. Fritzsche 2014) bezeichnet wird, gewinnt die Sicherheit der versendeten und gespeicherten Daten und Informationen immer mehr an Bedeutung. Besonders für Unternehmen und Organisationen, die zunehmend global agieren und sich über geografische Grenzen hinweg zwecks Kooperation, Handel oder Wissensaustausch vernetzen, ist die Sicherheit der verwendeten Informationstechnik und der verwalteten und übertragenen Daten und Informationen wichtiger denn je. So gelingt es Teilnehmern der Weltwirtschaft, sich innerhalb dieses weltumspannenden Netzes dank ihres einzigartigen Wissens und Know-Hows zu positionieren und dadurch einen entscheidenen Wettbewerbsvorteil zu erhalten. Dies legt einen besonderen Schutz dieser Erfolgsfaktoren nahe und erfordert deshalb die Anwendung gezielter Schutzmechanismen und sicherheitstechnischer Verfahren und Technologien.
Besonders deutlich und publik im unternehmerischen Kontext wird diese Notwendigkeit durch diverse Ereignisse, die gravierende Folgen für die betroffenen Firmen und Organisationen nach sich ziehen. So gewinnt beispielsweise das Thema der Industriespionage mehr und mehr an öffentlicher Brisanz, kann sie doch zur Insolvenz betroffener Unternehmen führen. Einem High-Tech-Unternehmen aus Erlangen gelingt es im Jahre 2013, einen unternehmerischen Schaden rechtzeitig zu verhindern. Es wird das Opfer eines Spionageangriffs. Chinesischen Kontrahenten gelingt es durch den unerlaubten Zugriff auf die Systeme der deutschen Firma wichtige Patente zu entwenden und das betreffende Produkt noch vor Veröffentlichung zu kopieren. Trotz der Abwehr dieser bedrohlichen Ereignisse warnt der Inhaber des mittelständischen Unternehmens und klärt auf:

> „Dabei öffnen nicht nur schlecht geschützte IT-Systeme, sondern auch die Mitarbeiter den Spionen die Tür. Vor allem mittelständische Unternehmen ignorieren diese Risiken jedoch noch zu häufig“ (Lüke 2013).

Bei der Auseinandersetzung mit geeigneten Maßnahmen zur erfolgreichen Abwehr beziehungsweise Vermeidung solcher Vorfälle erweist sich daher die Authentifikation der beteiligten Personen und Maschinen innerhalb der Kommunikation und vernetzten Geschäftsprozesse als einer der wichtigsten Aspekte. Erst duch die Identifizierung und Überprüfung

der Akteure und dem daraus resultierenden authentischen Zustand wird die Durchführung weiterer wichtiger Sicherheitsmechanismen zur Herstellung von Vertraulichkeit und Integrität ermöglicht (vgl. Eckert 2013, S. 465). Folglich nehmen Authentifikationsverfahren sowie die zugrunde liegenden Technologien und Regeln eine besondere Stellung im Rahmen der infrastrukturellen und informationstechnischen Absicherung ein und erfordern daher eine gewissenhafte und zielgerichtete Anwendung etablierter Technologien und Modelle.

1.2 Zielsetzung und Vorgehen

Ziel dieser Bachelorarbeit ist es, die zum Einsatz kommenden Authentifizierungsverfahren sowie damit einhergehende Maßnahmen im Rahmen der betrieblichen IT-Sicherheit in Organisationen auf deren Effizienz sowie ihre Eignung hin zu untersuchen. Hierzu soll festgestellt werden, ob die angewendeten Technologien die Erwartungen der Mitarbeiter beziehungsweise der Verantwortlichen innerhalb der Unternehmen und somit ihren Zweck als effizientes Werkzeug zur Absicherung interner IT-Systeme, Daten und Informationen erfüllen. Um diese Forschungserkenntnisse zu erlangen, werden im Rahmen einer qualitativen Untersuchung bestimmte Mitarbeiter einiger ausgewählter Unternehmen und Institutionen befragt. Die dabei entstehenden Aussagen werden mit fachbezogenen Inhalten ausgewählter Literatur abgeglichen und anschließend bewertet.

Während Kapitel 2 sich mit den allgemeinen Grundlagen der Authentifizierung und Authentizität beschäftigt, werden in Kapitel 3 die technologischen Hintergründe erläutert. Hier werden gängige und in der Praxis zum Einsatz kommende Verfahren und Techniken vorgestellt und kategorisiert.

Im Anschluss befasst sich Kapitel 4 mit der Notwendigkeit sicherheitsrelevanter Authentifizierungsmaßnahmen innerhalb von Unternehmen und Betrieben. Um dies zu erläutern werden Gründe im Hinblick auf den unternehmerischen Kontext sowie gesetzliche Regelungen und Standards genannt.

Anschließend werden in Kapitel 5 die sozialwissenschaftlichen Techniken erläutert, auf Basis derer die Befragungen durchgeführt und anschließend ausgewertet und interpretiert werden. Die Ergebnisse und Erkenntnisse der empirirschen Untersuchung werden anschließend gemäß eines ausgewählten Auswertungsverfahrens in Kapitel 6 dargestellt. Darauf folgt eine Schlussbetrachtung sowie ein Ausblick auf zukünftige Entwicklungen und Potentiale.

2 Grundlagen der digitalen Authentifizierung

Dieses Kapitel befasst sich mit den theoretischen Grundlagen dieser Arbeit und führt die notwendigen Begriffe ein, die für die nachfolgenden Kapitel benötigt werden. Zudem erfolgt eine Klassifizierung von Verfahren und Techniken, auf die in Kapitel 3 näher eingegangen wird.

2.1 Das Schutzziel der Authentizität

Die gespeicherten und bewegten Daten heutiger Informationssysteme sind „(…) zu schützende Güter (…)“ (Eckert 2013, S. 7) und bedürfen daher einer dedizierten Absicherung. Zu jenen Daten zählen neben personenbezogenen Daten wie etwa Adressen, Namen, Konto- und Bankdaten und geheim zu haltenden Informationen wie Passwörtern auch zunehmend betriebliche Daten. Unternehmen vernetzen sich mehr und mehr mit Partnern und anderen Organisationen und schaffen somit neben dem betriebsinternen einen globalen Datenpool.
Um diese angestrebte Sicherheit zu erzielen sind Schutzziele definiert worden. Diese Verklausulierungen veranschaulichen den Prozess, der notwendig ist, um eine mehrseitige Sicherheit der beteiligten Systeme und Daten zu erreichen.
Zu den primären Schutzzielen zählen die Datenintegrität, die Vertraulichkeit sowie die Authentizität der beteiligten Akteure. Unter Integrität versteht man die Korrektheit von übertragenen Daten und die Sicherstellung, dass sie nicht unbemerkt verändert worden sind. Die Vertraulichkeit ist dann gegeben, wenn keine unautorisierte Informationsgewinnung möglich ist, das heißt Daten vor unerlaubten Zugriffen geschützt sind (vgl. Eckert 2013, S. 9f).
Besonders die Definition der Informationsvertraulichkeit setzt eine gewisse Identifizierung des zugreifenden Subjekts oder Objekts sowie den zugeordneten Rechten voraus. Um den Zugriff auf die zu schützenden Informationen zu erlauben oder zu verbieten, muss also die Identität des Zugreifenden zweifelsfrei bestimmt werden. Hierbei spricht man von Authentizität:

> „Unter der Authentizität eines Objekts bzw. Subjekts (engl. *authenticity*) verstehen wir die Echtheit und Glaubwürdigkeit des Objekts bzw. Subjekts, die anhand einer eindeutigen Identität und charakteristischen Eigenschaften überprüfbar sind“ (Eckert 2013, S. 8).

Um einen authentischen Zustand zu erreichen und darauf aufbauend weitere Aktionen einzuleiten

bedarf es spezieller Maßnahmen, sogenannter Authentifizierungs- oder Authentifikationsmaßnahmen (vgl. Eckert 2013, S. 8). Hierbei muss anhand von gewissen Eigenschaften, sogenannten *Credentials*, sichergestellt und überprüft werden, dass die vorgegebene Identität auch tatsächlich mit der realen übereinstimmt. Ein klassisches Beispiel ist hier der Einsatz eines geheimen Passwortes, das der Anwender vorlegen muss.

Dieses Bündel an Maßnahmen umfasst bestimmte Grundfunktionen, die potentielle Angriffe im Hinblick auf die Authentizität des Anwenders erschweren oder verhindern sollen. Die Zusammenstellung dieses Bündels orientiert sich stets an den Sicherheitsanforderungen an die zum Einsatz kommenden Verfahren. Hierbei lassen sich verschiedene Abstufungen ausmachen. Zum einen kann eine einfache Identifizierung des Anwenders, von nun an Subjekt genannt, ausreichen, das heißt ein Nachweis der angegebenen Identität ist nicht notwendig[1] (vgl. Eckert 2013, S. 220). Zum anderen lässt sich auch die Authentifizierung der Identität vorgeben, wie es zum Beispiel bei Banktransaktionen notwendig ist. Hierzu müssen im Vorfeld die bereits erwähnten *Credentials* definiert werden, mit Hilfe derer das Subjekt seine Identität nachweisen kann (vgl. Eckert 2013, S. 8). Ein weiteres Kriterium, das bei der Formulierung der Sicherheitsanforderungen berücksichtigt werden muss, ist die Fälschungssicherheit sowie der „(…) Aufwand, der zur unautorisierten Erlangung einer Identität notwendig ist“ (Eckert 2013, S. 224).

Folglich gilt es bei der Auswahl von Sicherheitsmaßnahmen die Gefahrenpotentiale, die relevanten Bedrohungen sowie den notwendigen Grad des Schutzes der betroffenen Ressourcen auszumachen.

2.2 Klassifizierung von Authentifikationsverfahren

Authentifizierungstechniken lassen sich in drei übergeordnete Kategorien unterteilen, die jeweils unterschiedliche Arten von *Credentials* zum Nachweis der Identität nutzen. Jede dieser Verfahrensklassen hat seine individuellen Vor- und Nachteile, die nachfolgend kurz erläutert werden.

1 Dies ist zum Beispiel beim Zugriff auf öffentliche Ressourcen und Informationen der Fall, der keiner weiteren Authentifizierung bedarf.

2.2.1 Wissen

Ein sehr häufig eingesetztes Authentifikationsverfahren basiert auf speziellem Wissen, das das zu authentifizierende Subjekt beziehungsweise Objekt besitzt. Dies geschieht in den meisten Fällen durch die Angabe eines bestimmten Geheimnisses (vgl. Eckert 2013, S. 468), das im Optimalfall nur der betroffene Anwender kennt und diesem dadurch eindeutig zugeordnet werden kann. Daraus lässt sich der Nachteil ableiten, dass die Sicherheit dieser Verfahren mit der Geheimhaltung und der Erinnerung an jenes Wissen einhergeht, was einen bewussten Umgang damit voraussetzt. Von Vorteil ist wiederrum die einfache Implementierung dieser Techniken, da sie rein digital abläuft (vgl. Bernauer 2006).

2.2.2 Besitz

Im Gegensatz zur Authentifikation auf der Basis von Wissen gründet diese Kategorie auf dem Besitz eines spezifischen Gegenstandes, der auch hier dem zu authentifizierenden Anwender eindeutig zugeordnet werden kann. Ein herkömmliches Beispiel sind hier Chipkarten, „(…) die in unterschiedlichen Ausprägungen (…)“ vorkommen (Eckert 2013, S. 541). Folglich gilt es hierbei nicht, sich an ein gewisses Geheimnis zu erinnern, was die Handhabung erleichtert. Andererseits ist die Herstellung jener Gegenstände häufig mit Kosten verbunden, auch der Diebstahl oder das Abhandenkommen sind nicht auszuschließen (vgl. Bernauer 2006).

2.2.3 Biometrie

Die dritte Kategorie der Authentifizierungsverfahren basiert auf dem Nachweis gewisser biometrischer Merkmale. Damit sind „(…) physiologische oder verhaltenstypische Eigenschaften (…)“ (Eckert 2013, S. 495) eines Anwenders gemeint, zum Beispiel sein individueller Fingerabdruck. Diese Eigenschaften sind eindeutig zurechenbar aufgrund ihrer einzigartigen Natur und sind daher nur sehr schwer zu fälschen, was die biometrischen Verfahren mit zu den effektivsten macht (vgl. Tsolkas 2010, S. 148). Von Nachteil hierbei sind jedoch die einhergehenden Kosten sowie der erhöhte Aufwand dieser Techniken, da sie im Vorfeld die Erfassung jener biometrischen Attribute durch spezielle Geräte voraussetzen (vgl. Tsolkas 2010 S. 148, Grieser 2008). Zudem unterliegen diese Messgeräte natürlichen Schwankungen in der Qualität der Messungen, fehlerhafte Ergebnisse sind daher nicht auszuschließen (vgl. Bernauer 2006).

2.2.4 Mehr-Faktor-Authentifikation

In der realen Welt werden häufig Techniken unterschiedlicher Kategorien kombiniert, um von den jeweiligen Vorzügen zu profitieren (vgl. Eckert 2013, S. 467). Während es einem Angreifer genügt, bei einer einfachen wissensbasierten Authentifikation, wie etwa einer Passwortabfrage, jenes Geheimnis zu erraten oder sich anderweitig zu beschaffen, so nimmt die Sicherheit durch die Kombination mit einem biometrischen oder besitzbasierten Verfahren zu. Ist beispielsweise neben dem Passwort ein Fingerabdruck zur erfolgreichen Authentifizierung notwendig, so benötigt der Angreifer bereits zwei unterschiedliche *Credentials.* Gleiches gilt zum Beispiel auch für die Kombination mit einer Chipkarte oder einem ähnlichen Gegenstand. Somit wird ein Fälschen oder Beschaffen der Authentifikationsmerkmale und ein unerlaubter Zugriff erschwert.
Folglich ist diese Mehr-Faktor-Authentifizierung bei der Absicherung sensibler und kritischer Informationen zu bevorzugen (vgl. Witt 2006, S. 167).

3 Technologien und Maßnahmen zur Authentifikation

Es existieren eine Vielzahl an Technologien und Verfahren, um die Authentifikation von Anwendern und Maschinen in digitalen Netzen und Systemen zu realisieren. In diesem Kapitel werden ausgewählte Techniken vorgestellt, die in der Praxis häufig Anwendung finden.
Die Auswahl beschränkt sich hierbei neben grundlegenden auf jene Verfahren, die für die spätere Auswertung der Befragungen, die im Rahmen dieser Arbeit durchgeführt wurden, relevant sind.

3.1 Wissensbasierte Verfahren

Die erste Gruppe von Authentifizierungsmaßnahmen, die hier vorgestellt werden soll, ist die auf Wissen basierende, also auf der Kenntnis eines authentifizierenden Geheimnisses. Die folgenden Technologien haben demnach gemeinsam, dass sie eines oder mehrerer *Credentials* bedürfen, die nur dem Anwender (oder der Maschine) bekannt sein sollten.

3.1.1 Nutzerkennung und Passwort

Das Verfahren unter Verwendung einer Nutzerkennung sowie eines geheimen Schlüssels ist eine sehr weit verbreitete Authentifizierungsmaßnahme und wird unter anderem in Betriebssystemen wie zum Beispiel Windows oder Linux genutzt. Daneben verwenden eine Vielzahl anderer Systeme diese Methode, wie etwa zu installierende Programme oder Anwendungen im Internet, die über einen Browser angesprochen werden. Alle haben gemeinsam, dass sie personenbezogene Daten verwalten, auf die nur dazu autorisierte Benutzer Zugriff haben sollen. Um dies zu gewährleisten vereinbart das System mit dem jeweiligen Nutzer ein Kennwort, womit er seine Identität nachweisen kann (vgl. Eckert 2013, S. 468).
Der technische Ablauf einer solchen kennwortbasierten Authentifikation sieht allgemein wie folgt aus:

1. Das System fragt den Anwender nach seiner Nutzerkennung.

2. Der Nutzer antworter mit eben dieser. Darauf wird er zur Angabe seines Passwortes zwecks Authentifikation aufgefordert.

3. Nun vergleicht das System die Eingabe mit dem zuvor vereinbarten Geheimnis. Bei

erfolgreichem Vergleich ist die Nutzername-Kennwort-Zuordnung korrekt, der Nutzer ist authentifiziert (analog dazu der Fehlerfall) (vgl. Eckert 2013, S. 470).

Die Zuordnung von Passwort zu Nutzer legt eine besondere Verwaltung jener Kennwörter nahe, so dass unerlaubtes Auslesen verhindert wird. Dies ist in erster Linie Aufgabe des Systems. Hierzu bedienen sich Anwendungs- sowie Betriebssysteme häufig kryptographischer Funktionen, die es ermöglichen, Kennwörter statt in klar leserlicher in verschlüsselter Form abzulegen. Dies hat den Vorteil, dass die gespeicherten Geheimnisse selbst bei einem unautorisierten Zugriff unbrauchbar sind. Die besagten Verschlüsselungsverfahren nennt man Hashfunktionen (vgl. Eckert 2013, S. 468). Sie haben die Eigenschaft, dass sie Einwegfunktionen sind. Das heißt, dass der Klartext der Kennwörter nach erstmaliger Verschlüsselung nicht wieder hergestellt werden kann[2].

Neben der Verschlüsselung der Passwörter hängt die Sicherheit dieser gespeicherten Geheimnisse von der „(…) Qualität der Rechtevergabe und Zugriffskontrolle ab“ (Eckert 2013, S. 468f). Das heißt, dass seitens des Systems darauf geachtet werden muss, dass niemand lesenden Zugriff auf diese Datei hat. Dies soll vorallem gängige Angriffe wie das Passwort-Cracking (siehe Kapitel 3.5.1) verhindern.

Während die bisher beschriebenen Maßnahmen rein auf technischer Ebene ablaufen, ist ein weiteres Kriterium für die Sicherheit der Kennwörter von Bedeutung. Dies ist der Umgang des jeweiligen Nutzers mit seinem individuellen Passwort. Dies impliziert ein bewusstes Umgehen mit der geheimen Information, um es Angreifern zu erschweren, über Wege wie Ablesen der Eingabe[3] an das Kennwort zu gelangen (vgl. Eckert 2013, S. 469f).

3.1.2 One-Time-Passwords

One-Time-Passwords, also Einmalpassworte, sind eine besondere Form der wissensbasierten Kennwortauthentifizierung. Hierzu wird bei jedem Authentifikationsvorgang ein neues Passwort generiert, das auch nur für diese Sitzung gültig ist. Nach einmaligem Gebrauch wird es entwertet und ist ab diesem Zeitpunkt nicht mehr zu gebrauchen. Dies hat den Vorteil, dass ein Angreifer, dem ein solches *One-Time-Password* (OTP) in die Hände fällt, damit in der Regel keinen Schaden anrichten kann, da es kurz nach der Erzeugung bereits verwendet wird (vgl. Eckert 2013, S. 473). Des Weiteren findet keine persistente Speicherung der Einmalpasswörter auf den betreffenden

2 Der Grund für diese Eigenart ist mathematischer Natur. Im Zuge des Hash-Vorgangs findet eine Abbildung der jeweiligen Zeichen des Passwortes auf Zeichen eines kryptographischen Zeichenraums statt. Die Erläuterung dieser Funktionen soll nicht Teil der vorliegenden Arbeit sein. Für weitere literarische Recherche siehe Eckert, Claudia (2014): IT-Sicherheit: Konzepte – Verfahren – Protokolle.

3 Für diese und weitere Gefahren siehe Kapitel 3.5.

Systemen statt. Selbst bei einer Korrumption eines Informationssystems, das die OTP-Authentifikation unterstützt, findet ein Schädling folglich keine geheimen *Credentials* vor (vgl. Schmeh 2007, S. 351).

Der Einsatz von Einmalpasswörtern wird in der Praxis häufig mit einer besitzbasierten Authentifikationstechnik kombiniert. Eine sehr oft anzutreffende Vereinigung ist die Zwei-Faktor-Authentifizierung in Form eines Gerätes, genannt *Token*, das *One-Time-Passwörter* generiert.

3.1.3 Challenge-Response-Verfahren

Das sogenannte *Challenge-Response-Verfahren* (CR) ist ein Oberbegriff für viele verschiedene technische Realisierungen, die auf dem Wissen bestimmter geheimer *Credentials* basieren.

Das in den vorangegangenen Kapiteln beschriebene Passwortverfahren, sei es das klassische oder das unter Verwendung von Einmalpasswörtern, ist bereits eine konkrete Ausprägung dieses CR-Verfahrens. Während diese Techniken den Transport des geforderten Geheimnisses über die Kommunikationsleitung voraussetzen, so ist dies nicht immer zwingend notwendig (vgl. Tsolkas 2010, S. 133).

Es existieren diverse *Challenge-Response-Verfahren*, bei deren Ausführung es genügt, die reine Kenntnis eines bestimmten *Credentials* nachzuweisen, ohne dies eingeben und übertragen zu müssen. Um dies zu verwirklichen ist es nötig, im Vorfeld der abzusichernden Kommunikationssitzung ein gemeinsames Geheimnis, häufig Schlüssel oder *Key* genannt, auszuhandeln, das fortan im Besitz der beiden beteiligten Parteien ist. Dieser *Key* wird anschließend zum Verschlüsseln der Übertragungen verwendet[4].

Der folgende Authentifizierungsprozess veranschaulicht die Funktionsweise eines einfachen *Challenge-Response-Verfahrens* (vgl. Tsolkas 2010, S. 135):

1. Der Nutzer fordert eine Anmeldung bei einem Server an.

2. Der Server sendet daraufhin eine *Challenge*, also eine Frage nach dem zuvor geteilten Geheimnis. Dies ist in der Regel eine generierte Zufallszahl, so dass die Wahrscheinlichkeit einer Mehrfachverwendung identischer *Challenge*-Werte minimiert wird (vgl. Eckert 2013, S. 488). Dadurch soll verhindert werden, dass ein Angreifer eine bereits gesendete *Challenge* erneut versendet, um sich als Server auszugeben.

3. Der Anwender verschlüsselt nun die *Challenge* mit dem gemeinsamen Schlüssel und sendet

4 Die Verschlüsselung mittels eines zuvor geteilten kryptographischen Schlüssels wird als symmetrisch bezeichnet. Diesem Vorgehen stehen die asymmetrischen Kryptoverfahren gegenüber. Für weiterführende Literaturrecherche siehe Eckert, Claudia (2014): IT-Sicherheit: Konzepte – Verfahren – Protokolle.

diese Antwort an den Server zurück. Dieser Schritt wird *Response* genannt.

4. Serverseitig wird derweil die gleiche Verschlüsselung durchgeführt. Das Ergebnis wird mit der *Response* verglichen.
5. Stimmen die Ergebnisse überein, so kann davon ausgegangen werden, dass der Nutzer im Besitz des Schlüssels ist. Er ist somit authentifiziert und ihm kann der Zugriff gewährt werden. Der negative Fall läuft analog ab (vgl. Tsolkas 2010, S. 135).

Das hier beschriebene Verfahren hat den großen Vorteil, dass es zu keinem Zeitpunkt notwendig ist, das geteilte Geheimnis, auch *Pre-shared secret* genannt, über eine Leitung zu übertragen. Die Schlüssel verweilen dauerhaft auf den Systemen der beteiligten Kommunikationspartner und sind daher immun gegen unerlaubtes Abhören eines Dritten. Es besteht allerdings dennoch die Gefahr, dass ein Angreifer die übermittelten *Challenge*- bzw. *Response*-Nachrichten mitliest und versucht, daraus den Wert des Schlüssels zu berechnen. Dem kann mit einer Verschlüsselung des Kommunikationskanals mittels eines geeigneten kryptographischen Verfahrens entgegen gewirkt werden (vgl. Tsolkas 2010, S. 134).

3.1.4 Dictionary- und Brute-Force-Attacken

Wie bereits erwähnt ist das Authentifikationsverfahren unter Nutzung einer Identifikationskennung sowie eines Passworts immer noch eine der populärsten und verbreitetsten Techniken. Diese Gegebenheiten führen zu einer Vielzahl von Angriffen auf Nutzerpasswörter und damit versehene Zugangskontrollen. Zwei der am häufigsten auftretenden Vorgehensweisen sind hierbei sogenannte *Dictionary*- und *Brute-Force-Attacken* (vgl. Meyers 2007, S. 72).

Die Wörterbuchattacke (engl. dictionary attack) basiert auf dem Vorhandensein einer Sammlung vieler Zeichenkombinationen, die häufig als Passwörter gewählt werden. Fängt der Angreifer ein durch eine Hash-Funktion verschlüsseltes Passwort eines Anwenders ab, so vergleicht er dieses mit den möglichen Hashwerten in seiner Tabelle. Bei Übereinstimmung beider Werte wird ein Zugriffsversuch unter Verwendung der ausgemachten Zeichenkette unternommen (vgl. Meyers 2007, S. 72). Bei erfolgreichem Login ist der Angreifer authentifiziert, bei einem Misserfolg wird mit der nächsten Übereinstimmung fortgefahren. Die Erfolgschance dieses Verfahrens hängt also von der Größe des genutzten „Wörterbuchs“ ab. Die Existenz und freie Verfügbarkeit vieler Tools zur Ausübung von *Dictionary-Attacken* macht dieses Verfahren besonders zugänglich.

Ein weiteres häufig ausgeübtes Verfahren zur Kompromittierung von Nutzerpasswörtern ist der *Brute-Force-Angriff*. Bei dieser Technik versucht der Angreifer das Kennwort durch Ausprobieren

vieler Zeichen sowie Zeichenketten zu erraten. Er stellt also wiederholt Authentifizierungsanfragen im Namen des betroffenen Anwenders an den Server, jeder Versuch verwendet eine neue Kombination (vgl. Meyers 2007, S. 72). Ziel ist es also hierbei, durch wiederholtes Austesten eine erfolgreiche Anmeldung zu erreichen. Im Gegensatz zur Dictionary-Attacke bedarf dieses Vorgehen einer stetigen Verbindung zum Zielserver oder -system, damit die Anfragen durchgeführt werden können. Er findet also *online* statt, während der Angriff mittels Wörterbuch auch *offline* vorbereitet werden kann.

3.2 Besitzbasierte Verfahren

Die auf dem Besitz eines bestimmten identifizierenden Gegenstandes basierenden Authentifikationsverfahren sind eine weitere weit verbreitete Kategorie. In den nachfolgenden Unterkapiteln werden unterschiedliche Technologien vorgestellt, die sich in der Praxis bewährt haben. Einige davon tauchen häufig in Kombination mit wissensbasierten Verfahren auf, die bereits in Kapitel 3.1 beschrieben wurden. Somit handelt es sich häufig um hybride Verfahren, welche die Vorteile beider Systemarten nutzen.

3.2.1 Hardware-Token im Virtual Private Network

Die Authentifizierung von Nutzern mittels eines sogenannten *Tokens* ist eine weitere in der Praxis weit verbreitete Technologie (vgl. Eckert 2013, S. 479). Als *Token* bezeichnet man ein kleines Gerät, das dem Anwender ausgehändigt wird, der sich fortan bei einem bestimmten Dienst oder System authentifizieren muss. Ähnlich dem Passwortverfahren ist jeder Person exakt ein Gerät zugeordnet, welches aus Sicherheitsgründen niemand anderem zugänglich gemacht werden darf.
Dieser *Token* ist in der Lage, *One-Time-Passwords* in Form eines einmalig nutzbaren Passworts, einer persönlichen Identifikationsnummer (PIN) oder Transaktionsnummer (TAN), also einer Folge von Ziffern, zu generieren. Daraus ergibt sich die Kombination wissensbasierter und besitzbasierter Verfahren zur Authentifikation, da ein Nutzer sowohl im Besitz des Gerätes sein muss als auch über das generierte Wissen verfügen muss (vgl. Tsolkas 2010, S. 141). Dies geschieht in der Regel durch das Ablesen des erzeugten OTPs von einem kleinen Display.
Um diese Form der Authentifizierung zu ermöglichen ist es notwendig, das Gerät mit dem System zu synchronisieren, an dem sich der Nutzer ausweisen soll, etwa durch beidseitige Verwendung

eines identischen *Challenge-Response-Verfahrens* (vgl. Tsolkas 2010, S. 141f). Hierzu verfügen das Gerät sowie das System in der Regel über einen gemeinsamen, symmetrischen Schlüssel sowie eine zeitliche Gleichschaltung, also eine identische Uhrzeit (vgl. Eckert 2013, S. 479). Will sich ein Nutzer mit Hilfe des *Hardware-Token* an dem zuständigen Dienst des Zielsystems authentifizieren, so generiert das Gerät eine zufällige[5] Folge von Zeichen oder Ziffern, die auf eine entsprechende Anfrage hin eingegeben werden muss. Die im Vorfeld geschehene Synchronisation beider Systeme stellt dabei sicher, dass auf beiden Seiten das gleiche OTP generiert wird. Die Erzeugung basiert hierbei auf der synchronen Uhrzeit und dem geteilten Schlüssel (vgl. Eckert 2013, S. 479). Stimmen beide Einmalpassworte überein, so ist der zugreifende Nutzer authentifiziert.
Diese Abstimmung der beteiligten Parteien sowie die Bereitstellung der Hardware stellen im Gegensatz zu wissensbasierten Verfahren einen gewissen ökonomischen, zeitlichen und administrativen Aufwand dar, da eine Vielzahl von Geräten verteilt, verwaltet und gewartet werden muss.

3.2.1.1 Synchrone und asynchrone Hardware-Token

Bei den in der Praxis eingesetzten OTP-Generatoren wird zwischen *synchronen* und *asynchronen Token* unterschieden (vgl. Tsolkas 2010, S. 142).
Das im vorherigen Kapitel beschriebene, zeitbasierte Verfahren wird als synchron bezeichnet. Es bedarf, wie beschrieben, einer absolut gleichlaufenden, inneren Uhr beider Systeme. Somit sind sie in der Lage unabhängig voneinander identische *One-Time-Passwords* zu generieren, die mit Hilfe eines zuvor geteilten Schlüssels ver- und entschlüsselt werden. Bei besonders hohen Sicherheitsanforderungen an das zu schützende System ist es zusätzlich möglich, neben der Nutzerkennung und dem generierten OTP ein individuelles Passwort abzufragen im Sinne des klassischen Nutzerkennung-Passwort-Verfahrens. Neben dieser zeitgesteuerten Authentifikation existiert noch eine ereignisbasierte. Hierbei startet der Nutzer per Anfrage an das System manuell den Anmeldevorgang und erzeugt auf seinem *Hardware-Token* durch Knopfdruck ein neues OTP. Dies geschieht ebenfalls systemseitig, so dass ebenfalls eine synchrone OTP-Erzeugnung stattfindet (vgl. Tsolkas 2010, S. 142).
Im Gegensatz zu der synchronen Variante macht die asynchrone Token-Authentifikation Gebrauch von einem *Challenge-Response-Verfahren* und bedarf keiner gleichlaufenden Uhr. Es findet also eine Interaktion zwischen Authentifizierungsdienst und *Token* statt. Hierzu gibt das System zu

5 Die Erzeugung dieser Information läuft nicht rein zufällig ab. Viel mehr unterliegt sie einem deterministischen Algorithmus, dessen Ergebnisse stets auf einem bestimmten Startwert sowie Zeitwerten basieren.

Beginn des Anmeldevorgangs einen Wert vor, den der Nutzer manuell in sein Gerät eingeben muss. Dieses berechnet daraus nun unter Hinzunahme eines gemeinsamen Schlüssels ein OTP, das dem System anschließend in Verbindung mit der Nutzerkennung genannt werden muss. Stimmt dieses Einmalpasswort mit dem überein, was seitens des Systems berechnet wurde, so ist die Authentifikation erfolgreich (vgl. Tsolkas 2010, S. 143).

3.2.1.2 Das Virtual Private Network

Die vorgestellten Verfahren unter Verwendung von *Hardware-Token* zur synchronen oder asynchronen Passworterzeugung werden häufig innerhalb sogenntar *Virtual Private Networks* angewandt:

> „Unter einem virtuellen privaten Netz verstehen wir eine Netzinfrastruktur, bei der Komponenten eines privaten Netzes über ein öffentliches Netz wie dem Internet miteinander kommunizieren, wobei sie die Illusion besitzen, das Netz zu ihrer alleinigen Verfügung zu haben“ (Eckert 2013, S. 765).

Der Kernpunkt dieser Definition ist der, dass ein virtuelles privates Netz, kurz VPN, bei der Realisierung einer sicheren Kommunikation über einen unsicheren, öffentlichen Kanal eingesetzt wird. Dabei wird zwischen den beiden beteiligten Parteien eine Verbindung aufgebaut, die trotz ihres offen zugänglichen Charakters die Sicherheitsgegebenheiten der jeweiligen privaten Netze fortsetzt und somit „(...) als eine dedizierte private Verbindung (...)“ (Eckert 2013, S. 765) wahrgenommen wird. Es stellt die Authentizität der beteiligten Parteien, die Vertraulichkeit der Daten sowie die Schlüsselerzeugung zwecks kryptographischer Verschlüsselung sicher (vgl. Eckert 2013, S. 765).
Virtuelle private Netze lassen sich in vielen Bereichen einsetzen, um unterschiedlichste Aufgaben zu erfüllen. Eine in der Praxis häufig anzutreffende Ausprägung ist die Vernetzung verteilter Organisationen und Firmen über geographische Grenzen hinaus. So lässt sich mittels bestehender Telekommunikationsinfrastruktur ein gemeinsamenes Netz erzeugen, obwohl die Teilnehmer ihr jeweils eigenes Subnetz besitzen (vgl. Eckert 2013, S. 765f). Dies ermöglicht unter anderem das kooperative Arbeiten an gemeinsamen Projekten, Dateien und Systemen.
Ein weiterer Anwendungsbereich eines VPN ist der entfernte Zugriff auf das interne Netz eines Unternehmens. Dadurch ist es autorisierten Mitarbeitern oder Kunden möglich, von zu Hause aus

oder während eines Außeneinsatzes auf geschützte Inhalte oder Server im Firmennetz zuzugreifen. Um dies zu realisieren bedarf es einer bestimmten VPN-Software, die auf den beteiligten Rechnern und Systemen installiert werden muss. Sie ist zuständig für die notwendige Authentifizierung der zugreifenden Anwender und den Aufbau sowie die Verschlüsselung des Kommunikationskanals (vgl. Eckert 2013, S. 766).

3.2.1.3 Duale Authentifizierung am Beispiel des RSA-SecureID-Token

Mit dem Begriff der dualen Authentifizierung ist eine Zwei-Faktor-Authentifizierung gemeint. Sie basiert, wie bereits beschrieben, auf spezifischem Wissen und dem Besitz eines eindeutig zugeordneten, synchronen oder asynchronen *Tokens*.
Ein sehr weit verbeitetes und bekanntes Verfahren ist hierbei die sogenannte *RSA SecurID*, die in Form eines kleinen USB-Sticks oder einer elektronischen Scheckkarte von der Firma RSA Security vertrieben wird[6]. Ihre einfache und nachvollziehbare Handhabung hat sie zu einer der erfolgreichsten Token-Lösungen gemacht (vgl. Schmeh 2007, S. 353f). Sie findet in der Sicherheitspraxis vieler Unternehmen Einsatz, die besonders hohe Anforderungen an den Zugriff und die Authentizität ihrer Nutzer und Administratoren haben und dies mittels Mehr-Faktor-Authentifikation umsetzen (vgl. Tsolkas 2010, S. 143).
Bei der Authentifizierung mittels der *RSA SecurID* ist es notwendig, sich zur sicheren Anmeldung am Zielsystem oder -server zuerst gegenüber dem RSA-Server auszuweisen. Dieser verwaltet Seriennummern und geteilte, geheime Schlüssel, die sich auf den jeweiligen Geräten befinden. Im Jahr 2011 wird ein Angriff auf die Server bekannt, bei dem es Eindringlingen gelingt, jene Informationen zu stehlen. Dies macht die Berechnung der generierten Einmalpassworte möglich, so dass die Sicherheit der im Umlauf befindlichen *SecurID-Token* nicht länger gewährleistet ist und rund 40 Millionen Exemplare zurückgerufen werden (vgl. Eckert 2013, S. 480). Dieser Vorfall macht die Verwundbarkeit solcher Verfahren sichtbar.

3.2.2 Software-Token

Softwarebasierte Generatoren von Einmalpasswörtern ähneln den hadrwarebasierten in ihrer Funktionalität. Wie der Name bereits vermuten lässt kommt diese Lösung ohne ein Gerät aus, das

6 Für weitere Informationen zu der Firma RSA Security sowie dessen Produkte siehe: http://www.emc.com/domains/rsa/index.htm (Aufruf am 17.01.2015).

der zugreifende Anwender mit sich führen muss. Es ist lediglich nötig, ein Programm auf dem Rechner oder System zu installieren, von dem aus auf die geschützten Ressourcen des Zielservers zugegriffen werden soll[7]. Diese Anwendung übernimmt die auf einem gemeinsamen Schlüssel basierende Erzeugung von OTPs und visualisiert sie auf dem Bildschirm (vgl. Psmail 2010).
Dass keine Hardware mitgeführt werden muss ist jedoch zugleich nachteilig, da die Sicherheit des *Software-Token* von dem betreibenden System und dessen Vertraulichkeit abhängig ist. Verschafft sich ein Angreifer Zugriff auf den Rechner des Nutzers, so ist die Kompromittierung des zugrunde liegenden geheimen Schlüssels nicht auszuschließen. Ein physischer Gegenstand wie etwa die *RSA-SecureID* verhindert dies indem er voraussetzt, dass ein Angreifer den *Hardware-Token* in seinen Besitz bringen muss.

3.2.3 Smartcards

Die Anwendung sogenannter *Smartcards* ähnelt dem in Kapitel 3.2.1 beschriebenen Token-Verfahren und zählt damit ebenso zu den besitzbasierten Authentifikationsverfahren, die in der Praxis Anwendung finden.
Smartcards erscheinen in der Form einer herkömmlichen Chipkarte. Im Gegensatz zu Karten, die legiglich über einen kleinen flüchtigen Speicher verfügen[8], besitzen die behandelten intelligenten Speicherkarten eine „(...) zusätzliche Sicherheitslogik, die meist für eine PIN-Speicherung und -Überprüfung verwendet wird“ (Eckert 2013, S. 542). Darüber hinaus zeichnet die *Smartcard* aus, dass sie über einen eigenen Prozessor sowie Lese- und Arbeitsspeicher und einen programmierbaren Speicher verfügt (vgl. Schmeh 2007, S. 377). Im Gegensatz zu tokenbasierten Verfahren bedarf die Erkennung und Anwendung einer solchen Chipkarte eines Lesegerätes, das mit dem Rechner des Nutzers verbunden werden muss. Zudem sind sie durch ihren meist freiligenden Chip empfindlicher und anfälliger für Defekte (vgl. Grieser 2008).
Smartcards werden aufgrund ihrer kostengünstigen Produktion und einfachen Handhabung als Authentifikationswerkzeug eingesetzt und dienen bespielsweise als universitärer oder betrieblicher Ausweis sowie als Bank- und Kreditkarte. Nachfolgend wird zur Verdeutlichung ein kartenbasiertes Authentfikationsverfahren vereinfacht vorgestellt.
Der erste Schritt dieses Verfahrens besteht aus der Authentifizierung des Anwenders gegenüber der

7 Dies hat unter anderem den Vorteil, dass keine Geräte verloren gehen und wiederbeschafft oder gesperrt werden müssen. Dies in Verbindung mit einer einfachen virtuellen Distribution schafft monetäre und administrative Vorteile. Für weitere Informationen siehe Warden 2014.

8 Zu diesen Ausprägungen zählen zum Beispiel Telefon- oder Krankenversicherungskarten, auf denen geringe Mengen an Daten gespeichert werden. Sie verfügen über keinerlei Authentifizierungslogik.

Smartcard. Hierzu ist in der Regel die Eingabe einer PIN notwendig, die der Person bekannt ist. Das Kartenlesegerät überträgt nun diese geheime Ziffernfolge an den Prozessor der Karte, der sie mit der im Speicher hinterlegten Nummer vergleicht, wobei mehrmalige Fehlversuche zur Sperrung der Karte führen können (vgl. Eckert 2013, S. 548).
In einem zweiten Schritt wird ein *Challenge-Response-Verfahren* zwischen der Smartcard und dem Lesegerät eingeleitet. Hierzu sendet das Gerät eine *Challenge*, woraufhin die Karte eine Antwort unter Verwendung eines zuvor geteilten, gemeinsamen Schlüssels berechnet. Dadurch wird die Authentizität der Karte gegenüber der lesenden Instanz sichergestellt. Anschließend authentifiziert sich die *Smartcard* in einem letzten Schritt gegenüber dem Zielsystem, ebenfalls unter Anwendung eines vereinbarten CR-Verfahrens (vgl. Eckert 2013, S. 549).

3.2.4 Digitale Zertifikate und Signaturen

Als ein digitales Zertifikat bezeichnet man ein strukturiertes Manifest, das neben einer Identität, beispielsweise ein Name einer Person oder einer Firma, weitere charakterisierende Eigenschaften aufweist. Es wird von einer zentralen Stelle, genannt *Certificate Authority*, ausgestellt und einer bestimmten Identität zugeordnet. Dieses Zertifikat erfüllt den Zweck, die in ihm enthaltene Identität und dessen Eigenschaften zu bestätigen und zu beglaubigen.
Es existieren vielerlei Zertifikate unterschiedlichster Ausprägungen, eines der bekanntesten ist hierbei das X.509-Zertifikat. Folgende Informationen können neben anderen in einem digitalen Zertifikat enthalten sein:

- eine Seriennummer, die die zentrale Verwaltung und eindeutige Zuordnung ermöglicht,
- eine Versionsnummer des Zertifikats,
- verschiedene Informationen zur betroffenen Identität wie Name und Adresse,
- der dem zugeteilten Schlüssel zugrunde liegende Algorithmus,
- die Lebensdauer und Gültigkeit des Zertifikats und
- die Signatur der Zertifizierungsstelle (vgl. Tsolkas 2010, S. 144).

Hierbei ist unter anderem die Rede von einem zugeteilten Schlüssel und dessen Algorithmus. Dieser sogenannte öffentliche Schlüssel ermöglicht neben der Verschlüsselung eines Kommunikationskanals die Authentifizierung des betroffenen Zertifikatinhabers (vgl. Grieser 2008).
Bei der Erzeugung dieses Zertifikats durch die CA wird basierend auf mathematischen Berechnungen ein kryptographisches Schlüsselpaar generiert, bestehend aus einem privaten

(*Private Key*) und öffentlichen Schlüssel (*Public Key*). Der private Schlüssel ist geheim zu halten, während der öffentliche Schlüssel publiziert wird (vgl. Schmeh 2007, S. 153). Infolge dessen besitzt nur der Zertifikatsnehmer das zum im Zertifikat genannten Schlüssel passende Gegenstück. Ein besitzbasiertes Authentifizierungsverfahren entsteht[9].

Nun ist es dem Anwender möglich, sich durch den Nachweis, dass er im Besitz des privaten Schlüssels ist, zu authentifizieren. Beispielsweise können Daten, die an den Zertifikatsinhaber gesendet werden, mit dessen Public Key verschlüsselt werden. Da diese Informationen ausschließlich mit dem zugehörigen Private Key entschlüsselt werden können, ist eine vertrauliche Kommunikation sichergestellt (vgl. Schmeh 2007, S. 153). Dies funktioniert auch in entgegengesetzter Richtung. Die zu authentifizierende Person kann die von ihr stammenden Daten oder Anfragen mit ihrem privaten Schlüssel kombinieren, dessen Echtheit später mittels mathematischer Operationen und unter Anwendung des zugehörigen öffentlichen Schlüssels überprüft werden kann[10]. Diesen Vorgang nennt man digitale Signatur.

Die vorgestellte Methode, auch *Public-Key-Verfahren* oder *Public-Key-Infrastructure* (PKI) genannt, setzt neben bestimmten Datenformaten, Protokollen und Richtlinien, wie bereits erwähnt, eine zentrale Verwaltungsstelle voraus, der alle Teilnehmer dieses Netzes zwecks gegenseitiger Signatur und Verschlüsselung vertrauen (vgl. Tsolkas 2010, S. 152f). Schließlich werden die Schlüssel, auf deren Sicherheit und Einmaligkeit die Effektivität der Lösung beruht, von eben dieser Instanz generiert. Aus diesem Grund befindet sich auf einem X.509-Zertifikat neben anderen Informationen die Signatur der ausstellenden Zertifizierungsstelle. Diese kann unter Hinzunahme des ebenfalls auf dem Zertifikat befindlichen öffentlichen Schlüssels der CA überprüft werden, was der Fälschung solcher Zertifikate vorbeugt (vgl. Schmeh 2007, S. 445).

3.2.5 Dezentrale Systeme am Beispiel des „Web Of Trust“

Wie bereits in Kapitel 3.2.4 beschrieben existieren Public-Key-Infrastrukturen, die auf speziellen zentralen Zertifizierungsbehörden basieren. Innerhalb dieser Infrastrukturen ist das Ausstellen und Signieren von Zertifikaten ausschließlich jenen Behörden vorenthalten, was ein gewisses Maß an Vertrauen seitens der Zertifikatnehmer voraussetzt. Folglich basiert die Sicherheit einer zentralen

9 Die beiden kryptographischen Schlüssel sind so konstruiert, dass der private nicht aus dem öffentlichen Schlüssel berechnet werden kann. Dies ist der zugrunde liegenden Mathematik geschuldet und soll im Rahmen dieser Arbeit nicht näher erläutert werden. Für weitere Recherchen siehe Schmeh 2007.

10 Die genannten Operationen setzen voraus, dass mathematische Funktionen existieren, die die genannten Eigenschaften der Ver- und Entschlüsselung aufweisen. Auch hierfür siehe Schmeh 2007.

PKI auf der Vertrauenswürdigkeit weniger Certification Authorities und deren Sorgfalt was die Überprüfung der jeweiligen Identitäten und das Ausstellen der Zertifikate anbelangt. Neben dieser zentralen Lösung existieren einige dezentrale[11] Lösungen, die praktische Anwendung finden und ohne übergeordnete Autoritäten auskommen (vgl. Schmeh 2007, S. 445). Zu diesen Technologien zählt das sogenannte *Web Of Trust* (WOT), also ein Netz basierend auf gegenseitigem Vertrauen.

Die dezentrale Natur dieses Vertrauensnetzwerkes ermöglicht es, dass Zertifikate im Gegensatz zu herkömmlichen PKIs von den Teilnehmern des Netzes selbst ausgestellt werden. Folgender Ablauf skizziert die Vorgänge innerhalb des *Web Of Trust* und verdeutlicht seine Entstehung am Beispiel eines E-Mail-Verkehrs mehrerer Personen (vgl. Schmeh 2007, S. 447):

1. Die beteiligten Personen Anton, Barbara und Christian erstellen jeweils ein persönliches Schlüsselpaar und veröffentlichen ihren *Public Key*.

2. Anton möchte mit Barbara kommunizieren. Hierzu validiert er ihren öffentlichen Schlüssel, beispielsweise durch ein persönliches Treffen. Von nun an vertraut Anton Barbara und ihrem öffentlichen Schlüssel, ein authentifizierter Mail-Austausch ist möglich.

3. Nun möchte Anton aber auch E-Mails an Christian senden. Angenommen, Barbara kennt Christian und hat bereits dessen *Public Key* überprüft und vertraut seiner Echtheit. Es bietet sich nun an, dass Barbara Christians Schlüssel signiert, wodurch sie seine Validität bestätigt.

4. Anschließend kann Anton anhand der Signatur auf Christians Zertifikat sehen, dass Barbara diesem vertraut. Stellt Anton nun bei einer Prüfung der Signatur seine Echtheit fest, so ergibt sich daraus automatisch die vertrauensbasierte Echtheit von Christians öffentlichem Schlüssel.

5. Diese Vertrauenskette lässt sich beliebig fortsetzen. Signiert beispielsweise Christian das Zertifikat seines Freundes David, so entsteht ebenfalls eine Vertrauensbasis zwischen Anton und David.

Die Beziehungen, die in den Schritten vier und fünf entstehen, nennt man transitives Vertrauen. In anderen Worten setzt sich das Vertrauen in eine gewisse Person fort, sobald diese mittels einer Signatur die Echtheit weiterer öffentlicher Schlüssel bestätigt. Folglich basiert dieses Verfahren einzig und allein auf dem Vertrauen in die Personen, die man persönlich überprüft hat, und deren korrektem Verhalten. Es wird implizit davon ausgegangen, dass überprüfte Personen sorgsam die Echtheit weiterer Schlüssel sicherstellen und nur solche signieren.

Der Vorteil des *Web Of Trust* ist sicherlich seine einfache Einrichtung sowie ihre verhältnismäßig hohe Leistungsfähigkeit (vgl. Schmeh 2007, S. 447f). Es kommt ohne die Etablierung einer oder

11 Dezentral deshalb, da sie ohne die erwähnte zentrale Zertifizierungsstelle auskommen. Somit werden die Aufgaben dieser Behörde auf verschiedene Instanzen innerhalb des Netzes verteilt.

mehrerer zentraler Instanzen aus und basiert auf sozialen Beziehungen. Das vorausgesetzte Vertrauen in eine übergeordnete und verwaltende Autorität entfällt. Nachteilig ist jedoch seine transitive Struktur. Die entstehenden Vertrauensketten können sehr lang werden, besonders in einem großen Netzwerk wie dem Internet (vgl. Schmeh 2007, S. 447f). Möchten zwei Personen authentisch miteinander kommunizieren, so setzt dies unter Umständen eine Vielzahl von Echtheitsüberprüfungen und Signaturen voraus[12].

3.3 Biometrische Verfahren

Die Kategorie der biometrischen Verfahren (von „(...) griechisch *bios* = Leben und *metron* = Maß (…)“ (Eckert 2014, S. 495)) umfasst Technologien, die Personen anhand ihrer einzigartigen physiologischen Eigenschaften identifizieren und authentifizieren, wodurch sie einen hohen Grad der Fälschungssicherheit ermöglichen (vgl. Tsolkas 2010, S. 148). Obwohl sie zu den effektivsten Mechanismen der Authentifizierung gehören, sind sie doch empfindlich und unterliegen technischen Schwankungen (vgl. Bernauer 2006).

Um die Authentizität einer Person herzustellen muss ein biometrisches System deren anatomische Attribute messen und mit den zuvor gespeicherten Referenzwerten vergleichen. Diese Vergleichsmessung muss im Optimalfall stets das selbe Ergebnis liefern, was eine genaue Kalibirierung und Einstellung der Messgeräte voraussetzt[13] (vgl. Tsolkas 2010, S. 148). Hinsichtlich der möglichen Fehler, die bei dem Authentifikationsvorgang auftreten können, unterscheidet man zwischen *false rejection* und *false acceptance*. Im Falle der *false rejection* wird eine Person abgelehnt, die eigentlich für den Zugriff autorisiert ist. Sie wird also fälschlicherweise als fehlerhaft authentifiziert. Analog dazu wird bei einem Auftreten eines *false acceptance* einer nicht-autorisierten Person der Zugang gewährt (vgl. Eckert 2013, S. 502). Die Häufigkeit des Auftretens dieser beiden Zustände gibt Auskunft über die Zuverlässigkeit und Effektivität des zugrunde liegenden biometrischen Systems (vgl. Tsolkas 2010, S. 149).

Beispiele für biometrische Authentifikationsverfahren sind neben Stimmerkennung und dem Scan der Augen oder des Gesichts der zu authentifizierenden Person die Fingerabdruckerkennung mittels eines entsprechenden Messgerätes[14]. Die zuletzt genannte Technik weist aufgrund der unveränderlichen Einzigartigkeit des menschlichen Fingerabdrucks eine hohe Marktpräsenz auf

12 Für den Fall, dass keine verbindende Kette existiert, ist die aufwändige persönliche Überprüfung nptwendig. Die betroffenen Personen müssen sich also in der realen Welt treffen und ihre Schlüssel validieren.

13 Diese Kalibrierung und Wartung der Messgeräte ist unter Umständen mit zeitintensiven Arbeiten verbunden. Die Beschäftigung von nötigem Fachpersonal ist zudem ein Kostenfaktor.

14 Für detaillierte Beschreibungen der genannten Methoden siehe Eckert 2013 und Tsolkas 2010.

(vgl. Eckert 2013, S. 503f).

Die Authentifikation mittels biometrischer Eigenschaften bringt viele Vorteile mit sich. So gelten die zu messenden Attribute aufgrund ihrer physiologischen Natur als sehr schwer zu fälschen, zudem können sie nicht verloren gehen oder vergessen werden. Außerdem genügt es einem Angreifer nicht, beispielsweise im Gegensatz zur Passwortauthentifikation, im Besitz der Referenzwerte zu sein, die das System zum Vergleich der gemessenen Daten heranzieht. Problematisch wird es jedoch, sobald das Lesegeräte gemessene Daten unverschlüsselt an das prüfende System sendet, da diese seitens des Angreifers abgefangen und zur Maskierung[15] der eigenen Identität verwendet werden können (vgl. Eckert 2013, S. 507). Folglich ist eine lückenlose Absicherung der zum Einsatz kommenden Hard- und Software notwendig.

Des Weiteren kann die Unveränderlichkeit der biometrischen Attribute zu diversen Problemen führen. Im Gegensatz zu wissens- oder besitzbasierten Verfahren zur Authentifikation, die einen einfachen Austausch der Credentials bei einer Kompromittierung erlauben, ist dies bei biometrischen Mechanismen nicht möglich. Die zu messenden Merkmale sind fix und lassen sich nicht erneuern, was unter Umständen dazu führen kann, dass ein Anwender fortan nicht mehr über das eingesetzte biometrische System authentifiziert werden kann. Auch dieser Umstand impliziert eine besondere Sicherstellung der Integrität gespeicherter Referenzdaten (vgl. Eckert 2013, S. 509).

Ein weiterer Problembereich ist krimineller Natur. Da die Informationen, die zur Authentifizierung nötig sind, nun nicht mehr digital sondern physisch sind, setzt die Aneignung und der Diebstahl dieser „Daten“ andere Vorgehensweisen voraus. So steigt zum Beispiel „die Gefahr gewaltsamer Aktionen, um sich in den „Besitz“ dieser menschlichen Schlüssel zu bringen“ (Eckert 2013, S. 508f), beispielsweise durch Erpressung oder anderweitige Drohungen.

3.4 Single Sign-On

> „Ich möchte mir am liebsten nur eine BenutzerID und ein Passwort merken müssen, um mich an alle Anwendungen und Computersysteme in unserem Unternehmen anmelden zu können“ (Tsolkas 2010, S. 181).

Dieses Zitat einer IT-Anwenderin eines größeren Unternehmens aus dem Jahre 2007 verdeutlicht die Umstände, die auf immer mehr Organisationen und Betriebe zutreffen. Die heutige Vernetzung

15 Maskierung bedeutet hier, dass der Angreifer seine eigene Identität verschleiert, indem er sie mit einer autorisierten überlagert.

vieler verschiedener Anwendungen, Server, IT-Systeme sowie der damit einhergehenden Ressourcen setzen eine ausgeprägt Nutzerverwaltung und eine Vielzahl von Zugängen voraus, die kontrolliert werden müssen. Folglich muss sich jeder Anwender zwecks Authentifizierung häufig mehrere Nutzerkennungen und Passwörter merken, die je nach Art der Anwendung variieren können (vgl. Tsolkas 2010, S. 181). Eventuell kommen bei einzelnen Anmeldungen zusätzlich Zwei-Faktor-Authentifizierungsverfahren zum Einsatz, die die Lage komplexer gestalten[16].

Diese Gegebenheiten können zu diversen Problemen führen, die während des Arbeitsalltags auftreten. So steigt zum Beispiel mit der Anzahl an Anwendern und Zugängen die Häufigkeit, in der Kennwörter vergessen, zurückgesetzt und neu vergeben werden müssen. Dies geht mit hohem administrativen Aufwand einher (vgl. Tsolkas 2010, S. 181). Des Weiteren senkt das Vorhandensein multipler Anmeldedaten die Produktivität des jeweiligen Mitarbeiters, da jede Anmeldung, sei es die einer Anwendung, eines Computersystems oder eines Netzwerks, Zeit kostet. Diese Problematik wird noch durch eventuelle Fehleingaben sowie die sinkende Akzeptanz seitens der Anwender erschwert (vgl. Tsolkas 2010, S. 181f).

Die beschriebene Situation legt das Ziel nahe, die verschiedenen Authentifikationsvorgänge der beteiligten Systeme und Anwendungen nutzerseitig zu bündeln, so dass eine Anmeldung genügt, um den Anwender an allen notwendigen Endpunkten anzumelden. Dieses Verfahren bezeichnet man als *Single Sign-On* (SSO). Die einmalige Anmeldung mit anschließendem Zugriff auf alle Systeme wirft zwar die Problematik auf, dass ein potenzieller Angreifer ebenfalls nur eine Hürde zu überwinden hat, die gezielte Absicherung dieser Authentifizierung sowie die damit einhergehende Benutzerfreundlichkeit überwiegen jedoch in der Praxis. Der Anwender wird effektiv entlastet, was sowohl seine als auch die Produktivität der zuständigen Administratoren steigert (vgl. Schmeh 2007, S. 360). *Single Sign-On* lässt sich auf verschiedene Weisen umsetzen.

Eine rudimentäre Lösung zur Vereinheitlichung mehrerer Authentifikationsvorgänge ist die der „*Credential-Synchronisation*“ (Schmeh 2007, Seite 361). Hierbei werden alle *Credentials*, die die Anmeldungen der betreffenden Systeme und Anwendungen verlangen, gleich gesetzt. Folglich kann sich ein Anwender an allen Endpunkten mit den selben Informationen authentifizieren[17]. Dennoch ist eine mehrmalige Anmeldung nötig (vgl. Schmeh 2007, S. 361).

Eine weitere Methode ist die des *lokalen Single Sign-Ons*. Hierbei wird auf dem Rechner der betroffenen Person eine Anwendung installiert, die fortan sämtliche Login-Anforderungen der Server oder Anwendungen entgegen nimmt und diese mit den zugehörigen hinterlegten Passwörtern beantwortet. Hierzu bedarf es einer initialen Authentifizierung der Person gegenüber der Software,

16 Ein Beispiel wäre die Anmeldung mittels Passwort an einem Webportal in Kombination mit einem Zugriff auf eine Datenbank, der das Auslesen einer Smartcard bedarf (vgl. Schmeh 2007).

17 Dies können selbstverständlich neben einem Passwort auch biometrische oder besitzbasierte Credentials sein.

was wiederum auf diversen Wegen möglich ist. Dieses Verfahren setzt voraus, dass alle beteiligten Ressourcen die Preisgabe eines Passwortes verlangen. Nur so lässt sich SSO mittels einer Software umsetzen, da sie keinen Zugriff auf *Token* oder biometrische Merkmale hat (vgl. Schmeh 2007, S. 362).

Eine andere Methode ist der sogenannte *Ticket-Single-Sign-On*. Diese Technik bedarf zusätzlich eines Authentifizierungsservers, der ausschließlich bei Anmeldevorgängen zum Einsatz kommt. Ähnlich dem lokalen SSO authentifiziert sich der Anwender initial gegenüber dem Server. Dieser erstellt fortan sogenannte Tickets, mittel derer der Nutzer an den gewünschten Servern authentifiziert wird. Tickets sind hierbei bestimmte Datensätze, die die Zugangsinformationen der Anwender enthalten und vom Authentifizierungsserver signiert oder verschlüsselt werden. Diese Verfahren setzt ein einheitliches Protokoll voraus, auf Basis dessen die beteiligten Parteien kommunizieren (vgl. Schmeh 2007, S. 362f).

Das sogenannte *Web-Single-Sign-On* bietet sich besonders dann an, wenn die Anwendungen, auf die der Anwender zugreifen will, webbasiert sind, also über einen Browser durch Eingabe einer Web-Adresse zugänglich sind. Hierbei authentifiziert sich der Zugreifende gegenüber einem zentralen Webportal, über das er Zugriff auf weitere Applikationen erhält. Solche Web-Anwendungen und der damit einhergehende Einsatz von Web-SSO sind heutzutage weit verbreitet[18] (vgl. Schmeh 2007, S. 363).

18 Häufig wird Web-SSO mit einem ticketbasierten SSO kombiniert, wodurch die Authentifikation an den beteiligten Servern erreicht wird (vgl. Schmeh 2007).

4 IT-Sicherheit und Authentifikation in Unternehmen

Dieses Kapitel beschäftigt sich mit der Notwendigkeit der praktischen Umsetzung gezielter Schutz- und Abwehrmechanismen hinsichtlich der Authentizität von Mitarbeitern, Kooperationspartnern, Kunden und anderen Subjekten, deren Zugriff auf unternehmenseigene Ressourcen kontrolliert und überwacht werden muss.
Nachfolgend wird anhand von speziellen Gefahrenpotentialen und Risiken erläutert, welche betrieblichen, infrastrukturellen und personellen Eigenschaften eines Unternehmens die Notwendigkeit einer gezielten Authentifizierung begründen.

4.1 Besondere Herausforderungen im unternehmerischen Kontext

> „Die internationale Präsenz, Verflechtung und Vernetzung von Unternehmen im Rahmen der Globalisierung vervielfältigt die Angriffspunkte. Schwachstellen, aufgezeigt durch einen erfolgreichen Angriff oder den Ausfall technischer Systeme, haben durch die Vernetzung und den damit verbundenen Dominoeffekt potenziell stärkere Auswirkungen.“ (Müller 2011, S. 1).

Aus diesem Zitat geht bereits ein wichtiger Aspekt der Notwendigkeit spezifischer IT-Sicherheitsmechanismen hervor. Die fortschreitende Globalisierung vieler Unternehmen und ihre informationstechnologische Vernetzung untereinander über geographische Grenzen hinaus sorgt dafür, dass die Attraktivität eines Angriffes auf dieses weltweite Netz von Ressourcen und Informationen ansteigt. Dies liegt nicht zuletzt darin begründet, dass mit einer immer komplexer und umfassender werdenden IT-Infrastruktur der Aufwand zu deren Überwachung und Absicherung zu nimmt, wodurch es häufiger vorkommt, dass Sicherheitslücken unentdeckt oder unbeachtet bleiben (vgl. Müller 2011, S. 1). Folglich wird die Angriffsfläche für potentielle Attacken größer und unübersichtlicher.
Ein weiterer wichtiger Punkt für den erhöhten Stellenwert von Technologien und Verfahren zur Absicherung vernetzter und betriebseigener IT-Systeme und Anwendungen sind die steigenden Anforderungen durch neue Kooperationspartner, Kunden sowie staatliche Institutionen. Durch den immer größer werdenden internationalen Wettbewerb ist die Ausfallsicherheit von zu einem Geschäftsprozess beitragenden Informationssystemen wichtiger denn je. Ein Ausfall bestimmter

Teile dieser Infrastruktur kann zu Produktivitätseinbußen und monetären Verlusten führen, beispielsweise weil Liefertermine nicht eingehalten werden können oder Kunden mangels Vertrauen in die unternehmenseigene IT der betroffenen Betriebe abwandern (vgl. Müller 2011, S. 1).

4.2 Gesetzliche Regelungen und Normen

Neben den bereits erwähnten Faktoren erhöht sich der Druck auf Unternehmen hinsichtlich der Auseinandersetzung mit IT-Sicherheit und dessen Umsetzung durch behördliche Vorgaben in Form von Gesetzen und Verordnungen. Diese werden zu einem großen Teil im GmbH-Gesetz, im Aktiengesetz (AktG), im Bürgerlichen Gesetzbuch (BGB) sowie im Handelsgesetzbuch (HGB) erläutert[19]. Daneben existieren Normen und Standards, die zu einem Großteil auf Praxiserfahrung und bewährten Vorgehensweisen beruhen. Nachfolgend werden einige dieser Standards auszugsweise vorgestellt, da sie trotz der fehlenden gesetzlichen Pflicht von hoher Bedeutung für die betriebliche IT-Sicherheit sind (vgl. Müller 2011, S. 27).
Die erste hier vorgestellte Sammlung sind die Standards des Bundesamts für Sicherheit in der Informationstechnik (BSI). Diese setzt sich aus folgenden vier Dokumenten zusammen:

- BSI-Standard 100-1: Der erste Teil der 100er Serie beschäftigt sich mit dem Managementsystem für Informationssicherheit (ISMS) und dessen grundlegenden Bestandteilen. Dazu gehören die Management-Prinzipien, die notwendigen Ressourcen, die Mitarbeiter und deren Einbeziehung sowie der Sicherheitsprozess (vgl. Bundesamt 2008b).
- BSI-Standard 100-2: Dieser Teil befasst sich mit geeigneten Sicherheitsmaßnahmen und dem Aufbau eines ISMS zur Etablierung eines gewissen Schutzniveaus (vgl. Bundesamt 2008c).
- BSI-Standard 100-3: Hier wird die Risikoanalyse auf Basis von IT-Grundschutz zur Untersuchung bestehender Gefahren beschrieben (vgl. Bundesamt 2008d).
- BSI-Standard 100-4: Der letzte Teil beinhaltet den Aufbau eines Notfallmanagements, das den reibungslosen Geschäftsbetrieb gewährleisten soll (vgl. Bundesamt 2008e).

Neben dieser vierteiligen Dokumentensammlung der BSI-Standards führt das Bundesamt für Sicherheit in der Informationstechnik die sogenannten IT-Grundschutz-Kataloge. Diese umfassen mehrere Themen bezüglich der Informationssicherheit wie etwa personellen Aspekten,

19 Die in diesen Gesetzbüchern genannten, relevanten Vorgaben sind in ihrer Detailtiefe nicht Bestandteil dieser Arbeit.

Datensicherung und -schutz, Archivierung von Daten sowie Schulungsmaßnahmen. Zudem beschäftigen sich die Grundschutz-Kataloge mit der Sicherheit der betrieblichen Infrastruktur und der betroffenen IT-Systeme, Netze und Anwendungen (vgl. Müller 2011, S. 46f). Zusätzlich bieten sie diverse praktische Hilfsmittel wie zum Beispiel Checklisten, Muster, Beispiele, Dokumentationen und Studien (vgl. Bundesamt 2013).

Eine weitere weit verbreitete Ansammlung von Standards in der Informationssicherheit sind die der 27000er-Familie der International Organization for Standardization (ISO) und der International Electrotechnical Commission (IEC). Zu der ISO/IEC 27000-Gruppe gehören Standards zur Realisierung eines ISMS, Praxisanleitungen für das Management sowie Informationen zum Risikomanagement. Des Weiteren werden Messinstrumente vorgestellt, die die erreichte Sicherheit quantifizierbar machen (vgl. Müller 2011, S. 49). Zudem bietet die Umsetzung der unternehmenseigenen Sicherheitsrichtlinien gemäß ISO/IEC 27000 die Möglichkeit der Zertifizierung. Hierzu begutachtet ein sogenannter Auditor die realisierten Maßnahmen und Praktiken und stellt bei angemessenem Befund ein Zeugnis aus (vgl. Bundesamt 2014). Dieses Zeugnis hat den zusätzlichen Effekt einer imagefördernden Wirkung nach außen, da es Kunden und Partnern ein gewisses Sicherheitsniveau bescheinigt.

4.3 Risikoanalysen als Grundlage sicherheitstechnischer Maßnahmen

Um den notwendigen Aufwand hinsichtlich des Einsatzes von IT-Sicherheits- und Authentifizierungsmaßnahmen im Unternehmen festzustellen, bedarf es interner sowie externer Risikoanalysen.

Müller beschreibt ein solches sicherheitstechnisches Risiko als Zusammensetzung dreier Komponenten, nämlich die Bedrohung, die aktuellen Schwachstellen und die Höhe des potentiellen Schadens beziehungsweise der Schutzbedarf (vgl. Müller 2011, S. 2).

Bedrohungen lassen sich anhand ihrer Entstehung beziehungsweise ihrer Merkmale kategorisieren. Zum einen wären da bedrohliche Ereignisse höherer Gewalt. Dazu zählen unter anderem Unwetter, Erdbeben, Feuerausbrüche, Hochwasser und andere Vorkommnisse, die negative Auswirkungen auf die Verfügbarkeit und Sicherheit von IT-Systemen haben können. Beispiele sind hierbei Strom- und Netzausfälle, die die Einschränkung unternehmerischer Prozesse nach sich ziehen können (vgl. Müller 2011, S. 2ff). Besonders zu betonen ist hierbei der potentielle Ausfall authentifizierender Systeme wie etwa Fingerabdruckscanner oder PIN-basierter, elektronischer Schlösser, was Unbefugten den Zugang zu Gebäuden und Räumlichkeiten ermöglichen kann.

Daneben existieren Gefahrenpotentiale digitaler Natur, die im Hinblick auf die Nutzerauthentifikation und die damit einhergehende Zugriffskontrolle auf geschützte Ressourcen und Systeme von Relevanz sind. Hierzu zählen vor allem Attacken auf Rechnersysteme und unternehmenseigene Server. In diesem Zusammenhang wird häufig der Begriff der Cyberkriminalität genannt, welche die Verwendung von Informationstechnologien und Netzwerken zur Ausübung einer Straftat auszeichnet (vgl. Moore 2010, S. 4). Für das Jahr 2009 können der polizeilichen Kriminalstatistik der Bundesrepublik Deutschland 23.163 Fälle von „(...) Betrug mittels rechtswidrig erlangter Debitkarten mit PIN (…)“ (Müller 2011, S. 5), also eine Form der Authentifizierung, entnommen werden. Zudem weist die Statistik über zwanzigtausend Fälle des Computerbetrugs auf, welche das unerlaubte Erlangen sensibler Daten zur Folge hatten. Diese hohen Messwerte gründen zum Teil auf einer immer höher werdenden Frequenz von Attacken auf Rechnersysteme. Laut einer Aussage der Universität von Maryland aus dem Jahr 2007 „(...) erfolgt alle 39 Sekunden ein Angriff auf einen an das Internet angeschlossenen Computer (…)“ (Müller 2011, S. 5), das entspricht anderthalb Attacken pro Minute. Diese Umstände begründen folglich eine besondere Absicherung durch authentifizierende Technologien, um unautorisierten Zugriff zu erschweren.

Die zweite Komponente eines Risikos für die unternehmenseigene Sicherheit bilden die **Schwachstellen**, die aktuell vorliegen und die es zu untersuchen gilt. Folgende Missstände lassen sich unter anderem laut Müller (2011, S. 9) in Unternehmen beobachten[20]:

M1 „Sicherheitsschwerpunkte und -ziele des Unternehmens sind oftmals nicht, nicht ausreichend oder nicht verbindlich definiert“ (Müller 2011, S. 9). Aus diesem Verhalten der Unternehmensleitung resultiert also häufig ein individuelles Handeln der jeweiligen Fachbereiche, die nicht immer über das nötige Wissen oder die Motivation zur selbständigen Umsetzung ausgewählter Sicherheitsmechanismen verfügen.

M2 Es fehlt den Unternehmen häufig an einem Vorgehensmodell, das die infrastrukturellen und personellen Maßnahmen zur Absicherung der hauseigenen IT beschreibt, was zu Missverständnissen und Sicherheitslücken führen kann.

M3 Eine weitere Schwachstelle vieler Betriebe ist laut Müller die zu sehr betonte Fokussierung auf die Geschäftsprozesse und das Tagesgeschäft. So ist es Mitarbeitern meist ein primäres Anliegen, den Betrieb eines Systems sicherzustellen, ohne dabei frühzeitig an Sicherheitsmaßnahmen zu denken. Das nachträgliche Einbringen sicherheitstechnischer Mechanismen birgt Risiken und Kosten, die vermieden werden können.

20 Die aufgeführten Missstände werden mit den Kürzeln M1 bis M4 bezeichnet, um ein späteres Referenzieren zu erleichtern.

M4 Der letzte hier erwähnte Punkt ist die fehlende oder schwach ausgeprägt Standardisierung von Vorgehensweisen, Konzepten und Vorgaben. Dadurch, dass diese nicht ausformuliert, protokolliert und anderen Mitarbeitern zugänglich gemacht werden, können Differenzen in der erreichten Sicherheit von Systemen und Diensten entstehen. Spezifisches Know-How weisen häufig nur einzelne Mitarbeiter auf.

Neben den erwähnten Faktoren der Bedrohung sowie der vorliegenden Schwachstellen bildet die Höhe des potentiellen Schadens bei Missachtung der sicherheitstechnischen Auseinandersetzung mit der betrieblichen IT-Sicherheit die dritte Komponente eines realen Risikos. Wie bereits erläutert ziehen temporäre oder sogar dauerhafte Ausfälle der betriebseigenen Infrastruktur sowie der betriebenen Anwendungen und Systeme Folgen verschiedenster Art nach sich. Neben dem Vertrauensverlust seitens der Kunden und Partner ist vor allen Dingen der monetäre Schaden zu nennen. Von modernen Informationssystemen wird permanente Verfügbarkeit erwartet, um Geschäftsprozesse gewinnbringend abwickeln zu können (vgl. Müller 2011, S. 12). Ein Ausfall des Zugangs zu geschäftskritischen Ressourcen kann somit geschäftsschädigend sein.

4.4 Authentifizierung zum Schutz wichtiger Ressourcen

Wie bereits erwähnt kann der temporäre Einbruch einer kontinuierlichen Geschäftsfunktion eines betrieblichen Prozesses aufgrund seiner komplexen Vernetzung monetäre Verluste nach sich ziehen oder sich in anderer Weise negativ auf das Geschäft ausüben. Beispiele sind bereits in Form von Imageverlust und Kundenabwanderung beziehungsweise Beschwerden genannt worden.

Jene Prozesse sowie die Ressourcen, die zu ihrer Erledigung und ihrer Aufrechterhaltung notwendig sind, lassen sich als zu schützende Objekte klassifizieren. Zu den besagten Ressourcen zählen beispielsweise Räumlichkeiten, Informations- und Rechnersysteme, Daten, Maschinen und Anlagen, unternehmenseigenes Know-How sowie Personal. Der Schutz dieses unternehmerischen Kapitals in Form von IT, spezifischem Wissen und Humanressourcen bedarf wiederrum geeigneter Vorrichtungen und Maßnahmen. Dies ist der Punkt, an dem neben der Installation von Überwachungskameras, Notstromaggregaten sowie Firewalls und Virenscannern die Authentifikation der beteiligten Anwender und Geräte in Form einer Identitäts- und Rechtekontrolle relevant wird (vgl. Müller 2011, S. 110). Mit Hilfe geeigneter Identifizierungs- und Authentifizierungstechniken lassen sich Zugänge zu internen Ressourcen verwalten. Auf eventuelles Fehlverhalten oder potentielle Angriffe kann zeitnah und kosteneffizient reagiert werden.

5 Empirische Untersuchung der Authentifizierungsverfahren ausgewählter Organisationen

In diesem Kapitel werden die für die empirische Untersuchung herangezogenen Techniken und Methoden beschrieben und erläutert. Darauf folgt die Vorstellung der demographischen und beschreibenden Daten der befragten Organisationen.

5.1 Vorgehen und Methodik

Um die Bedeutung von Authentifizierungsverfahren und die damit einhergehenden Maßnahmen für die Praxis nachzuvollziehen wird im Rahmen dieser Arbeit eine qualitative Untersuchung mit Experten aus verschiedenen Bereichen durchgeführt, die im Alltag mit diesen Verfahren und Technologien in Berührung kommen. Zur Datenerhebung wird das sogenannte Leitfadeninterview genutzt, in dem die Experten gezielt Fragen über den Transfer von Theorie in Praxis beantworten (vgl. Mayer 2009, S. 37f).
Die nachfolgenden Unterkapitel erläutern die Konzeption und Durchführung der Interviews sowie die zugrunde liegenden sozialwissenschaftlichen Methoden.

5.1.1 Das Experteninterview als qualitative Methode

Um die Wahl zur Verwendung von Experteninterviews zur Informationsbeschaffung erklären zu können, ist es notwendig, den Begriff des „Experten“ näher zu erläutern.
In der Literatur herrscht weitestgehend Uneinigkeit darüber, wie dieser Begriff definitionsmäßig zu umranden ist (vgl. Helfferich 2011, S. 163). Dennoch lässt sich aus der Debatte herausfiltern, dass ein mögliches Kriterium zur Klassifizierung als Experte „(…) an dem spezifischen Wissen, an dem Experten teilhaben, festgemacht werden“ kann (Helfferich 2011, S. 163). Meuser und Nagel fügen dieser Definition hinzu, dass ein Experte „(...) in irgendeiner Weise Verantwortung trägt für den Entwurf, die Implementierung oder die Kontrolle einer Problemlösung (…)“ (Meuser 1991, S. 443). Folglich sind als Experten in Unternehmen bzw. Institutionen jene Personen zu betiteln, die in ihrem Tätigkeitsfeld über spezialisiertes, auf Erfahrungen aufbauendes, Wissen verfügen, was sich

in hohem Maße für diese Untersuchung eignet. Da der Experte eine repräsentative Rolle für sein Tätigkeitsfeld einnimmt (vgl. Mayer 2009, S. 38), ist es durch die Befragungen möglich, einen Querschnitt der untersuchten Bereiche in adäquatem Ausmaß zu erhalten.

5.1.2 Der Leitfaden als Befragungswerkzeug

Zur Unterstützung bei den Befragungen und als gedankliche Stütze ist ein Leitfaden verwendet worden, der die Themenkomplexe sowie mögliche Rückfragen grob skizziert. Er ist ein häufig eingesetztes Mittel und soll sich an der „(...) Problemstellung der Untersuchung“ orientieren (Mayer 2009, S. 43).
Hierzu werden möglichst offene Fragestellungen formuliert, ein „(...) Frage- und Antwort-Dialog (...)“ soll vermieden werden (Friebertshäuser 1997, S. 377). Dadurch entsteht ein freier Gesprächsfluss, der bei Bedarf durch gezielte Fragen in eine bestimmte Richtung gelenkt werden kann. Auch der Umfang des Leitfadens sollte auf das Wesentliche beschränkt werden, um die Menge an auszuwertendem Material und den damit verbunden Mehraufwand zu verringern (vgl. Mayer 2009, S. 44f).

5.1.3 Die Themenkomplexe der Befragungen

Der Interviewverlauf ist in zwei große Themenbereiche eingeteilt, die jeweils bestimmte Gegebenheiten in den Organisationen sowie Meinungen und Ansichten der Befragten ansprechen. Der erste Teil der Befragung beschäftigt sich mit den Authentifizierungsverfahren und -technologien, die in den befragten Einrichtungen zum Einsatz kommen, sowie den dazugehörigen Anwendungsbereichen. Wichtige inhaltliche Punkte, auf die in dem Gespräch durch den Interviewten oder durch Rückfragen eingegangen werden soll, sind hierbei unter anderem die Anforderungen an jene Verfahren, die persönliche Zufriedenheit mit den Umsetzungen und potentielle neue Technologien, deren Einsatz denkbar wäre.
Der zweite Themenbereich zielt mit seinen Fragen speziell auf die Anwenderperspektive sowie die Nutzbarkeit und Handhabung der eingesetzten Technologien ab. Neben Problemen, die bei der alltäglichen Nutzung auftreten können, soll hierbei in besonderem Maße das Bewusstsein und die Sensibilität der Nutzer hinsichtlich der Sicherheitsmaßnahmen sowie deren Schulung hinterfragt werden.

5.1.4 Durchführung der Interviews

Die Interviews im Rahmen der empirischen Untersuchung sind in persönlichen Gesprächen mit den Befragten durchgeführt worden. Die Treffen hierzu wurden in den jeweiligen Organisationen vor Ort in einem entsprechenden Besprechungsraum vereinbart. Vor Beginn der Interviews wurden die Personen nach ihrem Einverständnis, die Gespräche auf Tonband zwecks späterer Auswertung aufzuzeichnen, gefragt. Das Einverständnis aller Beteiligten ist demnach im Vorfeld eingeholt worden. Zudem wurden die Interviewten über die Anonymisierung ihrer Identität informiert.
Alle vier Befragungen fanden im November 2014 über einen Zeitraum von zwei Wochen statt. Die dabei entstandenen Audioaufzeichnungen sowie deren transkribierte Inhaltstexte dienen als Grundlage für die weitere Bearbeitung der Befragungsergebnisse.

5.1.5 Auswertung

Zur Auswertung des erhobenen Datenmaterials wird die sechsstufige Inhaltsanalyse nach Mühlfeld u.a. angewendet (vgl. Mühlfeld 1981, S. 335). Sie dient dazu, die Daten der verschiedenen Interviews miteinander vergleichen zu können. Mit der Methode nach Mühlfeld u.a. werden Problembereiche identifiziert und die Kernaussagen herausgefiltert (vgl. Mayer 2009, S. 48).
Die Grundlage der Auswertungsmethode ist die Transkription der Audioaufzeichnungen in Textform. Diese befinden sich im Anhang dieser Arbeit unter den Punkten A2 bis A5.
Der erste Schritt der Inhaltsanalyse sieht das Durchlesen der einzelnen transkribierten Interviews vor. Hierbei werden alle Stellen markiert, „(...) die spontan ersichtliche Antworten auf die entsprechenden Fragen des Leitfadens sind“ (Mayer 2009, S. 48). Anschließend werden die einzelnen Textausschnitte in Verfahrensstufe drei bestimmten Kategorien zugeordnet, die im Vorfeld zu erzeugen sind. Diese Kategorien mit ihren jeweiligen Unterkategorien leiten sich aus den Leitfragen sowie dem allgemeinen Forschungsinteresse ab. Hierbei werden die jeweiligen Interviews in ihre Einzelaussagen zerlegt (vgl. Mayer 2009, S. 49).
Die dritte Stufe sieht vor, eine innere Logik zwischen den Informationen innerhalb eines Interviews herzustellen, die anschließend in Stufe vier verschriftlicht wird (vgl. Mayer 2009, S. 50). Dadurch wird die Relevanz der Aussagen im Hinblick auf die Leitfragen ersichtlich.
Im fünften Schritt wird nun der eigentliche Auswertungstext erstellt. Hierzu wird der in den vorherigen Schritten entstandene Text mit passenden Zitaten aus dem Transkript kombiniert (vgl. Mayer 2009, S. 50). Die Darstellung dieser Auswertung und seiner Interpretation erfolgt im

nachfolgenden Hauptkapitel 6. Die sechste Stufe des Verfahrens sieht die Anfertigung eines Berichts vor, der einer Präsentation des Auswertungstextes dienen soll[21] (vgl. Mayer 2009, S. 50).

5.2 Die ausgewählten Organisationen

In diesem Kapitel werden die Organisationen vorgestellt, die für die empirische Untersuchung der Authentifikationsverfahren und -technologien im betrieblichen und institutionellen Umfeld ausgewählt worden sind. Neben dem Aufzeigen von demographischen Daten wird in den folgenden Unterkapiteln ebenfalls erläutert, in wiefern die jeweiligen Organisationen für die Befragung geeignet sind und welche infrastrukturellen Gegebenheiten sich als legitime Untersuchungsfelder anbieten. Im Rahmen der Untersuchung soll ein möglichst breiter Querschnitt entstehen, welcher durch zwei produzierende Industrieunternehmen, ein Dienstleistungsunternehmen sowie eine Hochschule abgedeckt wird.

5.2.1 Universität Siegen

Die Universität Siegen ist eine „(...) junge moderne Hochschule (...)“ (Universität Siegen 2014a), sesshaft in der gleichnamigen Stadt in Nordrhein-Westfalen. Sie umfasst 19.213 Studierende, gemessen im Wintersemester 2014/2015. Daneben beschäftigt sie 3.224 Mitarbeiter, davon sind 247 Professorinnen und Professoren, 938 wissenschaftliche und 685 nichtwissenschaftliche Mitarbeiterinnen und Mitarbeiter und insgesamt 303 Lehrbeauftragte (vgl. Universität Siegen 2014b).

Die Universität Siegen ist hierarchisch organisiert. Die Zentralverwaltung besteht neben zentralen wissenschaftlichen Einrichtungen und Service-Einrichtungen aus vier Fakultäten mit ihren dedizierten Prüfungsämtern und Forschungsinstituten (vgl. Universität Siegen 2014c).

Diese organisatorische Struktur impliziert einen hohen Verwaltungsaufwand und infrastrukturelle Maßnahmen, um die vielseitigen Interaktionen und Vernetzungen in adäquatem Ausmaß abzudecken. Zudem verarbeitet die Universität Siegen viele personenbezogene Daten, die der Geheimhaltung unterliegen. Dazu zählen neben den Leistungsbewertungen der Studenten auch deren Adressen, Kontoinformationen und weitere persönliche Informationen. Die eingesetzte

21 Der sechste Verfahrensschritt ist für diese Arbeit nicht relevant.

Kommunikationstechnik, die beteiligten Akteure und die Art der zu verarbeitenden Daten machen die Hochschule somit interessant für die empirische Untersuchung.

5.2.2 Deutsche Edelstahlwerke GmbH

Das Unternehmen Deutsche Edelstahlwerke GmbH (DEW) gehört dem international agierenden Konzern Schmolz + Bickenbach AG an (vgl. Schmolz + Bickenbach 2014a) und beschäftigt rund 4.000 Mitarbeiter an mehreren Standorten (vgl. Deutsche Edelstahlwerke 2014a).
Der Betrieb hat sich auf die Erzeugung von Edelstahl spezialisiert und verfügt über moderne Produktionsanlagen und qualifizierte Mitarbeiter (vgl. Deutsche Edelstahlwerke 2014b). Das Angebotsspektrum erstreckt sich über die Beratung bis hin zum Endprodukt nach dem Prinzip „(...) alles aus einer Hand“ (Deutsche Edelstahlwerke 2014b).
Das Leistungsangebot des Unternehmens beinhaltet demnach diverse Produktions- und Verfahrensschritte und bedarf somit technischem Know-How in mehreren Bereichen. Diese Wissensbasis in Kombination mit den weiltweiten Beziehungen und Kooperationen macht die Deutsche Edelstahlwerke GmbH besonders interessant für die Befragung im Rahmen dieser Arbeit, denn die eingesetzte IT-Infrastruktur muss die Sicherheit jener sensiblen Daten sicherstellen. Um dies zu gewährleisten bedarf es einer Nutzerauthentifikation, die den unerlaubten Zugriff verhindert.

5.2.3 Gesellschaft für Information und Bildung mbH

Die Gesellschaft für Information und Bildung mbH (G.I.B) ist ein „(...) mittelständisches Unternehmen der IT-Branche mit Sitz in Siegen“ (Gesellschaft für Information und Bildung 2014). Der 1992 gegründete Betrieb hat sich auf die Entwicklung und den Vertrieb von Softwareerweiterungen von SAP Systemen im Bereich der Logistikoptimierung spezialisiert. Die Kundenbeziehungen verteilen sich international auf Europa, die USA und fernöstliche Länder (vgl. Gesellschaft für Information und Bildung 2014).
Als ein Unternehmen der Informationstechnik-Branche bedarf es einer gewissen Infrastruktur, um die Entwicklung seiner Produkte zu ermöglichen. Zudem muss aufgrund der internationalen Kontakte die betriebsübergreifende Kommunikation gewährleistet sein, was ein Schutzziel der IT-

Sicherheitsmaßnahmen darstellt. Daneben verfügt die G.I.B über ein hohes technisches Know-How im Bereich der Softwareentwicklung und betriebswirtschaftlichen Prozessen, was durch geeignete Sicherheitsmaßnahmen wie etwa der Nutzerauthentifizierung geschützt werden sollte. Daraus ergibt sich eine Relevanz für die empirische Befragung im Bereich der IT-Infrastruktur.

5.2.4 MENNEKES Elektrotechnik GmbH & Co. KG

Das mittelständische Elektrotechnikunternehmen Mennekes GmbH wurde 1935 gegründet und beschäftigt heute rund 1000 Mitarbeiter. Es verfügt über mehrere ausländische Tochterunternehmen wie etwa in China, Russland und Indien (vgl. Mennekes 2014), die die dortigen Märkte bedienen. Das Unternehmen erzielt einen Großteil seines Umsatzes durch den Export seiner Erzeugnisse (vgl. Mennekes 2014). Zu diesen Produkten gehören unter anderem Steckvorrichtungen wie zum Beispiel Ladestecker und -dosen und „(…) Elektromobilitätslösungen in verschiedenen Ausführungen (…)“ (Mennekes 2014).
Wie bereits die Deutsche Edelstahlwerke GmbH tritt die Mennekes GmbH auf internationalen Märkten auf. Sie verwaltet und pflegt demnach einen weiten Kundenstamm, um die weltweiten Kontakte abzubilden. Dies und die Vernetzung mit den Tochterunternehmen bedarf einer ausgeprägten IT-Infrastruktur. Hinzu kommt das technische und produktspezifische Know-How, das die Firma in ihre Produkte einfließen lässt. Zusammen ergibt sich daraus ein wichtiges Schutzziel für die IT-Sicherheit und die dafür verantwortlichen Mitarbeiter, was die Mennekes GmbH zu einem geeigneten Unternehmen für die empirische Unterschung der IT-Sicherheits- und Authentifizierungsmaßnahmen macht.

6 Darstellung und Diskussion der inhaltsanalytischen Untersuchungsergebnisse

In diesem Kapitel werden die Auswertungsergebnisse der durchgeführten empirischen Untersuchung unter Anwendung der im vorangegangenen Kapitel beschriebenen Inhaltsanalyse dargestellt und diskutiert. Die folgenden Unterkapitel entsprechen dem Kategorienschema, das zur Einordnung der Befragungstextpassagen während der Auswertung entstanden ist. Folglich entspricht jedes Kapitel einem Kernaspekt der Interviews sowie dem zugrunde liegenden Leitfaden. Zur Veranschaulichung und gleichzeitigen Belegung der paraphrasierten und in Zusammenhang gebrachten Aussagen werden die Ergebnistexte mit passenden Originalzitaten kombiniert, die der vorgenommenen Deutung als Basis dienen. Die vollständigen transkribierten Interviewtexte können hierbei dem Anhang entnommen werden.

6.1 Aktuelle Situation in den Organisationen

Diese Kategorie umfasst die Aussagen der Befragten hinsichtlich der aktuellen Situation in ihrem Unternehmen was den Einsatz von Authentifikationsverfahren und Technologien anbelangt. Zudem werden die verschiedenen Anwendungsbereiche jener Verfahren sowie die diesbezüglichen organisationellen Vorgaben genannt.

6.1.1 Anwendungsbereiche und zum Einsatz kommende Technologien

Bei der Zusammenfassung der individuellen Aussagen wird deutlich, dass die Verwendung des Authentifizierungsverfahrens mittels Benutzername und Kennwort nach wie vor die gängigste Praxis ist. Laut den Interviewpartnern ist ein Großteil der IT-Infrastruktur der betroffenen Unternehmen zentral organisiert, die Beziehungen und Vernetzungen der Rechnersysteme und somit der jeweiligen Arbeitsplätze sind in einer übergreifenden Domänenstruktur vereinheitlicht. Folglich besteht der Authentifizierungsprozess der Nutzer primär aus der Anmeldung an ihren lokalen Arbeitsstationen mittels wissensbasierter Authentifikation, die die Anmeldung an der zentralen Recheneinheit nach sich zieht. Hierbei stehen den Nutzern also größtenteils personalisierte Zugänge zur Verfügung, auf Basis derer die Rechtevergabe beruht. Ist die Authentizität eines Nutzers

erfolgreich hergestellt, so stehen ihm alle Ressourcen zur Erledigung seiner Aufgaben zur Verfügung:

> „Wir haben verschiedene Systeme, also ob es jetzt im Web ist, dass wir uns da authentifizieren müssen, bezüglich jetzt Benutzername Passwort. Ist immernoch die Herkömmliche“ (Universität Siegen, Anhang A2).

> „(...) Und was aus dieser Sicht dann an Sicherheit auf den auf den Anwender zukommt sind im Grunde genommen die Windows-Authentifikation und zwar nicht am lokalen PC sondern an der Domäne. (…) Bedeutet eben, dass dass niemand irgendwie hier einen Rechner starten kann ohne sich entsprechend zu authentifizieren, grundsätzlich. (…) Also beispielsweise ist es nicht möglich, Arbeitsstationen zu betreiben, ohne Passwort beispielsweise, nur Benutzername und fertig“ (DEW, Anhang A3).

> „Ja also ganz klassisch natürlich die Authentifizierung lokal am Notebook des Mitarbeiters, das ist dann auch gleichzeitig, insofern Netzzugang besteht, auch die Authentifizierung bei uns im Active Directory. (…) Also alles da, wo man auch wirklich einen personlisierten Zugang für benötigt, der auch natürlich abgesichert werden soll, findet auch eine Authentifizierung statt“ (G.I.B, Anhang A4).

> „(...) wo halt jeder Rechner irgendwo, wenn er denn dann gestartet wird, einer Authentifizierung bedarf, sprich ein Benutzername, ein Passwort, womit er sich dann anmelden kann und entsprechende Ressourcen wie sein Outlook, seine Dinge, die er für das tägliche Arbeiten brauch nutzen darf“ (Mennekes, Anhang A5).

Weiterhin lässt sich den Interviews entnehmen, dass der Einsatz weiterer Technologien neben der Passwortabfrage nur punktuell auftritt und häufig je nach Anwendungsbereich variiert. So kommen zwecks Ausleih- und Gebührenvorgängen in der Bibliothek der Universität Siegen Ausweise in Kartenform zum Einsatz, deren Strichcode die Identität der betroffenen Person entnommen werden kann. Zur digitalen Authentifizierung wird hierbei zusätzlich ein Passwort vergeben.
Diese Mischform von Authentifizierungsverfahren lässt sich noch an weiteren Stellen ausmachen:

> „Ich weiß, dass Teile der Verwaltung auch eine Art Ausweis haben, in Anführungszeichen. Das heißt die haben eine Chipkarte schon, aber das sind nur eine Hand voll“ (Universität

Siegen, Anhang A2).

So findet beispielweise innerhalb eines befragten Unternehmens eine räumliche Zutrittskontrolle mittels Chipkarte statt, die Authentifizierung des Mitarbeiters gegenüber den Rechnersystemen und Anwendungen erfolgt jedoch durch multiple Passwortabfragen. Andere Betriebe wiederrum verzichten gänzlich auf physikalische Zugangsauthentifizierung:

> „(...) wo dann auch an Türen zum Beispiel so RFID-Leser sind und wenn der Benutzer dann mit seiner Karte davor steht und die Karte davor hält kommt er entweder rein oder kommt nicht rein“ (Mennekes, Anhang A5).

> „(...) wenn jemand Zugang zu unseren Räumlichkeiten hat, der hat Zugang auch zum Netzwerk“ (G.I.B, Anhang A4).

> „Wenn man jetzt daran denkt, auch Abteilungen körperlich abzuschotten (…), das wird im Großen und Ganzen hier nicht praktiziert, also die Abteilungen sind zunächst einmal offen, kann man sagen, für den Zugang“ (DEW, Anhang A3).

Auch die anderen Organisationen weisen diese Art von Strukturen auf, bei keinem untersuchten Unternehmen ist Single-Sign-On im Einsatz. Häufig müssen sich die Anwender mehrere Passwörter merken und je nach Anwendungsfall sogar Hardware-Token mit sich führen oder ein Software-Token generieren, beispielsweise bei der Einwahl in das eigene Netz oder Kundennetze mittels VPN:

> „Dann gibt es natürlich Authentifizierung noch gegenüber Programmen, (…) wo dann im Moment bei uns kein Single-Sign-On aktiv ist, wo sich dann auch der entsprechende Benutzer, wenn spezifische Programme genutzt werden müssen, dann auch entsprechend authentifizieren muss. (…) Dann gibt es noch Authentifizierung von Extern (…) und da ist dann eine Authentifizierung bei einer VPN über ein RSA-Secure-ID-Authentication-Manager notwendig mit der entsprechenden Secure-ID-Karte (…)“ (Mennekes, Anhang A5).

> „Dann natürlich bei der Einwahl in das Firmennetzwerk, da nutzen wir eine SSL-VPN-Verbindung für Homeoffice, Kundentermine und so weiter und sofort“ (G.I.B, Anhang A4).

Neben den genannten Verfahren setzt lediglich eine Organisation Zertifikate zwecks E-Mail-Verschlüsselung und serverseitiger Authentifizierung ein, jedoch nicht flächendeckend. Hierbei erstellen sich die betroffenen Anwender ihr Schlüsselpaar selbst, es exisitiert keine zentrale Instanz, Geräte zur sicheren Speicherung des privaten Schlüssels existieren nicht:

> „Das heißt also wir, die Studenten, generieren sich ein Schlüsselpaar selbst und authentifizieren sich dann eben entsprechend gegenüber uns dann serverseitig (…). Da ist es so, dass diese Schlüsselgenerierung wie gesagt selbst gemacht wird, es gibt keine zentrale Instanz erstmal dafür. Und das ist also noch so ein Thema mit dieser Public Key Authentifizierung, das ist also nicht flächendeckend“ (Universität Siegen, Anhang A2).

Anhand der genannten Auffälligkeiten ist erkennbar, dass den Umsetzungen der sicherheitsrelevanten Mitarbeiteridentifikation und -authentifikation häufig kein einheitliches Konzept zugrunde liegt. Viele Maßnahmen werden laut den Befragten erst dann eingeleitet, wenn ein entsprechendes Ereignis auf einen Missstand hinweist, was die IT-Landschaft der Organisationen unkontrolliert wachsen lässt und unübersichtlich macht. Auch stehen manche Lösungen dem betrieblichen Ablauf im Weg, wie zum Beispiel die Notwendigkeit der Registrierung der zum Einsatz kommenden Maschinen, was ein flexibles Austauschen oder Warten der Gerät erschwert:

> „Das ist so ein typischer Fall wo die Sicherheitsinteressen vielleicht den betrieblichen Interessen kurzfristig im Wege stehen“ (DEW, Anhang A3).

6.1.2 Interne Vorgaben und deren Umsetzung

Auf die Frage nach der Beschaffenheit unternehmensinterner Vorgaben hinsichtlich der Benutzerauthentifikation und ähnlicher sicherheitsrelevanter Verfahren und Verhaltensweisen antworten alle Organisationen ähnlich. Grundsätzlich ist die Vorgabe von Richtlinien, einzuhaltenden Regeln und Mechanismen hierarchisch strukturiert und gilt in der Regel unternehmensweit oder zumindest für alle Mitarbeiter, die Zugriff auf die IT-Systeme haben. Das heißt, dass die einzelnen Abteilungen nicht selbst über das Ausmaß und die Umsetzung bestimmter IT-Sicherheitsverfahren wie etwa die Benutzerauthentifikation und den Umgang mit Daten und Informationen bestimmen, sondern dies einheitlich und von zentraler Stelle aus koordiniert wird:

„Das heißt also nicht die einzelnen Abteilungen legen fest, wie Sicherheit praktiziert wird, sondern es gibt Richtlinien, die allgemeingültig sind das heißt für das ganze Unternehmen gelten. (…) Ja, die dann aber koordiniert werden von einer zentralen IT. (…) Es gibt also eine Abteilung, (…) die zuständig ist für die Belange der Gesamt-IT an den Standorten (…)“ (DEW, Anhang A3).

„Also wir sind da jetzt so vom Unternehmen her eigentlich so strukturiert, dass wir da in der IT weitestgehend freie Hand haben was wir umsetzen oder auch was für Kennwortrichtlinien wir da vergeben zum Beispiel“ (G.I.B, Anhang A4).

„Generell gibt es grundsätzlich Richtlinien für Mitarbeiter, die hier quasi Zugriff auf IT-Systeme haben, die den Umgang mit IT-Technik regeln, mit Daten regeln (…)“ (Mennekes, Anhang A5).

Hierbei spielen bei allen Befragten die jeweiligen IT-Abteilungen eine tragende Rolle. Diese spezifizieren Richtlinien, beispielsweise die Wahl der Passwörter betreffend, die allgemeingültig sind und auch kurzfristig geändert oder angepasst werden können. Folglich liegt dieser Festlegung kein komplexer Prozess zugrunde, der die Einführung oder Änderung legitimiert:

„Und das würde dann bei uns auch wirklich ganz, wie soll ich sagen, unkompliziert durchgesetzt, dass wir also dann zum Beispiel die Kennwortrichtlinien von heute auf morgen dann auch ändern können. Das ist natürlich vom Prinzip, vom Prozedere keine komplizierte Sache (…)“ (G.I.B, Anhang A4).

Während dies bei zwei der kleineren Betriebe der Fall ist, wird dieses Verfahren in dem Industrieunternehmen Deutsche Edelstahlwerke um die Delegation an Koordinatoren innerhalb der Abteilungen erweitert, die die Informationen an die Mitarbeiterschaft weiter geben:

„Aber um das alles zu vereinheitlichen hat man gesagt okay, wir versuchen, in den Hauptabteilungen (...) bestimmte Mitarbeiter mit bestimmten Aufgaben was auch IT-Infrastruktur angeht also denen bestimmte Aufgabe zu übertragen“ (DEW, Anhang A3).

Laut einem Interviewpartner hat der technische Sachverstand vieler Angestellter zugenommen, was

häufig dazu führt, dass gewisse Entscheidungen wie die Komplexität eines Kennwortes den Nutzern überlassen wird. Dies verdeutlicht den Ermessensspielraum mancher IT-Abteilungen, gewisse Verantwortungen an Endanwender abzugeben oder den Umfang und die Stringenz mancher Restriktionen beziehungsweise Richtlinien zu mindern, was den Missständen M1 und M4 nach Müller[22] entspricht:

> „Wir haben die Richtlinien sehr gering gehalten (…)“ (G.I.B, Anhang A4).

> „(...) also von der Struktur der IT sieht es so aus, dass von unten nach oben sag ich mal der Sachverstand zunimmt, das heißt also selbst auf unteren Ebenen gibt es mittlerweile sehr viele Mitarbeiter, die sich mit Rechnertechnik und diesen Dingen auskennen“ (DEW, Anhang A3).

> „(...) wobei wir jetzt im Moment noch nicht vorgeben, dass das Passwort nach vier, weiß ich nicht, vier sechs Wochen abläuft oder geändert werden muss. Also wir überlassen das im Moment dem Mitarbeiter, das selbstständig zu tun. Von daher haben wir jetzt da nicht ganz strikte Regelungen“ (Mennekes, Anhang A5).

Es liegt also bei den befragten Organisationen gemäß Missstand M4 keinerlei Standard oder Vorgehensmodell vor, die den Prozess der Einführung neuer Sicherheitsmechanismen abbilden oder verschriftlichen. Häufig werden Änderungen spontan und kurzfristig vorgenommen. Auf die Frage nach dem Einführungsprozess einer neuen Technologie hin skizzierte ein Experte einen groben improvisierten Ablaufplan, der zwar eindeutige Schritte enthielt, jedoch nicht vorgegeben zu sein scheint:

> „Also das muss man dann irgendwo in einer Testphase sicherlich mal so ein bisschen eroieren, Kostenfaktor Nutzenfaktor ganz klassisch gegenüber stellen und dann wird das in einer Testphase mal so auf Alltagstauglichkeit getestet und dann auch umgesetzt“ (G.I.B, Anhang A4).

22 Die vier Missstände, die sich laut Müller in Unternehmen beobachten lassen, werden in Kapitel 4.3 erläutert.

6.1.3 Zufriedenheit der Befragten mit der Gesamtsituation

Die Frage nach der Zufriedenheit der Befragten mit den aktuell im Einsatz befindlichen Lösungen hinsichtlich der Nutzerauthentifikation bringt unterschiedliche Aussagen hervor. Während das Kennwortverfahren weiterhin als gut funktionierendes und bewährtes Mittel beschrieben wird, gaben einige befragte Experten ihre punktuelle Unzufriedenheit kund. So wird das Mittel der Passwortauthentifikation nur als einfachste, grundlegendste Lösung gesehen, die es zu optimieren gilt. Diesbezügliche Richtlinien, die die Komplexität und Aktualität dieser Credentials festlegen, seien verbesserungswürdig beziehungsweise liegen stellenweise erst gar nicht vor. So lassen die Interviewpartner gewisse Defizite offenkundig werden, die in naher Zukunft beseitigt werden sollen:

> „Also Benutzername Passwort ist ein gängiges, gut funktionierendes Mittel. (…) Allerdings ist Benutzername Passwort prinzipiell immer nur das einfachste Mittel und nicht das beste. Aber wenn man keine anderen Möglichkeiten eben hat, muss man eben darauf zurückgreifen“ (Universität Siegen, Anhang A2).

> „Ja gut ich sag mal so, für die interne Authentifizierung, (…) da sind wir vielleicht sicherlich nicht so up-to-date. Da gibt es sicherlich schon Kennwortrichtlinien, die ein bisschen sicherer sind (…). Aber gerade mal das reine Kennwort, das werden wir also auf jeden Fall noch verschärfen müssen (…)“ (G.I.B, Anhang A4).

> „Aus IT-Sicht sind wir nicht zufrieden. Weil wir da sicherlich noch Bedarf haben, das noch zu verstärken beziehungsweise dann auch Authentifizierung zu vereinfachen (…). (…), wir wissen, dass wir noch Defizite haben“ (Mennekes, Anhang A5).

Hierbei wird jedoch darauf hingewiesen, dass die Einführung bestimmter neuer Systeme und Mechanismen unter Umständen hohe Kosten verursachen könnte, die der Sinnhaftigkeit jener Anschaffungen gegenüber zu stellen sind. Somit liege jeder Veränderung der Kompromiss zwischen Finanzierbarkeit, Benutzbarkeit und Sinnhaftigkeit zugrunde:

> „Und da gehts wieder darum, ja, es gibt Sachen, die kann man besser machen, aber die kosten soviel Geld, dass man sagt, das macht keinen Sinn. (…) Und das ist immer der Kompromiss, den man in der IT-Sicherheit irgwendwann schließen muss. Zwischen

> Finanzierbarkeit, Benutzbarkeit und macht es dann überhaupt Sinn (…)“ (Universität Siegen, Anhang A2).

Außerdem gibt ein Experte an, dass vollzogene oder geplante Maßnahmen häufig aus Sicht der Anwender nicht nachvollziehbar seien, beispielsweise die regelmäßige Änderung der Kennwörter. Zwar hätten die Nutzer gelernt, Restriktionen eher zu akzeptieren, dennoch seien die Interessen in dieser hinsichtlich gegeläufig:

> „Jemand der die Systeme nur benutzt um damit seinen alltäglichen Kram zu erledigen, seine Arbeit zu machen, der wird das nicht immer nachvollziehen können. (…) Da sind die Interessen ein bisschen gegenläufig, da wird häufig gewünscht die Hürden nicht ganz so hoch zu machen, um eben Rückfragen zu verhindern (…)“ (DEW, Anhang A3).

Zusammenfassend sind sich die Befragten einig, dass die Authentifizierungsvorgänge während der alltäglich zu verichtenden Arbeit vereinfacht beziehungsweise transparenter werden müssen:

> „Und ohne jetzt wirklich gute Beispiele parat zu haben (…) war es in manchen Fällen so, dass dann auch wieder Richtlinien, die halt zu scharf für die Praxis waren, ein bisschen gelockert werden mussten“ (DEW, Anhang A3).

Zudem müssten die zum Einsatz kommenden Verfahren stets anhand der zu schützenden Informationen und somit den Sicherheitsanforderungen der jeweiligen Bereiche bewertet werden:

> „Aber nochmal, prinzipiell ist immer, was will ich damit schützen und so ist die Situation okay (…)“ (Universität Siegen, Anhang A2).

6.2 Potentieller Einsatz neuer Techniken

Dieser Themenbereich der Befragungen beinhaltet die Vorstellungen und Wünsche der Experten hinsichtlich einer ihrer Meinung nach optimalen Konstellation von Authentifikationsverfahren und Techniken innerhalb ihrer Organisationen. Hierbei soll herausgefunden werden, den Einsatz welcher weiteren Technologien und Mechanismen sich die Interviewpartner vorstellen können, um

den von ihnen genannten Mängeln und Defiziten entgegen zu wirken.
Zusätzlich werden die Experten hinsichtlich der potentiellen Einrichtung eines dezentralen Authentifizierungsschemas befragt, das in seiner Funktionsweise der des *Web Of Trust* ähnelt.

6.2.1 Optimale Lösung und Einsatz weiterer Technologien

Bei Betrachtung der verschiedenen Aussagen der jeweiligen Epxerten fällt besonders der Wunsch nach Vereinheitlichung und Zentralisierung der unterschiedlichen im Einsatz befindlichen Techniken und Verfahren auf. So favorisiert ein Gesprächspartner den elektronischen Ausweis, beispielsweise in Form einer Smartcard, als alleiniges Mittel zur Authentifikation von Personen. Laut seiner Aussage lassen sich auf diese Weise die vielen verschiedenen Zugänge und Nutzeridentitäten auf einem einzigen Medium zusammenfassen, so dass die Vergabe multipler Passwörter unnötig wird. Diese Vorstellung wird von einem anderen Experten geteilt, welcher sich ebenfalls die Vergabe eines zentralen *Credentials* zwecks unternehmensweiter Authentifizierung wünscht. Er gibt weiterhin an, dass die Verwendung eines solchen Single-Sign-On-Verfahrens die Anmeldungen der Nutzer an internen sowie externen Rechensystemen und Anwendungen kontrollierbarer und transparenter mache. Zudem erleichtere dies den Arbeitsalltag der betroffenen Mitarbeiter:

> „Ich war immer ein Freund halt der von elektronischen Ausweisen. (…) auch hier wäre die Möglichkeit eben das eben zu zentralisieren, nur über Chipkarte oder über einen Chip (…). Die Idee dahinter wäre wie gesagt (…) ein richtiges Single Sign On, mit einer Karte und einer Pin“ (Universität Siegen, Anhang A2).

> „(...) und halt das Single-Sign-On, was dann dahinter steckt, dass Transparenz da ist zum Login, zu anderen Applikationen. Also dass quasi der Anwender sich ein Passwort merken muss und dann dementsprechend in allen Applikationen, die ihm zur Verfügung gestellt werden oder wofür er berechtigt ist dann drauf zugreifen darf“ (Mennekes, Anhang A5).

Daneben ergibt die empirische Untersuchung, dass die Nutzung einer zertifikatsbasierten Authentifikation von Arbeitsgeräten denkbar ist. So erläutern gleich zwei der vier Befragten, dass es wichtig zu wissen sei, welcher Mitarbeiter sich mit welchem Gerät in das Firmennetz einwählt. Dies sei laut den Experten durch die Vergabe und Installation individueller Zertifikate realisierbar,

anhand derer ein Rechner beziehungsweise sein Nutzer eindeutig identifiziert und authentifiziert werden könne:

> „Also wenn man sich da was wünschen dürfte, ich persönlich finde es immer ganz gut, wenn man wirklich weiß welche Personen sich einwählen und welche Geräte sich einwählen. (…) Und natürlich irgendwo von der Authentifizierung diese Geschichte, dass ich da wirklich sagen kann okay, nur der der das Zertifikat im Bauch hat darf sich pauschal hier einwählen, der kommt überhaupt erst auf die Login-Maske“ (G.I.B, Anhang A4).

> „Es wäre sicherlich schon irgendwas wo wir wissen, dass wirklich der Client auch unser Client ist, der sich hier authentifizieren möchte. Sprich eine Zertifikatslösung vielleicht abhängig von einem Client zu schaffen, dass man genau weiß aha der Client der darf hier rein“ (Mennekes, Anhang A5).

Eine weitere Übereinstimmung in den jeweiligen Befragungsergebnissen stellt der Einsatz einer Mischform unterschiedlich kategorisierter Authentifikationsverfahren dar. So seien die aktuellen beziehungsweise hypothetischen Maßnahmen erweiterbar, beispielsweise um biometrische oder besitzbasierte Authentifizierung. Die Technologien zur biometrischen Messung und Identifikation hätten sich hierzu gut entwickelt, jedoch stelle sich hierbei erneut die Frage nach der Akzeptanz der Endanwender. Folglich solle die Techniklandschaft in den Unternehmen nicht unnötig verkompliziert werden, um die Geschäftsprozesse sowie den Arbeitsalltag nicht zu behindern:

> „Und auch von biometrischen Merkmalen, (…) die Technologie hat sich dahingehend sehr gut entwickelt und auch, also sie ist halt robust geworden und das ist halt entscheidend“ (Universität Siegen, Anhang A2).

> „Also schon so diese One-Time-Passwords, was weiß ich, jetzt auch wieder das klassische Hardware-Token ist auch bei uns natürlich im Gespräch. (...) jeder Kollege bekommt so ein Teil in die Hand, was er dann an sein Schlüsselbund machen kann, wie auch immer. Das kann man ja handlen, das kann man ja auch administrieren“ (G.I.B, Anhang A4).

> „Also da wollen wir natürlich schon irgendwo auch so alltagsfreundlich bleiben, dass man das nicht irgendwie unnötig verkompliziert“ (G.I.B, Anhang A4).

6.2.2 Einschätzung der Entwicklung eines dezentralen Systems

Wie bereits erwähnt zielt dieser Fragenblock auf die hypothetische Einführung eines Systems ab, innerhalb dessen sich die teilnehmenden Nutzer, im Unternehmenskontext also Gruppen wie Mitarbeiter, Partner, Kunden und Interessenten, gegenseitig authentifizieren. Hierbei beruht also die Authentizität eines Einzelnen auf dem Vertrauen anderer in seine Identität und Credentials. Folglich werden Attribute und die Richtigkeit der individuellen Identität nicht von zentraler Stelle aus koordiniert, sondern setzen sich in entstehenden Vertrauensketten innerhalb des Unternehmens und über seine Grenzen hinaus fort.
Ein Großteil der Befragten hält die menschliche Komponente innerhalb des vorgestellten Verfahrens für den ausschlaggebenden Faktor. So stellt sich für die Experten vordergründig die Frage, ob die sozialen Strukturen dafür geeignet sind. Hierzu geben sie diverse Bedenken an, besonders im Hinblick auf plötzlichen Vertrauensverlust in andere Personen sowie der eventuellen Notwendigkeit, Fremden oder externen Personen ein gewisses Maß an Vertrauen entgegen zu bringen:

> „Jetzt kennen Sie wieder jemanden oder vielleicht auch nur halb und der ist aber nicht vertrauenswürdig und dann bin ich wieder in dieser Kette, dass ich dann auch sage, okay, dann will ich ihm dann aber auch vertrauen und ich will es aber nicht. Also die Frage ist immer, wie es sozial funktioniert“ (Universität Siegen, Anhang A2).

> „Ich habe jetzt andere Freunde als der (anonym) Freunde hat und ob ich jetzt automatisch seinen Freunden vertrauen würde weiß ich nicht, dafür kenne ich die Leute zu wenig und wenn ich verantwortlich für den Bereich wäre und sagen würde alle deine Freunde sind auch meine Freunde, hätte ich jetzt ein Problem mit ganz ehrlich gesagt“ (Mennekes, Anhang A5).

Dies führe unter Umständen zu einer ablehnenden Haltung der Anwender und sei daher in großen Gruppen, wie sie beispielsweise die Belegschaft eines größeren Unternehmens oder komplexe Kundenbeziehungen darstellen, nur schwer umzusetzen:

> „(...) dann müssen wir das ja wieder größer denken, denn die Uni an sich okay, aber wir arbeiten ja viel nach draußen (…), wenn ich dann einen Nutzen haben will muss ich natürlich auch allen anderen Unis das Vertrauen schenken (...), das heißt es ist ein

komplettes Netz was entstehen müsste (…)“ (Universität Siegen, Anhang A2).

Laut eines Experten wisse man nie, wie gewisse fremde Personen innerhalb einer entstehenden Vertrauenskette mit Informationen und Daten umgehen:

> „Da hätte ich wahrscheinlich auch ein Problem mit, weil ich die Freunde nicht kenne und auch nicht weiß, wie die ticken, wie die umgehen mit bestimmten Informationen“ (Mennekes, Anhang A5).

Zudem entspreche der Automatismus der Vertrauensfortsetzung wahrscheinlich nicht mehr den Richtlinien des betroffenen Unternehmens:

> „(...) also wenn er es runter deligiert auf den Mitarbeiter und der sagt dann ich habe tausend Freunde, die will ich auch alle mit da rein lassen (…), dann kann ich mir nicht vorstellen, dass das funktioniert und hinterher auch noch den Richtlinien der Firma entspricht“ (Mennekes, Anhang A5).

Ein anderer Interviewpartner wies zusätzlich darauf hin, dass viele Mitarbeiter nicht das notwendige technische Know-How aufweisen, um die Vertrauenswürdigkeit einer Person und seines Umgangs mit IT und Sicherheit zu bewerten:

> „(...) und nur, dass jetzt derjenige sich kennt oder sonstwas, dieser Zugang freigeschaltet wird, der weiß ja garnicht was nutzt der für Hardware, was nutzt der für Client-Software (…). (…) aber dass jetzt da ein Kollege, der jetzt irgendwo das entsprechende Know-How garnicht sowas zu bewerten, dass der das jetzt irgendwie freischaltet, da hätte ich jetzt glaube ich ein ungutes Gefühlt bei“ (G.I.B, Anhang A4).

Dies entspricht auch der Meinung eines dritten Experten, der die gegeben Strukturen für ungeeignet hält, da sie so konstruiert seien, von zentraler Stelle aus Benutzer und Rechtevergaben zu koordinieren und zu kontrollieren. Das automatische Wachsen solcher Vertrauensketten sei schlichtweg nicht vorgesehen und stellenweise sogar kritisch. So äußert einer der Befragten Bedenken, sobald jemand auf das firmeneigene Netz zugreift, der sich zwar in einer Vertrauenskette befindet, jedoch nicht direkt vom betroffenen Unternehmen überprüft und autorisiert worden ist:

„Zum Anderen glaube ich nicht, dass die Strukturen oder das Denken so von Sicherheit so etwas hergibt. So eine automatische Vererbung quasi von Vertrauen an Dritte womöglich. Ne ich glaube das wäre nicht so der gangbare Weg. (…) Weil einfach die Strukturen geeignet und auch dafür gedacht sind, von zentraler Stelle auch die Kontrolle zu behalten“ (DEW, Anhang A3).

„Und wenn jetzt dort eben unser Lieferant A, ohne dass wir das jetzt irgendwo steuern oder controllen können, auf einmal einem unbekannten Lieferanten B den Zugang auf unsere Systeme gewährt, dann muss ich sagen so spontan wäre ich dann sicherlich ein bisschen skeptisch“ (G.I.B, Anhang A4).

6.3 Menschliche Komponente im Authentifizierungsprozess

Der letzte Themenbereich der Befragungen befasst sich mit den erläuterten Gesamtsituationen in den jeweiligen Organisationen aus der Sicht der Anwender. Hierzu werden die Experten gezielt nach der Anwenderfreundlichkeit und Bedienbarkeit der eingesetzten Technologien und Mechanismen sowie dem möglichen Auftreten von Problemen und Fehlverhalten der Nutzer befragt. Zudem werden die Befragten gebeten, ihre Einschätzung bezüglich des Bewusstseins und der Sensibilität der Nutzer im Hinblick auf IT-Sicherheit und den damit einhergehenden Authentifizierungsmaßnahmen zu erläutern. Abschließend umfassen die Interviews eventuelle Schulungs- und Sensibiliserungsmaßnahmen, die in den Unternehmen bereits vollzogen worden oder in Planung sind.

6.3.1 Bedienbarkeit der Mechanismen

Fasst man die Aussagen der Interviewpartner zusammen, so wird eine gewisse generelle Zufriedenheit deutlich. Laut den Experten sei den Anwendern ein gewisses Maß an Komplexität zumutbar, wobei der Fokus darauf liege, die vorhandene Techniklandschaft im Hinblick auf die erzwungene Authentifizierung der Nutzer nicht zu sehr zu verkomplizieren. Es sei wichtig, dass der Nutzer sich keine Gedanken in diesem Zusammenhang machen müsse und möglichst nicht bei seiner alltäglichen Arbeit gestört werde. Ein Befragter gab an, dass eine einmalige Authentifikation des Anwenders zu Beginn des Tages ausreiche, um Zugriff auf alle seine benötigten Ressourcen zu

erhalten:

> „(...) Das heißt, dieser Schritt war schonmal gut, der war glaube ich auch gar nicht so einfach, weil da eine Menge Aufwand hinter steckt. Und in sofern finde ich jetzt die Benutzbarkeit dessen, was jetzt da ist ganz okay, ja“ (Universität Siegen, Anhang A2).

> „Gelingt diese Anmeldung, stehen alle entsprechend zugewiesenen Ressourcen sofort offen. Also (…) der Mitarbeiter kann natürlich sofort loslegen und der muss sich nicht drum kümmern, ob da ein Drucker eingerichtet ist oder irgendwas. Also seine Welt ist erstmal damit komplett verfügbar“ (DEW, Anhang A3).

> „(…) ich glaube im Vergleich zu anderen Unternehmen (…) haben wir was das Stichwort Authentifizierung angeht jetzt keine unnötige Verkomplizierung, so dass jetzt sicherlich bei uns der Anwender ich sage mal so ganz salopp sich nicht beschweren kann“ (G.I.B, Anhang A4).

> „Bedienbarkeit denke ich mal ist in Ordnung. Es hat eine gewisse Komplexität aber es ist noch relativ handhabbar (…)“ (Mennekes, Anhang A5).

Ein weiteres Argument für die Vereinfachung der notwendigen Anmeldevorgänge seien laut eines weiteren Experten die spezifischen Sicherheitsanforderungen des jeweiligen Unternehmens. So werden die Informationen innerhalb einer untersuchten Organisation als relativ unkritisch eingeschätzt, eine komplexe Nutzerauthentifikation stünde möglicherweise nicht mehr in Relation mit dem Unternehmen und dessen Produkten beziehungsweise Dienstleistungen:

> „Wenn ich jetzt irgendwo sagen muss okay, ich muss jetzt hier erst auf der Firma anrufen und sagen schaltet mich frei (…), dann hat man irgendwann die Stufe erreicht wo man sagt das steht jetzt vielleicht nicht mehr in einer Relation zu einem Unternehmen, was jetzt vielleicht nicht unbedingt in der Rüstungsindustrie tätig ist oder sowas. Die haben vielleicht berechtigterweise ein bisschen höhere Anforderungen was die Authentifizierung angeht“ (G.I.B, Anhang A4).

Dennoch geben einige der Experten gewisse Mängel und Verbesserungsvorschläge an. So sei laut eines Befragten Optimierungspotential im Hinblick auf die Nutzung von Single-Sign-On vorhanden. Aktuell müssen sich Anwender der Sicherheitsmechanismen teilweise mehrere

Kennwörter und Zugangsinformationen merken, um die gewünschten Anwendungen und Systeme nutzen zu können. Dies soll gemäß des Wunschdenkens der Experten vereinheitlicht und somit zugänglicher für die Menschen gemacht werden, die ihre alltägliche Arbeit verrichten möchten. Auch einen zusätzlichen Schutz dieses integrierten Zugangs durch die Kombination mit anderen Verfahren schließt ein Experte nicht aus:

> „Ja also, wie gesagt jetzt auch da Ist-Zustand bei uns, was vielleicht so ein bisschen ein Kritikpunkt des Anwenders sein kann, wo man Optimierungsbedarf hätte, ist sicherlich so das Stichwort Single-Sign-On. (…) Und dann kann man sicherlich da irgendwo einen Automatismus einrichten, dass ich mich nur einmalig anmelde und auf allen anderen Systemen, die ich während meines Arbeitstages nutze, wird dann eben dieses Login weitergereicht“ (G.I.B, Anhang A4).

> „Aber sicherlich, Username und Kennwort als alleinige Authentifizierung ist optimierungsbedürftig, das haben wir auch bei uns erkannt (…)“ (G.I.B, Anhang A4).

Die Einführung eines Single-Sign-On-Mechanismus führe allerdings auch dazu, dass gewisse Restriktionen, beispielsweise die Struktur der Passwörter betreffend, verschärft werden müssten, da in diesem Falle mehrere Systeme und Datenbereiche an dem zentralen Zugang hängen:

> „Und je mehr ich natürlich von einem Kennwort irgendwo abhängig mache, Stichwort Single-Sign-On, desto komplizierter muss ich natürlich mein Kennwort machen (…)“ (G.I.B, Anhang A4).

Hier gilt es also, die Balance zwischen Bedienbarkeit, Anwenderfreundlichkeit und dem notwendigen Maß an Sicherheit herzustellen. Dies obliegt gemäß der Aussage eines Experten der jeweiligen unternehmenseigenen IT-Abteilung:

> „(...) es hängt ein bisschen von der IT auch ab wie sicher die Systeme dann sind. Das ist ja unsere Verantwortung (…)“ (Mennekes, Anhang A5).

6.3.2 Verhalten und Bewusstsein der Nutzer hinsichtlich Sicherheit und Authentifizierung

Während die vorhandenen Systeme und Mechanismen den Umständen beziehungsweise den Anforderungen entsprechend als relativ sicher und angemessen eingeschätzt werden, so geben die Befragten häufig den Menschen selbst als Schwachstelle an. So gehen manche Nutzer beispielsweise recht sorglos mit der Vertraulichkeit und Sicherheit ihrer Kennwörter um, was sich in Form von Notizzetteln am Monitor des Arbeitsplatzes mit dem entsprechenden Kennwort im Klartext darauf äußert. Auch die erzwungene Passwortänderung wird oft dadurch entkräftet, dass die geheimen Zeichenketten nur marginal abgeändert werden:

> „Gut, die Schwachstelle sollte oder dürfte der Benutzer selbst sein in dem Fall“ (DEW, Anhang A3).

> „Indem man jetzt sagt naja, ich muss zwar jedes Mal mein Kennwort ändern aber ich zähle einfach nur die Zahl hoch, was ja dann dem Kennwortändern entspricht aber eigentlich vielleicht dem Grundgedanken nicht (…). (…) aber ich kann halt nicht verhindern, dass der sich es auf ein Blatt Papier schreibt und an den Monitor heftet“ (G.I.B, Anhang A4).

Diese zu beobachtende Sorglosigkeit hat laut einem Experten mitunter bereits zu sicherheitskritischen Vorfällen geführt, die aufgrund ihrer Schwere und Folgen den Mitarbeitern die möglichen Gefahren haben bewusst werden lassen. Hierdurch hätten viele Kollegen gelernt, dass sie ihren Teil zur System- und Unternehmenssicherheit beitragen müssen, die Nachlässigkeit habe deutlich nachgelassen:

> „(…) wir hatten schon Ereignisse, die durchaus geeignet waren den Anwendern oder überhaupt den Mitarbeitern hier klar zu machen, wie gefährlich eigentlich auch Datentechnik werden kann (…). (…) Also ich glaube spätestens danach war allen klar, dass jeder selbst auch seinen Teil an Verantwortung und Bemühen dazu beitragen mussten, um die Systeme wirklich sicher zu machen am Ende“ (DEW, Anhang A3).

Die Frage, wie die Experten das Bewusstsein der betroffenen Anwender einschätzen, ergibt unterschiedliche Aussagen. Ein Befragungsteilnehmer gibt an, das Bewusstsein derer, die mit Informationstechnologie zu tun haben oder daran interessiert seien, sei recht hoch. Im Gegensatz dazu weisen die reinen Anwender der Technik nur wenig Verständnis für die Notwendigkeit

bestimmter Verfahren auf. Ihnen ginge es primär darum, ihre Arbeit zu verichten, ohne dabei durch ihrer Meinung nach unnötige Hürden gestört zu werden, was dem Missstand M3 aus Kapitel 4.3 entspricht. Die eingesetzten Verfahren sollen daher einfach handzuhaben sein, was sich in einer geringen Kennwortkomplexität wiederspiegele. Dies erschwere laut den Experten in Kombination mit schwach ausgeprägtem technischen Wissen die Einführung neuer Technologien:

> „(…) die Nutzer, die mit IT zu tun haben, haben ein großes Bewusstsein dafür. (…) Die, die reine Anwender sind vom Dienst, also die nicht von der IT her kommen, denen ist das im Grunde erstmal egal, Hauptsache es funktioniert. (…) wenn man neue Verfahren einführt (…) dann kricht man richtig Gegenwind. (…) Die ganz normale Problematik, also sie dürfen nicht gestört werden in dem was sie eigentlich tun wollen“ (Universität Siegen, Anhang A2).

> „Ist noch nicht so weit, dass man sagen würde jedem wäre bewusst, was man mit dem Benutzernamen und dem dazugehörigen Passwort alles anrichten kann. Ich denke das Bewusstsein ist noch nicht wirklich da“ (Mennekes, Anhang A5).

Daneben sei jedoch gemäß der Aussage eines weiteren Befragten ein gewisses Engagement mancher Nutzer zu beobachten, die sich mehr und mehr als Glied des Unternehmens sehen und ihren Teil zum Erhalt ihres Arbeitsplatzes beitragen möchten. Dies wird laut eines Experten durch den hohen medialen Einfluss sowie die globale Berichterstattung beschleunigt:

> „(...) aber einfach vom Bewusstsein, ich habe hier einen Platz in der Firma und der Platz der soll also tunlichst nicht ins Chaos abgleiten. (…) Ich denke da ist schon ein allgemeines Verständnis und auch ein Commitment in der Richtung zu beobachten“ (DEW, Anhang A3).

> „Nein, also das ist halt auch glaube ich durch die ganzen Medien, die ganzen Nachrichten, die in dieser Hinsicht kommen (…), das sensibilisiert schon die Leute, ganz klar“ (G.I.B, Anhang A4).

Zusammenfassend lassen die Befragungsergebnisse durchaus einen Anstieg des menschlichen Bewusstseins und Verantwortungsgefühls erkennen. Hierbei sei allerdings Potential nach oben vorhanden, wodurch die entsprechenden Verantwortlichen innerhalb der Organisationen angehalten sind, die Anwender entsprechend zu sensibilisieren und technische Hilfestellung zu leisten:

„Also da ist sicherlich noch Potential nach oben und da müssen wir als IT-Abteilung natürlich auch Hilfestellung geben (…). (…) und das halt auch so einfach wie möglich zu machen (…) und garnicht erst in Verlegenheit kommt (…) , sein Kennwort in einer Excel-Tabelle im Klartext abzulegen (…)“ (G.I.B, Anhang A4).

„Also früher war es noch lascher sag ich mal, mittlerweile hat man schon so ein kleineres Bewusstsein dafür gekriegt (…). (…) Das Bewusstsein ist jetzt schon da, dass diese Passwörter vielleicht schon komplexer sein müssen (…)“ (Mennekes, Anhang A5).

6.3.3 Schulungs- und Sensibiliserungsmaßnahmen

Laut den Meinungen der Experten muss das zuvor diskutierte Bewusstsein der beteiligten Nutzer vor allem durch geeignete Sensibiliserungs- und Schulungsmaßnahmen geschaffen oder gestärkt werden. Nur so lasse sich das notwendige Verständnis für die Verwendung bestimmter Technologien erzeugen:

„Und da muss ich ja ein Bewusstsein erstmal für schaffen, weil dann sonst kommt nämlich dann wieder die Frage, warum. (…) Und das durch Sensibilisierungs- und Schulungsmaßnahmen zu machen ist auf jeden Fall auf der Agenda, aber die Frage ist dann, wie.“ (Universität Siegen, Anhang A2).

Trotz dieser Ansichten werden in keiner der untersuchten Organisationen Maßnahmen mit Schulungscharakter durchgeführt. Hierzu äußerten die Befragten unterschiedliche Probleme und Bedenken. So sei es laut einem Experten schwierig, einen großen Bestand zu schulen, vor allem wenn die betroffenen Mitarbeiter bereits Jahre lang ihrer Arbeit nachgehen und nun an einschneidende Änderungen herangeführt werden sollen. Schulungen erfordern, so sagt der Experte, viele Ressourcen und personellen Einsatz, so dass Organisationen hierbei schnell an ihre Grenzen stoßen. Auch müssen die Maßnahmen längerfristig angesetzt werden, da sich neue Sachverhalte ergeben:

„Da stoßen wir nur organisatorisch und personell an Grenzen. (…) Aber nochmal, das ist ein organisatorisches Problem den Bestand zu schulen“ (Universität Siegen, Anhang A2).

„(…) aber es muss ja weiter gehen, weil die Sachen verändern sich ja“ (Universität Siegen, Anhang A2).

„Und dann kommt der und sagt was will der mir jetzt erzählen, seit zwanzig Jahren funktioniert das doch“ (Universität Siegen, Anhang A2).

Ein Ansatz wäre laut des Befragten, bereits beim Einstellungsprozess anzusetzen, da potentielle neue Mitarbeiter eine höhere Motivation aufweisen:

„Also da denke ich wäre der Ansatz erstmal, bei der Einstellung schon einzugreifen. (…) Denn neue Mitarbeiter sind immer offen für die Sachen (…), der ist, weil er ja auch hier arbeiten will, motiviert“ (Universität Siegen, Anhang A2).

Die übrigen Interviewpartner geben gemeinhin an, lediglich schulungsähnliche Unterweisungen direkt am Arbeitsplatz des jeweiligen Mitarbeiters zu unternehmen, sobald dieser eine entsprechende Frage stellt oder ein sicherkritisches Ereignis, beispielsweise in Form eines Virenbefalls, aufgetreten ist. Die Bemühungen sind also dahingehend generell ereignisgesteuert:

„Wir machen das immer so am Arbeitsplatz des Kollegen. (…) Also da versuchen wir dann direkt im direkten Kontakt mit dem Kollegen zu sensibilisieren (…). (…) Das ist aber nicht wirklich irgendwo mit einem Konzept dahinter, das machen wir dann (…) meistens wenn wir feststellen oh da hat wieder ein Kollege sein Kennwort irgendwo im Klartext abgelegt“ (G.I.B, Anhang A4).

„Und so lange nichts Schlimmes passiert sieht man vielleicht auch nicht unmittelbar den Bedarf dafür“ (DEW, Anhang A3).

„Also Schulungen IT-sicherheitstechnisch erfolgen dann, wenn der Mitarbeiter vielleicht eine passende Frage an den Supportler stellt, der gerade bei ihm am Rechner steht. Aber eine generelle Schulung für alle Mitarbeiter ist nie gemacht worden und ich weiß nicht ob es geplant ist“ (Mennekes, Anhang A5).

Weiterhin geben die Experten an, die sicherheitsrelevanten Interaktionen der Nutzer im Hinblick auf Authentifizierung seien nur sehr gering, ein Bedarf wird häufig nicht gesehen. Auch die

vermeintlichen Kenntnisse der Anwender in Sachen IT und Technik halten oft von einer groß angesetzten Schulung ab:

> „Weil die wenigen Schritte, die der Benutzer durchführen muss und die wenigen Regeln, die er beachten muss, die sind relativ schnell erklärt. Zumal sie sich ja auch über die Systemgrenzen einheitlich fortsetzen“ (DEW, Anhang A3).

> „Das heißt wo wir in der Vergangenheit auch den Bedarf nicht hatten großartig was aus unserer IT-Abteilung zu verteilen, irgendwelche Restriktionen, weil wir eben viele Kollegen haben die auch selber IT-Spezialisten sind“ (G.I.B, Anhang A4).

Nichtsdestotrotz sehen alle Befragten den steigenden Bedarf an Schulungs- und Sensibiliserungsmaßnahmen. Zum einen sorge die anhaltende Fluktuation innerhalb der Mitarbeiterschaft für die Notwendigkeit, einen einheitlichen Wissensstand unter den Kollegen zu schaffen. Zum anderen können Schulungen laut einem Experten vor allem dann notwendig werden, sobald neue Technologien beispielsweise in Form von Zertifikaten eingeführt werden, die ein gewisses technisches Verständnis erfordern, um erfolgreich eingesetzt werden zu können. Auch sei es immer sinnvoller, für den Umgang mit Daten und Informationen zu sensibilisieren, da diese im Laufe der Zeit immer kritischer werden:

> „Zum Einen gibt es da eine Fluktuation innerhalb der Mitarbeiterschaft, manche Leute scheiden aus, da kommen neue nach. So dass da auch vielleicht (…), um einen einheitlichen Stand zu schaffen durchaus von Zeit zu Zeit solche Schulungen sinnvoll sind“ (DEW, Anhang A3).

> „Aber ich denke es wird eher dann ein Thema werden, wenn wir hier sei es mit Zertifikaten, Zukunftsmusik, oder sei es mit strikteren Passwortregeln hier vielleicht neue Richtlinien schaffen, wo dann die Leute auch das entsprechende Verständnis für haben müssen“ (Mennekes, Anhang A5).

6.4 Zusammenfassung der Untersuchungsergebnisse

Die nachfolgenden Tabellen fassen die Ergebnisse der Interviews zusammen.
Auf den horizontalen Achsen sind die vier untersuchten Organisationen aufgetragen. Hierbei wird die Universität Siegen mit **O1** bezeichnet, die beiden Industrieunternehmen Deutsche Edelstahlwerke und Mennekes mit **O2** und **O3** und das Dienstleistungsunternehmen G.I.B mit **O4**.
Auf den vertikalen Achsen befinden sich die Themenbereiche sowie die Forschungsfragen der Interviews. Zudem beinhaltet Tabelle 2 die beiden Punkte Single-Sign-On (SSO) und Mehr-Faktor-Authentifikation (MFA), die sich aus den Gesprächen mit den Experten ergeben haben.
Die Einträge in den Tabellen zeigen die aktuellen Situationen der befragten Organisationen, welche durch die entsprechenden Experten angegeben werden. Hierbei wird zwischen drei Stufen unterschieden:

+ Die angesprochene Thematik trifft auf die Organisation zu (grün hinterlegt),
+/- trifft teilweise zu (gelb hinterlegt) oder
- trifft nicht zu (rot hinterlegt).

Tabelle 1 beinhaltet die Ergebnisse des ersten Themenkomplexes, in dem die aktuelle Situation in den Organisationen untersucht wird:

	O1 Univ.	O2 Indus.	O3 Indus.	O4 DL
Komplex 1: Aktuelle Situation				
Vielfalt der eingesetzten Techniken	+	-	+/-	+/-
Zufriedenheit der Experten	-	+/-	-	+/-
Vorgaben und Regelungen	k.A.	+/-	-	-
Handlungsbedarf	-	+/-	-	-

Tabelle 1: Themenkomplex 1: Aktuelle Situation

Tabelle 2 umfasst die Befragungsergebnisse des zweiten Themenbereiches. Dieser beinhaltet den möglichen Einsatz neuer Technologien:

		O1 Univ.	O2 Indus.	O3 Indus.	O4 DL
Komplex 2: Einsatz neuer Techniken					
Planung neuer Verfahren	Allgemein	+	-	+/-	+/-
	Zertifikate	+/-	-	+	+
	SSO	+	-	+	+
	MFA	+/-	-	+/-	+/-
Einsatz von WOT		+/-	-	-	-

Tabelle 2: Themenkomplex 2: Einsatz neuer Techniken

Die Ergebnisse des Themenbereiches der menschlichen Komponente im Authentifikationsprozess werden in Tabelle 3 aufgezeigt:

		O1 Univ.	O2 Indus.	O3 Indus.	O4 DL
Komplex 3: Menschliche Komponente					
Usability	IST	-	+/-	-	-
	Bedarf	+/-	+/-	-	-
Nutzerverhalten und Probleme		-	+/-	-	-
Bewusstsein der Anwender		-	+/-	-	+/-
Schulungs- und Sensibilisierungs-maßnahmen	IST	-	-	-	-
	Planung	-	-	-	-
	Bedarf	-	+/-	-	-

Tabelle 3: Themenkomplex 3: Menschliche Komponente

7 Schlussbetrachtung und Ausblick

Im Hinblick auf die einleitende Zielsetzung dieser Bachelorthesis bringen die Ergebnisse und Auswertungen der durchgeführten Interviews sowie ihre Deutung und Diskussion meines Erachtens wichtige Erkenntnisse hervor.

Führt man sich die aktuelle Notwendigkeit ausgewählter und durchdachter Authentifikations- und Identifikationsverfahren in Zeiten der Globalisierung und damit einhergehedem, steigenden Wettbewerbsdruck vor Augen, so wird aus den in Kapitel 6 genannten Aussagen deutlich, dass die vier untersuchten Unternehmen beziehungsweise Institutionen stellvertretend signifikante Mängel und Optimierungsbedarfe aufweisen.

So ist das Verfahren unter Nutzung von Nutzerkennungen und Passwörtern immer noch das am häufigsten eingesetzte Mittel zur Nutzerauthentifizierung. Es hat sich laut den Experten über die Zeit bewährt, weshalb eine allgemeine Zufriedenheit zu beobachten ist. Dem Beibehalten gängiger Methoden liegt unter anderem die Vereinfachung und Effizienz dieses Verfahrens zugrunde. Zudem halten hohe Kosten die Verantwortlichen oft davon ab, neue Anschaffungen in diesem Bereich zu tätigen. Die Befragten schätzen außerdem die verwalteten und internen Daten und Informationen als wenig kritisch ein, der Bedarf einer gezielten und intensiveren Auseinandersetzung mit dem Thema wird häufig nicht gesehen, was besonders unter Berücksichtigung des internationalen Handels und Kooperierens der untersuchten Organisationen fragwürdig ist. So ist es meines Erachtens wichtiger denn je, der steigenden Gefahr eines Angriffs entgegen zu wirken. Dies spiegelt sich auch darin wieder, dass die Unternehmen oft kaum interne Vorgaben, Standards und Regelungen bezüglich der Umsetzung und der Qualität der einzusetzenden Technologien aufweisen. Wider meiner Erwartungen erwähnt keiner der Experten die Verwendung anerkannter Standards wie etwa die Grundschutzkataloge des BSI oder die ISO/IEC 27000-Gruppe. So ist die sicherheitstechnische Infrastruktur häufig historisch gewachsen und unübersichtlich, Maßnahmen dahingehend werden nur dann eingeleitet, wenn ein Bedarf durch ein konkretes, im schlimmsten Falle negatives Ereignis offenkundig wird. In einem solchen Szenario leitet die zuständige Abteilung kurzfristige Anpassungen ein, die keines Legitimierungsprozesses bedürfen, was einen gewissen Ermessensspielraum deutlich werden lässt. Dies erkennen auch die Experten und äußern hierzu ein Maß an Optimierungsbedarf. Diesen Defiziten lässt sich meiner Meinung nach leicht mit Hilfe der bereits erwähnten Standards und Normen des BSI beziehungsweise der International Organization for Standardization entgegenwirken, da sie klare Handlungsanweisungen aussprechen. Die Möglichkeit der Zertifizierung bietet zusätzlich ein geeignetes Mittel zur Bewerbung des eigenen

Unternehmens und kann zur Kundenakquirierung beitragen.

Während die infrastrukturellen Aspekte der Untersuchung in Form der jeweiligen IT-Landschaften und Vorgehensweisen zwar verbesserungswürdig aber auch als den Anforderungen und Aufgaben angemessen betrachtet werden, lassen die Befragungen die menschliche Komponente im Authentifizierungsprozess als besonders kritisch erkennen. Dies wird vor allem durch Tabelle 3 im vorangegangenen Kapitel deutlich, welche eine deutlich negative Tendenz aufweist. Laut den Experten liegt hier die größte Schwachstelle vor, gehen doch viele Nutzer sorglos und nachlässig mit der Vertraulichkeit und Sicherheit angewandter Verfahren um. Zwar hat der fachliche Sachverstand dahingehend zugenommen, dennoch ist das Bewusstsein der Nutzer nur wenig ausgeprägt. Dies gilt laut den Interviewpartnern vor allem für die steigende Anzahl der reinen Anwender, also derer ohne signifikantes Technikwissen. So weisen diese häufig kein großes Interesse an der Sicherheit von IT-Systemen und Anwendungen auf, sie priorisieren die Einfachheit der Verfahren und die ungestörte Ausführung ihrer alltäglichen Arbeit. Zwar gibt es gemäß den Befragungsergebnissen auch Ausnahmen, die ein gesteigertes Engagement der Mitarbeiterschaft erkennen lässt, jedoch wird dies vordergründig durch sicherheitskritische Ereignisse ausgelöst, die negative Auswirkungen auf das Unternehmen und den Betrieb haben.

Diese Punkte zeigen auf, dass die Sensibiliserung und Schulung der Mitarbeiter und Anwender notwendig ist, um das oft nicht vorhandene Bewusstsein und Verständnis für neue Technologien und Anpassungen zu schaffen. Die Aussagen der Experten sprechen hierzu eine deutliche Sprache. So führt keine der untersuchten Organisationen Maßnahmen in diese Richtung durch geschweige denn verfügt über ein Konzept, das eine gewisse Regelmäßigkeit und planmäßige Durchführung von Schulungen vorsieht. Durchgeführte Schritte mit Schulungscharakter belaufen sich lediglich auf kleinere, persönliche Unterweisungen am Arbeitsplatz des betroffenen Kollegen. Dies geschieht auch nur dann, wenn ein entsprechendes Ereignis oder eine Frage auf einen Missstand hinweist. Aus den genannten Gegebenheiten kann daher abgeleitet werden, dass die nutzerzentrierte Auseinandersetzung mit dem Thema Authentifikation und auch anderweitiger Verfahren der IT-Sicherheit für die Zukunft meiner Meinung nach im Vordergrund stehen sollte. Durch die Ausrichtung der verwendeten beziehungsweise geplanten Techniken und Prozeduren auf die Akzeptanz und den fachlichen Wissensstand der letztendlichen Anwender lassen sich viele der kritisierten und optimierungsbedürftigen Punkte beheben oder zumindest entkräften. So gilt es wie bereits in Kapitel 6 erwähnt laut den Experten, die Balance zwischen Bedienbarkeit, Anwenderfreundlichkeit und erreichter beziehungsweise notwendiger Sicherheit herzustellen, was letztendlich die IT-Landschaft transparenter macht, Fehlern bei der Nutzung von Technologien vorbeugt und somit den Alltag der Nutzer erleichtert.

Hierzu werden anhand der verschiedenen Befragungsergebnisse und bei Betrachtung des entsprechenden Themenbereiches in Tabelle 2 bereits erste Bestrebungen ersichtlich. So geben die Experten bei der Frage nach dem ihrer Meinung nach idealen Zustand beziehungsweise ihren Vorstellungen bezüglich neuer Technologien neben dem Einsatz von Zertifikaten ihren Wunsch nach einer Vereinheitlichung der zum Einsatz kommenden Authentifikationsmechanismen an. Hierbei spielt vordergründig das Prinzip des Single-Sign-On eine Rolle, mit Hilfe dessen es den Zuständigen gelingt, die mutliplen Identitäten und Zugänge in Form eines zentralen Zugangs zu vereinen. Dies führt in meinen Augen letztendlich zu einer gesteigerten Akzeptanz der Nutzer sowie der Erleichterung alltäglicher Arbeiten bei einem gleichzeitig hohen Sicherheitsniveau dank moderner Technologien, was den Anforderungen einer vernetzten und globalisierten Weltwirtschaft in gesteigertem Maße entspricht.

8 Literaturverzeichnis

BERNAUER, Matthias (2006): Benutzbare Benutzerauthentifizierung: Security and Usability of Passwords, unter http://uni.matthias-bernauer.com/~bernauer/usability_of_passwords/ [Stand: 04.01.2014]

BUNDESAMT für Sicherheit in der Informationstechnik (2008a): *IT-Grundschutz-Standards*, unter https://www.bsi.bund.de/DE/Themen/ITGrundschutz/ITGrundschutzStandards/ITGrundschutzStandards_node.html#doc471418bodyText1 [Stand: 04.02.2015]

BUNDESAMT für Sicherheit in der Informationstechnik (2008b): *BSI-Standard 100-1: Managementsysteme für Informationssicherheit (ISMS)*, unter https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Publikationen/ITGrundschutzstandards/standard_1001_pdf.pdf?__blob=publicationFile [Stand: 04.02.2015]

BUNDESAMT für Sicherheit in der Informationstechnik (2008c): *BSI-Standard 100-2: IT-Grundschutz-Vorgehensweise,* unter https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Publikationen/ITGrundschutzstandards/standard_1002_pdf.pdf?__blob=publicationFile [Stand: 04.02.2015]

BUNDESAMT für Sicherheit in der Informationstechnik (2008d): *BSI-Standard 100-3: Risikoanalyse auf der Basis von IT-Grundschutz,* unter https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Publikationen/ITGrundschutzstandards/standard_1003_pdf.pdf?__blob=publicationFile [Stand: 04.02.2015]

BUNDESAMT für Sicherheit in der Informationstechnik (2008e): *BSI-Standard 100-4: Notfallmanagement,* unter https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Publikationen/ITGrundschutzstandards/standard_1004_pdf.pdf?__blob=publicationFile [Stand: 04.02.2015]

BUNDESAMT für Sicherheit in der Informationstechnik (2013): *IT-Grundschutz-Kataloge,* unter https://www.bsi.bund.de/DE/Themen/ITGrundschutz/ITGrundschutzKataloge/itgrundschutzkataloge_node.html [Stand: 04.02.2015]

BUNDESAMT für Sicherheit in der Informationstechnik (2014): *ISO 27001 Zertifizierung auf Basis von IT-Grundschutz*, unter https://www.bsi.bund.de/DE/Themen/ZertifizierungundAnerkennung/Zertifizierung27001/GS_Zertifizierung_node.html [Stand: 04.02.2015]

DEUTSCHE Edelstahlwerke (2014a): *Willkommen bei der DEUTSCHEN EDELSTAHLWERKE GmbH*, unter http://www.dew-stahl.com/home/ [Stand: 23.12.2014]

DEUTSCHE Edelstahlwerke (2014b): *Flexible Edelstahllösungen aus einer Hand*, unter http://www.dew-stahl.com/unternehmen/ [Stand: 23.12.2014]

ECKERT, Claudia (2013): *IT-Sicherheit: Konzepte – Verfahren – Protokolle*, 8. Aufl., Oldenbourg Verlag München.

FRIEBERTSHÄUSER, Barbara (1997): *Interviewtechniken – ein Überblick*, in: Friebertshäuser, Barbara; Prengel, Annedore (Hg.): *Handbuch qualitative Forschungsmethoden in der Erziehungswissenschaft*, 1. Aufl., Juventa Verlag Weinheim/München.

FRITZSCHE, Kathleen (2014): *Digitales Zeitalter: Wie das Internet unsere Identität beeinflusst und verändert*, unter http://netzwertig.com/2014/07/17/internet-unsere-identitaet/ [Stand: 30.12.2014]

GESELLSCHAFT für Information und Bildung (2014): *Die G.I.B, Gesellschaft für Information und Bildung mbH, ist ein mittelständisches Unternehmen der IT Branche mit Sitz in Siegen*, unter http://www.gibmbh.de/_ueber-gib_ [Stand: 23.12.2014]

GRIESER, Franz (2008): *Bye bye Passwort-Authentifizierung und -Authentisierung: Biometrie, Token, Smartcards und digitale Zertifikate im Überblick*, unter http://www.security-insider.de/themenbereiche/identity-und-access-management/authentifizierung/articles/65263/index2.html [Stand: 19.01.2015]

HELFFERICH, Cornelia (2011): *Die Qualität qualitativer Daten. Manual für die Durchführung qualitativer Interviews*, 4. Aufl., VS Verlag für Sozialwissenschaften Wiesbaden.

LÜKE, Gabriele (2013): *Industriespionage – Spionageopfer Mittelstand*, unter https://www.muenchen.ihk.de/de/WirUeberUns/Publikationen/Magazin-wirtschaft-/Aktuelle-Ausgabe-und-Archiv2/magazin-02-2013/Titelthema/industriespionage-spionageopfer-mittelstand [Stand: 25.02.2015]

MAYER, Horst Otto (2009): *Interview und schriftliche Befragung. Entwicklung Durchführung Auswertung*, 5. Aufl., Oldenbourg Verlag München.

MENNEKES (2014): *MENNEKES - Plugs for the world*, unter http://www.mennekes.de/index.php?id=mennekes [Stand: 23.12.2014]

MEUSER, Michael; Nagel, Ulrike (1991): *Experteninterviews – vielfach erprobt, wenig bedacht. Ein Beitrag zur qualitativen Methodendiskussion*, in: GARZ, Detlef; Kraimer, Klaus (Hg.): *Qualitativ-empirische Sozialforschung*, 1. Aufl., Westdeutscher Verlag Opladen.

MEUSER, Michael; Nagel, Ulrike (1997): *Das Experteninterview - Wissenssoziologische Voraussetzungen und methodische Durchführung*, in: Friebertshäuser, Barbara; Prengel, Annedore (Hg.): *Handbuch qualitative Forschungsmethoden in der Erziehungswissenschaft*, 1. Aufl., Juventa Verlag Weinheim/München.

MEYERS, Mike; Harris, Shon (2007): *CISSP – Certified Information Systems Security Professional*, 2. Aufl., Redline Verlag Heidelberg.

MOORE, Robert (2010): *Cybercrime – Investigating High-Technology Computer Crime*, 2. Auflage, Routledge Verlag Abingdon.

MÜHLFELD, Claus; Windolf, Paul; Lampert, Norbert; Krüger, Heidi (1981): *Auswertungsprobleme offener Interviews*, in: Soziale Welt, Jg. 32.

MÜLLER, Klaus-Rainer (2011): *IT-Sicherheit mit System: Integratives IT-Sicherheits-, Kontinuitäts- und Risikomanagement – Sicherheitspyramide – Standards und Practices – SOA und Softwareentwicklung*, 4. Aufl., Vieweg+Teubner Verlag Wiesbaden.

PSMAIL (2010): *Software Token: What is a software token and how do I use it?*, unter https://info.psmail.net/noah/faq-top-link/psmailbox-questions/164-software-token.html [Stand: 19.01.2015]

SCHMEH, Klaus (2007): *Kryptographie: Verfahren, Protokolle, Infrastrukturen*, 3. Aufl., dpunkt.verlag Heidelberg.

SCHMOLZ + BICKENBACH (2014a): *Konzernstruktur*, unter http://www1.schmolz-bickenbach.com/konzern/konzernstruktur/ [Stand: 23.12.2014]

TSOLKAS, Alexander; Schmidt, Klaus (2010): *Rollen und Berechtigungskonzepte: Ansätze für das Identity- und Acess Management im Unternehmen*, 1. Aufl., Vieweg+Teubner Verlag Wiesbaden.

UNIVERSITÄT Siegen (2014a): *Universität Siegen*, unter http://www.uni-siegen.de/start/die_universitaet/?lang=de [Stand: 22.12.2014]

UNIVERSITÄT Siegen (2014b): *Organigramm*, unter http://www.uni-siegen.de/start/die_universitaet/organisation/?lang=de [Stand: 22.12.2014]

UNIVERSITÄT Siegen (2014c): *Zahlen und Daten*, unter http://www.uni-siegen.de/start/die_universitaet/ueber_uns/daten/?lang=de [Stand: 22.12.2014]

WARDEN, Waheed (2004): *Strong Authentication Alternatives Report For Customer X*, unter http://archive.securitypronews.com/2004/0121.html [Stand: 19.01.2015]

WITT, Bernhard C. (2006): *IT-Sicherheit kompakt und verständlich: Eine praxisorientierte Einführung*, 1. Aufl., Friedr. Vieweg & Sohn Verlag Wiesbaden.

9 Anhang

A1 Interviewleitfaden

Interviewleitfaden – Empirie - Bachelorthesis Marius Müller

Name: _____ **Organisation**: _____

Leitfrage	Check	Konkrete Fragen
TEIL I		
In welchen Bereichen kommt Authentifikation in Ihrer Organisation zum Einsatz und welche Technologien werden hierbei verwendet? (intern und extern)	☐ Anforderungen, ☐ Zufriedenheit, ☐ Notwendige Credentials, ☐ Gültigkeit der Credentials, ☐ Lücken, ☐ Vorgaben, ☐ Unterschiede je nach Bereich	☐ Wo tritt implizite Authentifizierung auf? ☐ Wie sähe eine optimale Lösung aus? ☐ Gedenken Sie, weitere Technologien einzusetzen? Welche? ☐ Wo ist Authentifizierung nicht notwendig?
	☐ **Mögl. Einsatzbereiche für gegenseitige Authentifizierung/Vertrauen, flexibles, spontanes Authentifizieren**	☐ **Könnten Sie sich vorstellen, an Stelle der herkömmlichen Mechanismen ein Netz einzurichten, in dem sich Teilnehmer gegenseitig ihre Identität bescheinigen?** ☐ **Wer dürfte wessen Authentizität bescheinigen?**
TEIL II		
Wo kommen Nutzer mit den eingesetzten Technologien in Berührung? Wie gestaltet sich die Bedienbarkeit?	☐ Probleme bei Nutzung, ☐ Bewusstsein der Nutzer	☐ Gibt es Abkürzungen im System? ☐ Oder ist das System „zu gut“?
	☐ **Schulungsmaßnahmen**	☐ **Was wurde vollzogen? Warum?** ☐ **Was ist geplant?** ☐ **Wo besteht Bedarf?** ☐ **Was wurde doch nicht umgesetzt?** ☐ **Warum nicht?**

A2

Interviewtranskript – Universität Siegen – 11.11.2014

I: So, Test Test, schlägt aus, gut. Alles klar. So, Herr Hoffmann, dann fange ich einfach mal an und zwar einfach mal einleitend die Frage, wo hier in der Universität Siegen Authentifikation, also Mechanismen zur Authentifikation, eingesetzt wird und wie das Ganze umgesetzt wird, also welche Technologien da zum Einsatz kommen.

B: Ja, wo ist nahezu überall. Wir haben verschiedene Systeme, also ob es jetzt im Web ist, dass wir uns da authentifizieren müssen, bezüglich jetzt Benutzername Passwort. Ist immernoch die Herkömmliche. Interessant jetzt vielleicht auch in dem Zuge ist jetzt die aktuelle Entwicklung, dass die Uni Siegen ein zentrales Identity Management aufbauen will. Also das Problem, was wir hier an der Uni haben, wir haben viele verschiedene Systeme. Also HIS haben wir, dann haben wir noch ALEF, also Uni Bibliothek und so weiter und sofort und überall muss ich mich ja anmelden. Jetzt ist das Problem, dass die alle ihren eigenen Datenbestand haben. Das heißt ich habe mehrere digitale Identitäten, zum Beispiel als Student, nehmen wir das Beispiel mal. Und das ist insofern ein Problem, weil sich diese ganze Struktur dahingehend entwickelt, wir haben eine Förderation, also das Deutsche Forschungsnetzwerk, und es gibt NRW weit Systeme die eben bedingen, dass ich mich an allen Unis, wie es bei Eduroam zum Beispiel ist, anmelden kann und kann mich also mit meinem Account, den ich jetzt hier habe, mich in Duisburg Essen anmelden im Eduroam. Das heißt ich brauch da keine digitale (...), ich habe nur eine, die ist in Siegen. Und die wird eben entsprechend, ... auch Shibboleth zum Beispiel als Protokoll, dass eben die entsprechende Authentifizierung dann eben statt findet. Und da gehts jetzt auch weiter, dass die Dienste, also Service, verteilt werden dahingehend, zum Beispiel für die Lehramtstudenten ist das Praktikumsplatzvergabe. Und da mussten wir jetzt als Uni Siegen auch dann irgendwie mal aktiv werden, weil wir mussten als eine Identität, als Identitätsprovider auftreten hier, da müssen wir so ein, IDP heißt das, eben erstellen und der allerdings erwartet wieder eine zentrale Identitätsdatenbank, also ein zentrales Identitätsmanagement. Und die gabs nicht. Das heißt also, um jetzt nochmal Authentifikation, Benutzername Passwort ist jetzt immernoch das Stichwort, aber es gibt auch viele andere. Beispielsweise die Uni Bib hat diesen Ausweis wo so ein Barcode drauf ist. Die werden jetzt so einen Kassenautomaten einrichten, wo ich jetzt Gebührenvorgänge selbst dann bezahlen kann, mit Kreditkarte. Und da authentifizier ich mich einfach nur mit der Karte. Das heißt also mit dem Ausweis, mit dem Barcode, also kein Passwort mehr dazu. (Unterbrechung) Also nochmal wegen der Authentifzierung, wir haben bei der Bib, dass die also die Möglichkeit haben jetzt ohne Benutzername Passwort, das heißt ich authentifiziere mich quasi nur mit der Karte und dem Barcode. Genau, also wir haben noch weitere, um jetzt weiter ins Detail zu gehen. Zum Beispiel - das ist aber nicht oder noch nicht die Regel - das ist wenn wir uns über SSH authentifizieren auf dem Server. Und da, SSH okay, aber plus Public Key Authentifizierung. Das heißt also wir, die Studenten, generieren sich ein Schlüsselpaar selbst und authentifizieren sich dann eben entsprechend gegenüber uns dann serverseitig, das ist diese von Herrn (anonym), um eben per SSH dann auf den Server zu kommen, von zu Hause aus oder was auch immer. Da ist es so, dass diese Schlüsselgenerierung wie gesagt selbst gemacht wird, es gibt keine zentrale Instanz erstmal dafür. Und das ist also noch so ein Thema mit dieser Public Key Authentifizierung, das ist also nicht flächendeckend. Das machen viele andere auch schon, aber das ist vom ZIMT auch so gewollt, weil dann können die das nämlich alles zu machen soweit und sie sind sicher, okay, das ist auch derjenige der drauf soll. Die andere Sache ist jetzt, kombinieren könnte man das, und alles was wir jetzt darüber reden, hat irgwendwann mit diesem zentralen Identity Management zu tun, irgendwann, das ist noch in der Mache halt. Aber was wir ja noch hier haben ist halt, dass ich mir ja auch ein Zertifikat ausstellen lassen kann. Das heißt ich gehe unten, ich fülle das aus, gehe zum

Herrn (anonym) und generiere mir die Schlüssel und habe dann eben auch entsprechend die Möglichkeit E-Mail zu signieren und zu verschlüsseln. Problem hier ist allerdings auch, das ist auch nur so eine einfache Kiste, weil es halt ein Softwarezertifikat ist. Das heißt diese Schlüssel werden nicht auf einer sogenannten sicheren Signaturerstellungseinheit wie einer Chipkarte beispielsweise gespeichert oder auch darauf generiert, was ja der Idealzustand dann ist, dass dieser geheime Schlüssel diese Karte nie verlässt. Das haben wir hier nicht. Aber auch da sind schon Bestrebungen im Gange, das auch jetzt für die Studierenden zum Beispiel hin zu einem elektronischen Studierendenausweis das Thema nochmal aufzugreifen, denn das Thema war schon vor - da war ich noch Student - langer Zeit mal aktiv und wurde dann vom ASTA abgelehnt. Und das hat jetzt verschiedene Gründe. Aber da ist wohl, das Bewusstsein hat sich dann doch wohl bei allen geändert und da ist wohl eine große Befürwortung. Ich meine wir rennen ja immernoch mit diesem Papierzettel durch die Gegend, wo andere Unis schon viel weiter sind.

I: Okay.Gut, Sie haben jetzt primär von den Studenten gesprochen, die sich authentifizieren. Gibt es da eventuell noch andere Gruppen oder noch andere, vielleicht auch Externe, die sich irgendwie authentifizieren müssen? Oder unter Mitarbeitern? Gibts da eventuell Unterschiede? Dass das intern sowie extern unterschieden wird?

B: Also bei Mitarbeitern, muss ich jetzt dazu sagen, zum Beispiel was in der Verwaltung läuft, jetz im Detail kann ich jetz nicht sagen. Ich weiß, dass Teile der Verwaltung auch eine Art Ausweis haben, in Anführungszeichen. Das heißt die haben eine Chipkarte schon, aber das sind nur eine Hand voll. Ob das die Dezernenten sind kann ich jetzt noch nicht mal mehr sagen, weil die Verwaltung ist ein eigener Part hier an der Uni. Als IT-Sicherheitsbeauftragter bin ich zwar auch für die zuständig, aber was da jetzt genau läuft kann ich jetzt nicht sagen. Grundsätzlich, deswegen konnte ich das mit den Studenten jetzt auch gut nehmen als Beispiel, unterscheiden wir uns als Mitarbeiter nicht groß von den Studierenden was die Möglichkeiten der Authentifizierung betrifft. Ich muss jetzt grad mal nachdenken. Also, wir haben die Kennung genauso wie die Studierenden auch und wir haben wie gesagt keine Chipkarten oder sonstige Sachen sondern wir haben einfach auch nur unser Benutzername Passwort. Genau wie bei E-Mail. Wir haben beide die Möglichkeit, uns ein Zertifikat zu holen zum Beispiel, das hat auch nix mit Student oder Mitarbeiter zu tun. Und, was ich wie gesagt nicht weiß ist, ob es noch irgendwelche alternativen Möglichkeiten innerhalb der Verwaltung, innerhalb der IT-Verfahren gibt, also dieser IT-Dienste, die die benutzen. Buchungssysteme, zum Beispiel. Wobei ich auch da weiß, dass das auch als Mitarbeiter über SAP läuft. Und SAP hat auch einfach nur das Benutzername Passwort Prinzip. Problem da im Moment, um die Problematik Benutzername Passwort allgemein jetzt als Authentifizierungsmethode zu sehen, haben wir bei SAP ganz krass, weil dort jeder Lehrstuhl nur der Lehrstuhlinhaber den Zugang bekommt. Das heißt der Lehrstuhlinhaber muss dann seine Kennung weiter geben an Mitarbeiter oder Sekretärin, damit die eben entsprechende Buchungen durchführen kann. Und das ist natürlich nicht im Sinne der Informationssicherheit. Der Grund liegt einfach daran, dass die Lizenzkosten explodieren würden, wenn jetzt jeder Lehrstuhl zwei oder drei dieser Zugänge für dieses SAP hätte. Das war ein Kostenfaktor. Da ist dann wieder das Problem, dann hat man eben darauf verzichtet und hat gesagt, dann musst du eben deinen Benutzernamen und dein Passwort weitergeben. Und das ist wieder die Problematik Benutzername Passwort.

I: Okay. Um einfach noch ein kleines Stichwort einzuwerfen, generell so die Zufriedenheit mit der aktuellen Situation. Also Sie haben jetzt erklärt, dass es da schon Bestrebungen gibt, in bestimmte andere Richtungen. Wie sieht da so die aktuelle Zufriedenheit aus mit den aktuellen Lösungen? Gibt es da irgendwo Dinge, wo Sie grundsätzlich sagen da sind Lücken, da müssen wir auf jeden Fall ran.

B: Ja, die eine habe ich grade genannt, die SAP Kiste ist eine ganz große, weil da gehts um Geld, also das ist ja jetzt nicht ein Zugang, wo ich dann nur, was weiß ich, ein Micky Maus Bild sehe, sondern da sehe ich ja wirklich meine ganzen Konten. Und ich kann buchen und das heißt also, das ist jetzt eher ein Problem. Ansonsten ist die Situation immer abhängig davon, wie die Schutzkategorie der Daten ist, die es betrifft. Also Benutzername Passwort ist ein gängiges, gut funktionierendes Mittel. Aber die Frage ist jetzt, was will ich denn, was verbirgt sich jetzt hinter dem Zugang? Also wenn ich jetzt sehe, wir haben ja noch, da müsste ich jetzt vielleicht selber mal nachfragen. Haben wir noch das TAN-Verfahren eigentlich? Bei der Anmeldung zu... ja? Gibts das noch? Gut. Denn das sehe ich, diese Kombination, relativ kritisch, weil sie nicht besonders benutzerfreundlich ist im Endeffekt. Das heißt ich kann nur diese Transaktion, auch wenn ich einen Bogen hab, dann muss ich mir einen neuen besorgen. Das ist nicht mehr zeitgemäß, meiner Meinung nach. Da gibts auch weitaus bessere Methoden. Allerdings ist man da wieder gebunden an diese HIS GmbH, die eben das System zur Verfügung stellt. Geht man zu denen hin, sagt, wir wollen ein anderes System, dann kommen die mit einer großen Summe an und dann machen die das. Und da gehts wieder darum, ja, es gibt Sachen, die kann man besser machen, aber die kosten soviel Geld, dass man sagt, das macht keinen Sinn. Ja, es ist so. Und das ist immer der Kompromiss, den man in der IT-Sicherheit irgwendwann schließen muss. Zwischen Finanzierbarkeit, Benutzbarkeit und macht es dann überhaupt Sinn, wie groß die Paranoia dann bei den ein oder anderen ist. Grundsätzlich, um jetzt nochmal auf die Frage allgemein zurück zu kommen, ist man schon zufrieden so wie es jetzt ist. Allerdings ist Benutzername Passwort prinzipiell immer nur das einfachste Mittel und nicht das beste. Aber wenn man keine anderen Möglichkeiten eben hat, muss man eben darauf zurückgreifen. Denn das Problem bei Benutzername Passwort - das müsste man jetzt mit dem ZIMT abklären, zum Beispiel mit dem Herrn (anonym) unten im Benutzerservice - bei großen Firmen ist es so, die haben enorme Kosten bei Benutzername Passwort Authentifizierung, wenn es um das Vergessen von Passwörtern geht. Die müssen zurückgesetzt werden. Es gibt einen Mechanismus gegebenenfalls oder aber, wenn ich sagen will ich habe da jemanden, der vergibt sich ein neues Passwort und ich hab dann nachher fünf oder sechs und dann weiß ich nicht mehr, welches es ist. Ich geb es dreimal falsch ein, dann ist es gesperrt. Dann muss ich es wieder freisetzen. Und diese Kosten sind für innerhalb der Industrie enorm. Wie es an der Uni Siegen ist ist natürlich jetzt so eine Sache, aber auch da rennen die Leute runter und sagen, ich habe meine Passwort vergessen. Ich kann nicht meine E-Mails mehr lesen oder nicht ins HIS und so weiter und sofort, LSF. Was mach ich denn jetzt? Ja, gehe dann dahin und der Herr (anonym) sitzt dann da und versucht dem ein neues Passwort zu geben. Ich sage jetzt mal, das ist halt der Aufwand, der dahinter steckt. Aber nochmal, prinzipiell ist immer, was will ich damit schützen und so ist die Situation okay, vor allen Dingen auch dahingehend, weil sie sich ja ändert. Es wäre immer problematisch, wenn man diesen Zustand erhalten will. Man kann ihn nicht mehr erhalten, weil wir gezwungen sind eben diesen Identity Provider zur Verfügung zu stellen. Dazu brauchen wir ein zentrales Identity Management. Da ist nur die Diskussion, hat jetzt mit der Authentifizierung nix zu tun, aber wie kommen denn diese Daten zusammen von HIS, von ALEF, von diesen ganzen Systemen. Wie kommen die zusammen in ein zentrales Identity Management. Und das ist so ein bisschen noch eine Krücke da, das erfolgt über einen Export mit CSV Dateien, nachts automatisiert, und dann wieder ein Import in diese IDM halt. Und tja, das ist jetzt nicht so schön eigentlich. Aber es ist eine Möglichkeit, um eben wie gesagt eine zentrale Identität eben entsprechend zur Verfügung zu stellen.

I: Okay, also davon ausgehend, was Sie jetz gesagt haben, frage ich Sie einfach, wie Sie sich jetzt spontan eine optimale Lösung der ganzen Geschichte vorstellen könnten. So aus dem Stand. Also ist es jetzt das, was was Sie gerade am aufbauen sind oder gäbe es da eventuell noch was wo Sie sagen würden, das wäre das Non-Plus-Ultra in dem Fall?

B: Das Non-Plus-Ultra...

I: Oder..

B: Ist immer schwierig. Das ist immer, ist immer Sache, wie also sagen wir zum jetzigen Zeitpunkt. So muss man das ja meinen man kann ja nicht sagen für hundert Jahre hält das

I: Klar.

B: Ich war immer ein Freund halt der von elektronischen Ausweisen. Ganz klar. Und und auch von biometrischen Merkmalen, also

I: Mhm

B: das ich mich authentifiziere und wenn es der Daumen ist oder der Finger, zum Beispiel, die Technologie hat sich dahingehend sehr gut entwickelt und auch, also sie ist halt robust geworden und das ist halt entscheidend. Auch ich, wir hantieren hier mit verschiedenen Schlüsseln für die Tür, beispielsweise für diese Tür hab ich einen anderen Schlüssel wie für mein Büro, habe ich einen anderen Schlüssel wie für im Labor, da habe ich eine Chipkarte, also ich habe drei verschiedene Sachen um eben überhaupt jetzt Infrastruktur hier zu benutzen, auch hier wäre die Möglichkeit eben das eben zu zentralisieren, nur über Chipkarte oder über einen Chip, der NFC oder RFID je nachdem dann in einer Chipkarte zu Hause ist. Die Idee dahinter wäre wie gesagt, dass ich einfach nur mich authentifiziere, ein komplettes Single Sign On, ein richtiges Single Sign On, mit einer Karte und einer Pin

I: Mmh.

B: Also kein Passwort mehr für UB, kein Passwort mehr, was ja immer noch ist, ich muss ja, also zumindest für Mitarbeiter, also ich muss mich da mit der UB-Nummer und hab da ein eigenes Passwort, ich hab also nich die G-Kennung zum Beispiel, da hab ich die G-Kennung für meine Emails und sonstige Sachen, ja und wie gesagt also da würde ich mir wünschen, das wäre für mich so der Idealzustand.

I: Mhm.

B: Dann hab ich die Zweifaktorauthentifizierung halt mit Besitz und Wissen und gegebenenfalls noch mit einem biometrischen Merkmal anstelle der Pin, ja zum Beispiel

I: Mhm.

B: Nur jetzt reden wir wieder über Geld. Damit das bewerkstelligt werden kann ist sehr viel Geld in die Hand zu nehmen. Das heißt also die Mitarbeiter müssen entsprechend ausgerüstet werden, dass sie eben auch eine Chipkarte einlesen können, also ein Lesegerät, entweder kontaktlos oder aber mit kontaktbehaftet halt und die Sachen sind sehr teuer.

I: Mhm.

B: Und dann die Studierenden natürlich auch. Sonst macht es keinen Sinn. Prinzipiell muss man wirklich dazu sagen, ich habe mit Kollegen auch aus der Industrie gesprochen, die gucken mich immer mitleidig an, weil an der Uni kann man oder in der Firma kann man eben die Sachen

bestimmen. Man sagt wir machen das jetzt. Wenn man das an der Uni macht, dann schreien wirklich tausend Stellen erst mal oh nein und das geht doch nicht ich fühl mich in meiner Freiheit von Forschung und Lehre bedroht. Das ist immer das große Thema und dem muss man dann immer Rechnung tragen, deswegen, das ist jetzt so ein Wunschdenken, mit dieser Chipkarte, da kommen wieder andere und sagen ich werde verfolgt weil ich kann dann gecrackt werden wann ich wo wie mich eingeloggt habe und so weiter und das ist halt ein riesen Prozess an einer Uni so etwas einzuführen. Das muss sehr gut überlegt sein. Aber die Frage war ja, was ich mir wünschen würde. Wir haben kurz vor Weihnachten, also, das würde ich mir wünschen.

I: Okay. Darauf jetzt mal aufbauend einfach alternativ mal zu der Sache: Könnten Sie sich vorstellen, statt jetzt den herkömmlichen Mechanismen, wie sie jetzt zum Einsatz kommen oder wie Sie sie ja auch geplant haben

B: Mhh.

I: eventuell so eine Art Netz aufzubauen, in dem sich Nutzer oder auch Mitarbeiter gegenseitig ihre Identität bestätigen oder verifizieren, so dass das nicht mehr zentral gesteuert ist sondern dass das ein

B: Ja

I: quasi ein

B: Ja

I: Prozess ist, in dem so flexibles spontanes Authentifizieren möglich ist.

B: Ja, ja. Da bewegen wir uns dann wieder hin, dass man sagt, also erst mal ja.

I: Mhm.

B: Weil ich bin ja auch Wissenschaftler und das ist natürlich immer eine Sache, man sagt okay, das hat was mit einem Experiment zu tun. Da sind ja zwei Sachen. Das eine ist ja, das kann ich mir vorstellen, vor allen Dingen auch weil es innerhalb so einem Mikrokosmos wie einer Hochschule funktionieren würde. Bin ich mir sicher.

I: Mhm.

B: Nutzen wäre da und Funktionsweise, also, es würde funktionieren. Die Frage ist nur wie gesagt, wie ich das eben gesagt habe, wenn wir uns jetzt dann müssen wir das ja wieder größer denken, denn die Uni an sich okay, aber wir arbeiten ja viel nach draußen, wie jetzt diese Vergabe von Praktikumsplätzen auch NRW-weit, das heißt ich muss ja sehen, wenn ich dann einen Nutzen haben will muss ich natürlich auch allen anderen Unis das Vertrauen schenken zum Beispiel und den Leuten, das heißt es ist ein komplettes Netz was entstehen müsste und dann ist die Frage gut okay ja. Ja da hab ich mit dem (anonym) schon mal länger drüber schwadroniert und das Thema, was da ist, ist immer der Mensch. Ja also es gibt irgendwann die Komponente Mensch, wir reden hier über digitale Identitäten und so weiter aber der Mensch ist ja irgendwann auch der Punkt. Ich muss jetzt Ihnen trauen, oder ich sage jawohl ich kenne ihn und ich bestätige auch die Identität und ich schätze Sie auch als vertrauenswürdig ein. Das kann ich aber nur dann, wenn ich den wirklich kenne. Jetzt geht es wieder los. Jetzt kennen Sie wieder jemanden oder vielleicht auch nur halb und der ist aber

nicht vertrauenswürdig und dann bin ich wieder in dieser Kette, dass ich dann auch sage, okay, dann will ich ihm dann aber auch vertrauen und ich will es aber nicht.

I: Mhm.

B: Also die Frage ist immer, wie es sozial funktioniert.

I: Mhm.

B: Das ist jetzt eine offene Frage. Ich weiß es nicht, kann man drüber diskutieren. Aber so ein, nochmal, wie gesagt auch aus wissenschaftlicher Sicht ist das immer interessant.

I: Mhm.

B: Was ich jetzt nicht weiß ist, ob es diese Bestrebung nicht schon an irgendwelchen Unis mal gegeben hat, das weiß ich jetzt wie gesagt nicht, und ob da nicht bereits Erkenntnisse sind, die dann dafür oder dagegen vielleicht sprechen. Ich weiß es nicht.

I: Mhm. Okay. Also könnten Sie sich da irgendwelche speziellen Gruppen vorstellen, die sich da gegenseitig authentifizieren oder mehr so allgemein?

B: Also Gruppen, wir haben, wie ich das eben schon sagte, wir haben zwanzigtausend Studenten, wir haben dreieinhalbtausend Mitarbeiter, an die fünfundzwanzigtausend Menschen, die es alle betrifft.

I: Mhm.

B: Über das wir reden, ja.

I: Ja.

B: Das ist ja schon gewaltig. Also das ist schon und da muss man das, wir haben Studierende, wir haben Mitarbeiter und wir haben, also wissenschaftliche und nichtwissenschaftliche, so muss man es irgendwie aufdröseln. Die Idee wäre, dass man sagt man nimmt die Verwaltung. Weil die meiner Meinung nach den größten, also die Mitarbeiter der Verwaltung den größten Bedarf an Sicherheit haben, denn dort laufen alle Daten zusammen.

I: Mhm.

B: Also ob es Gelder sind, ob es nachher die Studierendendaten sind, die dort entsprechend verarbeitet werden und da ist ein entsprechendes Vertrauen finde ich entsprechend abzubilden jetzt.

I: Mhm.

B: Und ich habe eine kleine Gruppe. Ich weiß nicht wie viele Mitarbeiter das sind. Aber man, die Idee wäre dann halt, das vielleicht dann zu nehmen, zu analysieren, zu gucken und dann weiter zu gehen.

I: Mhm.

B: Wie gesagt, wenn wir dann über die Studierenden reden, das sind zwanzigtausend, dann reden wir wieder darüber was ich eben gesagt hatte die soziale Komponente zwischenmenschlich. Was ist wenn ich plötzlich jemanden nicht mehr leider kann, ist er dann nicht mehr vertrauenswürdig?

I: Mhm.

B: Ja. Beispiel.

I: Mhm. Ja okay, das ist auch eine ganz gute Überleitung, denn mein nächster Teil wäre jetzt tatsächlich die Nutzer, die irgendwo mit Authentifikationsverfahren in Berühurng kommen.

B. Mhm, ja.

I: Und da genau wollte ich Sie einfach mal fragen wo jetzt die Nutzer, gut da haben wir jetzt schon drüber gesprochen, aber sobald Nutzer in Berührung kommen mit diesem Verfahren, wie sich da so die Bedienbarkeit gestaltet.

B. Ja, gut. Ja die, gut, ich bin jetzt ein Nutzer, ich habe natürlich nicht alle Nutzer befragt oder so, sondern, wenn ich jetzt selbst mich als Nutzer sehe, ist die Bedienbarkeit dessen was wir haben ganz okay. So, jetzt ist immer die Frage kann man es besser machen, waren wir eben schonmal.

I: Mhm.

B: Kann man. Ich finde, also noch früher als Student war es viel viel schwieriger, weiß ich noch aus der Erfahrung. Weil wie gesagt, wir hatten dann nicht diese G-Kennung und so ein Single-Sign-On, sage ich jetzt mal so in Anführungszeichen, in großen. Sondern ich hatte dann irgendwie auch ein Passwort für die Mail und dann für alle anderen Sachen noch mit Webdiensten und jeder Lehrstuhl hat natürlich irgendwann eine Anmeldeliste gehabt oder was auch immer und immer wieder neu musste ich mich anmelden mit einem neuen Passwort und hatte keine Anbindung, wie wir es jetzt haben, dann im LDAP, was da das große Thema ist als Protokoll für einen Verzeichnisdienst. Und, also ich finde so die Handhabung okay, zumal die G-Kennungen dann eingeführt wurden. Aus Informationssicherheitsperspektive eine gute Lösung, denn früher war es so, als Student hatte man eine S-Kennung, die war ein S und gefolgt von einer Matrikelnummer. Und jetzt ist die G-Kennung, ich glaube es ist eine Zufalls oder fortlaufende Zahl, die dahinter läuft, und ich kann nicht auf eine Matrikelnummer schließen und damit auf einen Studenten. Das heißt, dieser Schritt war schonmal gut, der war glaube ich auch gar nicht so einfach, weil da eine Menge Aufwand hinter steckt. Und in sofern finde ich jetzt die Benutzbarkeit dessen, was jetzt da ist ganz okay, ja.

I: Mhm.

B: Als Nutzer, als Benutzer jetzt. Ich kann jetzt nicht sagen, wie andere sich, andere, die kommen nicht zu mir und sagen, das ist ja ätzend hier oder sowas, nein, da gehen die halt zum Benutzerservice, das ist dann Usability in dem Fall dann.

I: Mhm. Also, genau. Gut, über die Probleme, die da auftreten können, haben wir ja schon gesprochen, da war das Stichwort TAN zum Beispiel, oder Stichwort Passwort vergessen, oder Stichwort, ich weiß nicht wie es, falls die Karte mal abhanden kommt. Das ist ja dann ähnlich einzustufen.

B: Genau.

I: Wie schätzen Sie denn so das Bewusstsein der Nutzer ein hinsichtlich IT-Sicherheit aber speziell jetzt in Richtung Authentifikation, also wie schätzen Sie ein, wie bewusst ist den Nutzern das, wodrums da genau geht. Also, wie schätzen die Nutzer da so die Sicherheit ein aus Ihrer Sicht.

B: Man kann jetzt nicht alle über einen Kamm scheren, aber ich sag jetzt mal, die Nutzer, die mit IT zu tun haben, haben ein großes Bewusstsein dafür. Das kricht man auch mit. Die, die reine Anwender sind vom Dienst, also die nicht von der IT her kommen, denen ist das im Grunde erstmal egal, Hauptsache es funktioniert. So, Stichwort Passwort an den Monitor kleben oder...

I: Mhm.

B: Oder um das, oder die Ablage, ja, so dass ein möglichst einfaches Passwort, das haben wir natürlich im Rahmen der Passwortrichtlinien ja jetzt etwas verkompliziert, vor, weiß nicht, zwei Jahren oder drei Jahren, dass halt bestimmte Voraussetzungen, Groß- Kleinbuchstaben Zahl Sonderzeichen und so weiter, mindestens acht Zeichen glaub ich oder sechs. Damit man da einen gewissen Riegel halt vorschiebt, damit nicht eins zwei drei als Passwort immer nur genommen wird.

I: Mhm.

B: Was halt sehr, wohl auch hier gut verbreitet war habe ich mir sagen lassen. Aber nochmal grundsätzlich, der Nutzer, dem ist das eigentlich Wurst. Das hat damit zu tun, dass jedermann dann, die Antwort heißt dann, soll jemand meine E-Mails lesen, ist ja eh dienstlich. Und gerade aus IT-Sicherheitssicht natürlich eine Katastrophe, weil es gerade dienstliche E-Mails sind.

I: Mhm.

B: Und, aber man muss es so sagen wie es ist, da wäre es jetzt, da habe ich jetzt eben auch wieder gesprochen, wenn man neue Verfahren einführt, moderne, ob das eine Chip-Karte wäre oder was auch immer, dann kricht man richtig Gegenwind.

I: Mhm.

B: Denn gerade in Sekreteriaten oder so weiter die wollen es einfach haben, es muss ganz einfach sein. Und ich weiß nicht, ob das es ist. Und einfach und eigentlich keine Veränderung. Also eine Veränderung ist immer schwierig, da hat man dann volle Kapelle, kricht man dann zurück, weil das hat doch früher geklappt, warum muss man das jetzt ändern. Und da gehts halt um Aufklärung, Schulungs- und Sensibilisierungsmaßnahmen.

I: Mhm.

B: Die alle durchzuführen wären im Vorfeld, damit man eben diese Wellen schon mal ein bisschen abschwächt, die dann kommen. Man kann denen, man kann natürlich auch nicht hergehen und geht jetzt in die Sekreteriate und sagt jetzt so, hier habt ihr einen Chipkarten-Leser, hier Chipkarte musst du da und da abholen, ja dann machst du das jetzt so. Und dann geht es los. Ja, warum und wieso und weshalb. Und das ist eben wiederum das Problem an der Uni. Bei einer Firma gäb es die Diskussion nicht, dann würde zwar intern auch ein bisschen gemurmelt und hin und her aber dann wäre das halt so. Und das geht nicht an einer Uni.

I: Mhm.

B: Weil da halt jeder auch seinen Freiheitsgrad irgendwie haben will und wie gesagt, einfach muss es sein.

I: Mhm, okay.

B: Und insofern sehe ich da das Bewusstsein jetzt grade auch für IT-Sicherheit im Großteil eher nicht so, trotz NSA und trotz was weiß ich. Die Leute regen sich darüber auf aber posten noch alles bei Facebook und nicht mehr, also, ja das Bewusstsein hat sich eigentlich nicht geändert.

I: Mhm.

B: Es gab den ein oder anderen, das sind dann die, die jetzt richtig paranoid geworden sind durch die ganze Sache, die haben sich gemeldet, das ist eine Hand voll. Die jetzt gesagt haben, hier müssen wir doch was ändern und wie verschlüssel ich jetzt meine E-Mails. Von den Leuten, die jetzt selbst zu einem gekommen sind, haben gesagt jetzt muss ich das, jetzt muss ich meine E-Mails alle verschlüsseln. Da brauch ich noch keine zwei Hände für. Wir reden hier von über zwanzigtausend Menschen. Andere machen es einfach, weil sie sich selbst damit auseinander setzen, aber der Großteil, die interessiert es nicht. Und die sehen auch, sehen sich auch niemals gefährdet, das ist auch immer so interessant. Wenn wir jetzt mal privat denken, da haben Sie auch private E-Mails und private Konten was auch immer. Aber die sehen sich nie gefährdet. Was sollen die denn von mir rauskriegen?

I: Mhm.

B: Dass ich nichts auf dem Konto habe oder was? Aber jeder hat was zu verbergen und zu schützen, sein irgendwas. Aber das sieht aber keiner. Ist mir egal, warum soll ich mir denn meine E-Mails verschlüsseln, das ist ja Aufwand. Ist es auch. Also wie gesagt, das Bewusstsein ist eher, hat sich nicht verändert im großen und ganzen, das ist meine Meinung dazu, leider.

I: Mhm, okay. Nochmal um zurück zu kommen auf dieses gegenseitige Authentifizieren, meinen Sie, dass sich das Bewusstsein da eventuell ändern könnte, sobald wirklich jeder mal in der Lage ist, seinen Mitmenschen irgendwo zu authentifizieren? Könnte sich da was ändern eventuell im Bewusstsein der...?

B: Nein, glaub ich nicht.

I: Nicht? Okay.

B: Ich denke halt, dass, es muss einfach sein. Also mit nahezu null Aufwand betrieben werden. Dann entwickelt sich vielleicht auch ein, naja Bewusstsein ist jetzt das falsche Wort.. Das ist so, dass die Leute einfach sagen, och Gott Moment, jetzt muss ich hier was installieren, jetzt muss ich hier klicken, jetzt muss ich das. Die ganz normale Problematik, also sie dürfen nicht gestört werden in dem was sie eigentlich tun wollen. Und dann würden die das akzeptieren, dann würden die sagen ja, dann machen wir das so. Das heißt, also ich glaube, dass sich da nichts ändern würde.

I: Mhm, okay. Ein letzter Punkt noch. Den hatten Sie auch eben schonmal kurz angesprochen, Stichwort Schulungsmaßnahmen, Sensibilisierung. Das ist ja auch ein sehr wichtiger Punkt gerade wenn wir jetzt über den Faktor Mensch reden. Gab es da schon Bestrebungen in die Richtung oder

gibt es da eventuell sogar noch was, was noch auf der Agenda steht und wurde da bereits was umgesetzt, und wenn ja, wie sah das aus?

B: Öhm.

I: Also sowohl jetzt unter, weiß ich nicht, Studenten oder Mitarbeitern generell. Ja.

B: Ja. Da stoßen wir nur organisatorisch und personell an Grenzen. Wenn ich, auch hier muss ich dann wieder verschiedene Bereiche betrachten. Wenn wir jetzt, eben haben wir jetzt über gesagt Bewusstsein oder aber sagen eine Veränderung herführen, indem wir sagen wir wollen E-Mails verschlüsseln, die alle dienstlich sind. Also von Mitarbeitern, also die Studenten nehmen wir jetzt gerade mal raus, wenn wir nur die Mitarbeiter sehen. Dann muss ich schulen, ja. Dann muss ich sagen okay, so installiere ich das Zertifikat bei den und den verschiedenen Mail-Clients und was auch immer. Was ist, wenn das Zertifikat verlängert werden muss, was ist dann, wenn es abgelaufen ist. Kann ich alte E-Mails noch verschlüsseln, sehen und so weiter. Und da muss ich ja ein Bewusstsein erstmal für schaffen, weil dann sonst kommt nämlich dann wieder die Frage, warum. Warum, ja? Und das durch Sensibilisierungs- und Schulungsmaßnahmen zu machen ist auf jeden Fall auf der Agenda, aber die Frage ist dann, wie. So, gehe ich jetzt, da reden wir jetzt über Zwang oder nicht, ganz klar, mach ich jetzt das Audimax voll oder die Turnhalle mit einem Tag a eine Stunde von A bis D, von D bis G, Nachnamen und durch jagen. Die sitzen dann da und dann sagen die ja gut, jetzt verbringe ich mal hier eine Stunde, ich hätte aber eigentlich was zu arbeiten und dann gehen die wieder nach Hause oder an ihren Arbeitsplatz. Da muss ein richtiges, meiner Meinung nach ein Konzept her und das haben wir noch nicht, ein Schulungskonzept, und das Problem ist dann, wer macht es? Weil, nochmal, ich kann nicht, wenn ich jetzt nur die Studierenden sehe, zwanzigtausend, wie will ich die jetzt schulen? Mitarbeiter, okay, das ist ein kleinerer Teil, sind immernoch dreieinhalbtausend. Also da denke ich wäre der Ansatz erstmal, bei der Einstellung schon einzugreifen. Also den Bestand muss man natürlich jetzt auch irgendwie abgreifen aber gerade in dem Einstellungsprozess, neue Mitarbeiter einstellen, denen dort, oder die sagen wir mal an drei oder vier Terminen pro Jahr dann zusammen zu trommeln. Die eben in dem Zeitraum neu eingestellt wurden. Das könnte man auch noch ein bisschen auf die SHKs nachher vielleicht ausweiten, um da dann anzusetzen, direkt am Anfang. Denn neue Mitarbeiter sind immer offen für die Sachen, also neuen Mitarbeitern, wenn ein neuer Mitarbeiter hier hin kommt, ob wissenschaftlich oder nicht wissenschaftlich oder in der Verwaltung, der ist, weil er ja auch hier arbeiten will, motiviert. Und wenn man jetzt zu ihm hingeht und sagt pass auf, wir müssen dir erklären, wir verschlüsseln die E-Mails jetzt alle, das funktioniert so und so. Der ist viel motivierter, das dann auch zu machen als jemand, der schon zwanzig Jahre hier sitzt und schon seit zwanzig Jahren das schon so gemacht hat, und dem muss ich jetzt sagen jetzt musst du es anders machen. Und dann kommt der und sagt was will der mir jetzt erzählen, seit zwanzig Jahren funktioniert das doch. Also da wäre der, um jetzt nochmal über ein Konzept zu reden, der Ansatz wie gesagt, das da anzusetzen und dann diesen Bestand, der jetzt da ist, auch versuchen zu schulen, aber das ist schwierig.

I: Mhm.

B: Und dann eben zu hoffen, dass über die Jahre das sich eben auswächst. Das wäre eine Möglichkeit und gerade diese, mit dieser Einstellung, da sind wir eigentlich schon dran, dass wir zumindest mal über Infomaterial und so weiter dann versuchen Mitarbeiter dann, die neuen Mitarbeiter dann da auszurüsten. Aber auch da ist jetzt die Situation aktuell, ich habe nur noch eine halbe Stelle jetzt auf dieser Ziso. Es kommt jetzt ein Nachfolger auf die andere halbe Stelle, die dann nachher wieder zu einer ganzen wird.

I: Mhm.

B: Und ich habe jetzt diese Organisation der IT-Sicherheit zu sehen, also eine Art Gremium, eine Art Sicherheitsmanagement-Team, das sind die Vertreter der Fakultäten, der UB, der Verwaltung und das ZIMT jeweils vertreten und die sind für ihren Bereich als IT-Sicherheitsbeauftragter eigentlich zuständig. Und dann könnte man hergehen und könnte sagen wenn man jetzt die Leute alle erreichen will, dann muss man das über die kanalisieren. Die haben aber ja einen normalen Job, die machen das nebenbei. Und da ist es auch wieder schwierig. Meiner Meinung nach muss das immer von oben kommen.

I: Mhm.

B: Wie gesagt, ich bin als Mitarbeiter des Rektorat an Stabstelle des Rektors, von oben muss das kommen. Aber alleine schwierig. Also sonst, dann bräuchte ich nichts mehr zu machen. Garnichts mehr. Wenn ich jetzt nur noch schulen würde und sensibilisieren. Sensibilisieren ist auch immer schön, da kann man dann ein bisschen mit Effekten arbeiten, bei gewissen Sachen wie mit Trojanern und so weiter, dass man das so ein bisschen böse darstellt, auch alles was passieren kann. Aber nochmal, das ist ein organisatorisches Problem den Bestand zu schulen. Da müsste, nochmal, also gerade sensibilisieren schulen am Anfang aber es muss ja weiter gehen, weil die Sachen verändern sich ja. Und gegebenenfalls neue Sachen, wir haben jetzt, wir könnten jetzt sagen okay verschlüssel deine E-Mails, indem du dir jetzt sofort beim Einstellungsprozess dein Zertifikat holst.

I: Mhm.

B: Gehe ich jetzt hier zu den Leuten und schick an alle ihr sollt euch jetzt ein Zertifikat holen platzt dem (anonym) da die Bude, weil er ist die einzige Registrierungsautorität an der Uni, ach nein der Herr (anonym) ist jetzt auch noch, genau dann sind es zwei. Aber das macht der nebenbei, der hat auch noch einen anderen Job, es gibt keine hauptberufliche Stelle dafür, die dafür zuständig ist. Und wie gesagt, das ist dann schwierig. Also wie gesagt ja, Konzept in der Mache, Planung ja, aber aktuell stoßen wir komplett personell und organisatorisch da an die Grenze.

I: Also das waren dann auch so ich sag mal die Hürden, die da in der Vergangenheit ein bisschen abschrecken haben lassen, dass man da nicht zugegriffen hat, ja?

B: Ja, nochmal, das beste Beispiel war jetzt diese E-Mail Verschlüsselung, dass wir sagen wenn dann machen wir das auch über das Zertifikat, wir könnten natürlich auch PGP also S/MIME dann, also PGP versuchen ja, dann sind wir wieder auch nachher mit irgendwelchen vertrauenswürdigen Ketten aufzubauen aber wir haben halt die Basis über diese Zertifikatstruktur und weil wir ja angebunden sind auch dann entsprechend deutschlandweit damit zu agieren. Und ja, ich sage jetzt mal die Infrastruktur muss da erst dann gebaut werden, wie gesagt der Herr (anonym) sitzt dann da und da kommen dann, stellen Sie sich mal vor ich würde das jetzt so sagen, okay ab sofort E-Mail Verschlüsselung mit S/MIME, hä was, und dann ja Zertifikat holen Schritt eins zwei drei klar und dann rennen die alle da runter und dann kricht der die Krise. Also das heißt erst da muss was aufgebaut werden damit überhaupt auch so Sachen umzusetzen sind. Ja, genau.

I: Mhm, ja.

B: Also es ist ein weites, ein sehr sehr weites großes Feld, also das habe ich jetzt in den anderthalb Jahren jetzt hier gesehen, dass eine Uni, wir sind ja relativ klein noch, wenn ich jetzt Köln sehe oder

sowas mit fünfzig- sechzigtausend Studenten und siebentausend Mitarbeitern doppelt so groß ist, wobei es eigentlich egal ist ob zwanzigtausend oder dreißigtausend oder fünfzigtausend, das Problem ist, diese Freiheit von Forschung und Lehre musst du immer beachten und das ist auch richtig so, aber die Umsetzungen dann von Sicherheitsmaßnahmen sind wirklich hart, von neuen Sachen. Rundschreiben, alles schön und gut, einen IT-Grundschutzkatalog für Anwender haben wir ja rausgegeben, da folgen dann nachher noch entsprechende Maßnahmen, also konkrete Schritte, wie auch jetzt mit der E-Mail Verschlüsselung, aber nochmal, das hat alles einen Impact auf die Gesamtstruktur und wie gesagt das, also es ist sehr sehr anstrengend aber auch interessant, das muss man sagen. Ja, aber trotzdem sind wir auf einem guten Weg.

I: Ja, okay. Ja das wars von meiner Seite.

B: Ja.

I: Wenn Sie nicht noch was haben, was Sie vielleicht nochmal betonen wollen, nein?. Gut, ja dann bedanke ich mich recht herzlich.

B: Gerne.

A3

Interviewtranskript – Firma DEW Stahl GmbH – 12.11.2014

I: So ja dann fangen wir mal an. Und zwar, Herr Feist, möchte ich Sie einfach mal einleitend fragen, wo hier in der Firma, also in Ihrem Bereich, wo Sie mit zu tun haben, Authentifikation eingesetzt wird, also Mechanismen zur Benutzerauthentifikation, Mitarbeiterauthentifikation und was da genau zum Einsatz kommt. Also welche Technologien oder welche Verfahren da eingesetzt werden.

B: Das lässt sich relativ einfach beantworten, weil wir haben für den für die Masse der Anwender einheitlich Windows-Oberflächen. Und was aus dieser Sicht dann an Sicherheit auf den auf den Anwender zukommt sind im Grunde genommen die Windows-Authentifikation und zwar nicht am lokalen PC sondern an der Domäne. Das heißt also unser gesamtes Rechner, unsere gesamte Windowsrechner-Welt ist in der als als in der Domänentechnik organisiert. Domänentechnik bedeutet einfach, dass es zentrale Einrichtungen gibt, die alle verfügbaren Windowsressourcen verwalten. Dazu zählen natürlich Benutzer, dazu zählen aber auch die Rechner selbst, dazu zählen Server, die bestimmte administrative und Dienstanwendungen zur Verfügung stellen, beispielsweise der E-Mail-Dienst, oder File-Ablagen, Shares und so weiter. Das ist also nicht Sache des Benutzers zu sagen, ich lege meine Daten irgendwo hin wo es mir gerade gefällt, sondern dort werden Windowsmechanismen benutzt.

I: Mhm.

B: Bedeutet eben, dass dass niemand irgendwie hier einen Rechner starten kann ohne sich entsprechend zu authentifizieren, grundsätzlich.

I: Mhm.

B: Früher war das ein bisschen anders.

I: Mhm.

B: Da gabs also in einzelnen Bereichen uneinheitliche Strukturen und da lag es beim Anwender sein Passwort festzulegen, wenn überhaupt, ...

I: Mhm.

B: ... und sich dort anzumelden.

I: Okay.

B: Ja. Also beispielsweise ist es nicht möglich, Arbeitsstationen zu betreiben, ohne Passwort beispielsweise, nur Benutzername und fertig. So etwas gibt es nicht mehr. Also Administrator, blankes leeres Passwort, das ...

I: Mhm.

B: ... das geht nicht. Gut. Das hat auch zur Folge, dass beispielsweise Ressourcen benutzerabhängig verwaltet werden können. Beispielsweise kann man in diesem System, ich weiß nicht ob es wirklich praktiziert wird, zum Beispiel Quotas zum Teil, dass also bestimmte Benutzergruppen nur über

bestimmte Kapazitäten auf Fileservern beispielsweise verfügen, sowas in der Art.

I: Mhm.

B: Gut, und ja das ist eigentlich der Hauptsicherheitsmechanismus, der greift. Über diese Domänenbenutzerstruktur lässt sich natürlich weiterhin erreichen, dass man innerhalb der Benutzer selbst differenzieren kann, welcher Benutzer halt was darf.

I: Mhm.

B: Das heißt also grundsätzlich werden in dieses Domänensystem oder in das vernetzte Rechnersystem nur authentifizierte Benutzer gelassen, das geht über die Anmeldung. Zum zweiten wird aber auch geregelt was darf dann so ein Benutzer. Und da kann man sehr fein strukturieren, Zugang zu Servern beispielsweise oder Zugang zu Ressourcen generell, das betrifft also Drucken, das betrifft die File-Ablagen und kann da im Grunde genommen so Abteilungen voneinander abgrenzen beispielsweise. Es gibt ja in jedem Unternehmen recht sensible Datenbereiche, wo man wünscht, dass dort wirklich nur die entsprechend qualifizierten und zugelassenen Mitarbeiter Zugriff haben. Das lässt sich beispielsweise über solche Dinge erreichen.

I: Mhm.

B: Also, üblicherweise werden werden Benutzer zu Gruppen zusammengefasst, oder andersrum, wir kreieren im Grunde genommen für bestimmte Aufgaben Berechtigungsgruppen. Das heißt also die Gruppe wird berechtigt, bestimmte Dinge zu tun. Zugriff, Lesen, Schreiben, wie auch immer auf bestimmte Ressourcen und dadurch, dass bestimmte Benutzer so einer Gruppe zugeordnet werden, erhalten die Benutzer dann entsprechend die selben die Rechte der Gruppe.

I: Sie sprachen jetzt eben schonmal davon, dass das nicht immer so war, ich zitiere das hat sich ja schon ein bisschen geändert und daraus lassen sich ja das lässt sich ja bestimmt irgendwo zurückführen auf Vorgaben, die von irgendwo kommen beziehungsweise es ist ja schon irgendwo aus irgendeiner Intention heraus entstanden, dass da irgendwo vielleicht mal gesagt wurde, so und so, das wird vorgegeben. Können Sie da was zu sagen, wie die Vorgaben da sind und wie die Umsetzung da sich so gestaltet? Dieser Vorgaben?

B: Also grundsätzlich die bestehende Struktur ist was diese Dinge angeht hierarchisch geordnet.

I: Mhm.

B: Das heißt also nicht die einzelnen Abteilungen legen fest, wie Sicherheit praktiziert wird, sondern es gibt Richtlinien, die allgemeingültig sind das heißt für das ganze Unternehmen gelten. Also dort, wo es möglich ist Sicherheit zu spezifizieren, beispielsweise wie muss ein Passwort aussehen. Wann muss ich ein Passwort ändern, wie lange darf es gültig sein und dergleichen. Dort wo das möglich ist wird es eben durchgesetzt. Und zwar erlaubt es ja die Domänenstruktur quasi solche Regeln bis auf den letzten Benutzer quasi herunter zu verteilen oder zur Anwendung zu bringen.

I: Mhm.

B: Und genau das passiert auch. Also wir haben also von der Struktur der IT sieht es so aus, dass von unten nach oben sag ich mal der Sachverstand zunimmt, das heißt also selbst auf unteren

Ebenen gibt es mittlerweile sehr viele Mitarbeiter, die sich mit Rechnertechnik und diesen Dingen auskennen.

I: Mhm.

B: Auch das war nicht immer so, das ist gewachsen, ja?

I: Mhm.

B: Aber um das alles zu vereinheitlichen hat man gesagt okay, wir versuchen, in den Hauptabteilungen, sagen wir jetzt mal Stahlwerk, Walzwerk oder ähnlichen großen Strukturen, bestimmte Mitarbeiter mit bestimmten Aufgaben was auch IT-Infrastruktur angeht also denen bestimmte Aufgabe zu übertragen.

I: Mhm.

B: Ja, die dann aber koordiniert werden von einer zentralen IT. Und die zentrale IT sitzt hier am Standort, nein die ist auch verteilt. Die verteilt sich über mehrere Standorte, ist aber strukturell einheitlich. Es gibt also eine Abteilung, CIT heißt die bei uns, die zuständig ist für die Belange der Gesamt-IT an den Standorten der DEW Stahl. Und das sind also soweit ich weiß vier Stück an der Zahl. Also standortübergreifend wird von einer IT festgelegt, wie Sicherheit, wie Datentechnik zu leben ist.

I: Mhm.

B: Und weitergereicht wird das halt über sogenannte Koordinatoren an den einzelnen Standorten in bestimmten Abteilungen, die dann wiederum verantwortlich sind für eine bestimmte Anzahl von Geräten, für eine bestimmte Anzahl von Benutzern.

I: Okay.

B: Also es geht also wenn man so will top down.

I: Mhm. Ja, gut dann, gut jetzt mal die aktuelle Situation, wenn wir uns die mal betrachten so wie Sie mir die jetzt auch geschildert haben, wie sind Sie aus Ihrer eigenen Sicht, wie sehr zufrieden sind Sie mit der Geschichte? Also sehen Sie irgendwo Lücken oder Verbesserungsdinge, wo man verbessern kann oder sind da vielleicht irgendwo, ja genau, Potenziale noch nicht ganz ausgeschöpft? Einfach aus Ihrer Sicht.

B: Ja gut Zufriedenheit ist ja immer ein relativer Begriff.

I: Ja.

B: Zufriedenheit bedeutet ja für denjenigen, der diesen Begriff für sich in Anspruch nimmt, dass er die bestehenden Konstrukte als nützlich für das empfindet, was er leisten soll, für was er verantwortlich ist.

I: Mhm.

B: Das heißt also jemand der für IT-Sicherheit zuständig ist wird alles tun um beispielsweise

irgendwelche sicherheitsrelevanten Verfälle, was weiß ich, Virenattacken und was es da alles gibt, auf ein Minimum zu begrenzen. Das heißt also er wird versuchen relativ hohe Hürden einzubauen, die eben solche unerwünschten Vorfälle verhindern sollen.

I: Mhm.

B: Jemand der die Systeme nur benutzt um damit seinen alltäglichen Kram zu erledigen, seine Arbeit zu machen, der wird das nicht immer nachvollziehen können. Der wird sagen warum muss ich jetzt mein Passwort schon wieder ändern beispielsweise, solche Dinge. Da sind die Interessen ein bisschen gegenläufig, da wird häufig gewünscht die Hürden nicht ganz so hoch zu machen, um eben Rückfragen zu verhindern oder Unsicherheit zu verändern, was ist jetzt schon wieder los, warum verstehe ich das nicht und sowas in der Art.

I: Mhm.

B: Ich denke wir haben hier ein relativ ausgewogenes Konzept mittlerweile umgesetzt. Das heißt also sowohl die verantwortlichen Leiter werden oder haben erfahren, dass die sicherheitsrelevanten Vorfälle eigentlich sehr gering geworden sind, von der Häufigkeit her und auch von der Schwere. Und die Benutzer haben gelernt, mit den notwendigen sag ich mal Restriktionen erfolgreich zurecht zu kommen. Das war aber ein gewisser Lernprozess, das war nicht immer ganz einfach. Und ohne jetzt wirklich gute Beispiele parat zu haben, vielleicht fällt mir ja noch eins ein, war es in manchen Fällen so, dass dann auch wieder Richtlinien, die halt zu scharf für die Praxis waren, ein bisschen gelockert werden mussten.

I: Okay.

B: Ich meine man hat mal versucht, extra starke Passwörter einzuführen und das war dann für die Benutzer ein bisschen zu schwierig, sagen wir mal gedankentechnisch oder memotechnisch damit zu Recht zu kommen.

I: Okay. Genau daraus jetzt ableitend, auch aus dieser Entschärfung sag ich mal, beziehungsweise das jetzt noch vorweg, fallen Ihnen jetzt konkret noch weitere Technologien oder noch weitere Mechanismen ein, die Sie in Zukunft eventuell sich vorstellen könnten einzusetzen oder die vielleicht sogar irgendwo in der Planung sind oder die aus Ihrer Sicht umsetzbar wären und auch sinnbehaftet wären?

B: Es gibt für einzelne Anwender oder für einzelne Anwendungsbereiche gibt es spezielle Sicherheitsmechanismen, beispielsweise, also die jetzt schon eingeführt sind, beispielsweise für den Bereich der mobilen Geräte, also dort wo Laptops im Einsatz sind gelten artens die selben Regeln, wie für alle Rechner innerhalb der Firma stationär existieren. Das heißt also hier, was weiß ich, Authentifizierung und der gleichen, Domänenzugehörigkeit. Aber zusätzlich wird beispielsweise bei mobilen Geräten eine Festplattenverschlüsselung standardmäßig angewandt. Das heißt also falls mal so ein Gerät, in der Regel ist das ein Laptop, verloren gehen sollte, hat also der Finder nicht unmittelbar die Chance die Festplatte auszubauen und auszulesen beispielsweise.

I: Mhm.

B: Und das ist ja sag ich mal ein Fall, der gar nicht so unwahrscheinlich ist. Diebstahl oder einfach nur Laptop am Flughafen vergessen oder sowas in der Art. Und damit werden also Unternehmensdaten oder auch sensible Informationen durchaus für einen Dritten abzulesen oder

auszulesen, wenn man auf so ein Sicherheitsfeature verzichten würde. Das fällt mir gerade so ein. Das haben wir aber schon.

I: Okay.

B: Möglicherweise ist Verschlüsselung durchaus ein Thema für Bereiche, E-Mail zum Beispiel.

I: Mhm, okay.

B: Da gibt es also auch entsprechende Überlegungen soweit ich weiß. Haben wir sonst noch sowas? Nein. Was wir haben ist eine Firewall-Technologie zur Abschottung des Firmennetzes gegenüber dem Internet. Das heißt also Internetzugang aus dem Firmennetz raus ist also nur möglich, wenn im Grunde genommen der Benutzer an der Firewall bekannt ist. Das heißt also jemand der oder Benutzergruppen, denen man dieses Recht nicht zubilligt, haben auch zunächst mal keine Möglichkeit ins Internet rein zu gehen.

I: Mhm.

B: Und umgekehrt Zugriff aus dem Internet auf unsere Systeme werden auch strikt von der Firewall kontrolliert.

I: Okay. Darauf gerade noch aufbauend auf den Dingen, die Sie sich vorstellen könnten oder die Sie mir gerade beschrieben haben, wenn Sie sich einfach mal Gedanken machen müssten, aus Ihrer Sicht jetzt über eine optimale Lösung oder zumindest über eine optimale Teillösung. Fällt Ihnen da spontan etwas ein, wie es aus Ihrer Sicht sein sollte? Wenn Sie da Fügungsgewalt hätten, sag ich mal.

B: Das ist eine schwierige Frage.

I: Also...

B: Beispiel, geben Sie mir mal ein Beispiel. Was könnte es sein?

I: Ja, also Sie können das auch gerne beschränken jetzt auf einen Teil, auf den Sie jetzt in der Praxis häufig mit zu tun haben, wo Sie sich einfach denken, warum macht man das nicht besser so oder so. Oder optimalerweise wäre das und das der Fall. Also ein konkretes Beispiel kann ich Ihnen jetzt auch nicht geben, da frag ich Sie ob Ihnen spontan einfällt, vielleicht aus der Praxis raus.

B: Da bringen Sie mich echt ins Grübeln. Da bringen Sie mich echt ins Grübeln, ja. Was könnte es sein? Also ich würde mir vielleicht den Bereich der mobilen Datenträger vielleicht nochmal vornehmen, also all das was mit USB-Technik heutzutage zu bewegen ist. Weil ich kann mir vorstellen, dass das also immer noch die einfachste Möglichkeite ist artens fremde Daten in die Firma rein zu schleusen aber auch Firmendaten leicht und unbehelligt zu transportieren, wo auch immer hin. Allerdings konkret oder andersrum. Ich weiß, dass es da Möglichkeiten gibt auch am USB-Port Barrieren zu setzen. Sei es jetzt durch, also rein technisch, dafür zu sorgen, dass also wirklich nur noch die wenigsten Benutzer dort Zugriff haben. Wäre vielleicht ein Punkt den ich angehen würde, wenn man mich fragt in der Richtung. Ne ansonsten fühlen wir uns also hier sagen wir mal was die Sicherheitseinrichtungen angeht relativ gut aufgehoben.

I: Mhm. Okay, um gerade nochmal kurz auf die verschiedenen Bereiche beziehungsweise die

verschiedenen Anwendungen zurück zu kommen, fällt Ihnen da noch neben der, wir haben jetzt primär über digitale Authentifikation gesprochen, also wo es um Benutzername Passwort geht, um digitale Identitätskontrolle sag ich mal. Gibt es da eventuell noch andere Verfahren, die nicht direkt am Bildschirm stattfinden sondern anderweitig umgesetzt werden?

B: Okay. Wenn man jetzt daran denkt, auch Abteilungen körperlich abzuschotten, mal mit Türen oder Sicherheitssystemen an diesen Stellen, das wird im Großen und Ganzen hier nicht praktiziert, also die Abteilungen sind zunächst einmal offen, kann man sagen, für den Zugang.

I: Okay.

B: Also man hat ja die Möglichkeit durchaus mit, was weiß ich, mit Kartentechnik und so weiter da Zugänge zu kontrollieren und auch gegen Unbefugte zu sichern. Das haben wir hier noch nicht praktiziert, in der Tat.

I: Okay. Wäre das was, was Sie sich vorstellen könnten?

B: Das ist immer eine Frage wie, also vorstellen kann ich mir es, durchaus. Ich könnte mir beispielsweise vorstellen, dass dort wo wirklich auch mit sensiblen Informationen umgegangen wird, was weiß ich, eine Personalabteilung wird immer ganz gerne genannt oder so etwas oder auch die IT selbst, dort wo Sicherheit gemacht wird. Dass man sich durchaus nicht unwohler fühlen müsste, wenn man sagt okay, also hier kommen erstmal nur unsere Mitarbeiter rein. Und andere haben vielleicht erstmal sich zu melden oder um Zugang zu bitten. Ganz einfach. Und an den Werkstoren ist das weitgehend umgesetzt, da haben also nur Mitarbeiter Zugang oder entsprechende Inhaber eines Ausweises eine Karte erhalten. Aber im Großen und Ganzen ist es so, dass die Abteilungsflure zugänglich sind für jemanden, der sich im Werk aufhält.

I: Okay.

B: Also dort ist sicherlich mehr möglich.

I: Okay. Also ist es im Moment so die Situation, wenn ich das richtig deute, dass da so ein bisschen implizit dann davon ausgegangen wird, dass derjenige, der hier rein kommt, auch das Recht dazu hat?

B: Ich denke mal das ist so und das ist immer so lange so natürlich wie solch ein Vertrauen sag ich mal, was man in die Mitarbeiter setzt, nicht missbraucht wird. Also ich denke mal wenn Vorgänge sich ereignen, die dort zu einer sag ich mal zu einem Vertrauensmissbrauch oder auf einen Vertrauensmissbrauch hinweisen, sei es jetzt Diebstahl am Arbeitsplatz oder solche Dinge, dass dann möglicherweise auch eine Diskussion wieder in Gang kommt die sagt, also okay, wir brauchen schon etwas mehr auch an der Stelle. Aber vielleicht wird der Bereich Stahlindustrie oder allgemein noch nicht als so sensibel eingestuft, generell.

I: Okay.

B: Also sag ich mal jetzt im Vergleich zu vielleicht Behörden oder der gleichen. Andererseits, wenn man mal im Finanzamt ist, dann denke ich mal kommt man auch auf jeden Flur. Und wenn dann so eine Tür offen steht dann ist man im Steuergeheimnis sozusagen. Ich habs noch nicht ausprobiert.

I: Gut. Okay so als nächstes, um den Bereich der Systeme so ein bisschen abzuschließen, habe ich

noch eine Frage, ob Sie sich vorstellen könnten, also jetzt rein aus Ihrer Sicht ob Sie sich vorstellen könnten, statt jetzt den herkömmlichen Methoden oder den herkömmlichen Authentifizierungsmaßnahmen die hier getroffen wurden oder im Moment so im Einsatz sind, ob Sie sich vorstellen könnten, dass das vielleicht, dass vielleicht umgesetzt wird, dass irgendwie eine Art Netz aufgebaut wird aus den Mitarbeitern, oder auch aus also aus Teilnehmern an dieser ganzen Geschichte, ein Netz aufgebaut wird, wo die Teilnehmer sich gegenseitig authentifizieren, also wo das nicht zentral gesteuert wird sondern wo die Nutzer gegenseitig sozusagen Ihre Identität verifizieren, bestätigen können? So dass da Vertrauen so die Basis der ganzen Authentifikation ist?

B: Ich gebe zu, das ist mir jetzt ein neuer Gedanken. Wie soll das in der Praxis aussehen oder wie könnte das aussehen? Wenn ich mal zurückfragen darf.

I: Also ja ein Beispiel wäre jetzt zum Beispiel, dass, um einfach mal ein Beispiel zu nennen, meinetwegen ein Lieferant von jetzt in Ihrem Fall Schrott zum Beispiel, dass der wiederrum anderen Lieferanten ausstellt, ich kenne diesen Lieferanten XY, ich vertraue ihm, also ist er sozusagen gleichzeitig authentifiziert. Weil derjenige, den man schon kennt, der authentifiziert ist, wiederrum einem anderen bestätigt hat, ja dem kann man vertrauen und dass dadurch dann so ein Netz entsteht sozusagen. Was dann auch erlaubt irgendwo kurzfristig die Erlaubnis zu geben oder die Authentifikation dann zu liefern. Das kann man dann auch übertragen auf andere Bereiche.

B: Mhm, also schwer, schwer glaube ich.

I: Mhm.

B: Also zum Einen fehlt mir ein bisschen jetzt die Fantasie mir vorzustellen, wo das nützlich sein könnte, für das Ganze. Zum Anderen glaube ich nicht, dass die Strukturen oder das Denken so von Sicherheit so etwas hergibt. So eine automatische Vererbung quasi von Vertrauen an Dritte womöglich. Ne ich glaube das wäre nicht so der gangbare Weg. Also wenn man, da könnte man für werben irgendwie, wenn man die Möglichkeit hätte, aber ich glaube die erste Reaktion wäre eher da auch restriktiv.

I: Mhm.

B: Weil einfach die Strukturen geeignet und auch dafür gedacht sind, von zentraler Stelle auch die Kontrolle zu behalten. Und da ist es eben so, dass beispielsweise die Benutzer wirklich zentral administriert werden und die vermehren sich nicht in irgendeiner Art und Weise sondern man kennt sie im Grunde genommen und auf der Basis sagt man okay das ist unser Mitarbeiter, der hat einen Namen, der hat eine Personalnummer und dem geben wir die Rechte, an unseren Rechnersystemen zu arbeiten.

I: Mhm.

B: Und auch Daten im Netz zu bewegen und dergleichen mehr. Das, ja da steckt kein Automatismus drin. Der einzige Automatismus ist oder wenn Automatismen drin stecken, dann sind das eben die, dass im Gegenteil Sicherheit abgebaut wird, wenn beispielsweise sich ein Benutzer eine bestimmte Zeit lang nicht am Netz angemeldet hat. Dann sagt irgendjemand da stimmt was nicht, den legen wir erstmal still. Das gilt für Maschinen und das gilt auch für Benutzer. Das heißt also Passwörter verfallen irgendwann mal.

I: Okay.

B: Und Maschinenkonten verfallen ebenfalls. Also die haben eine bestimmte Lebensdauer nur. Gut, zu Maschinen könnte ich auch noch was erzählen.

I: Gerne.

B: Und zwar ist unser Netzwerk durchaus mit Intelligenz versehen. Das heißt also der Zugang zu unserem Netzwerk ist also nicht allein dadurch gegeben, dass jemand eine Netzwerkdose findet und sich dann mit einem Gerät dann aufstöpfselt und hurra, ich habe eine IP-Adresse oder so so etwas, was vielleicht auch manchmal geht. Nein, es ist so, dass die Gerätschaften, also die Hardware, die mit dem, die am Netz kommuniziert und teilnimmt, dass die letztlich auch administriert und registriert sein muss. Das heißt also wenn beispielsweise hier jemand rein kommt mit einem eigenen Laptop, der wird also nicht im Netz eine IP-Adresse bekommen und kommunizieren können. Das geht nicht. Das ist natürlich in manchen Situationen jetzt beispielsweise wenn es darum geht, Ersatzgeräte kurzfristig in Betrieb zu nehmen, im Falle eines Defekts beispielsweise, kann das hinderlich sein, weil wenn das Ersatzgerät lange Zeit nicht am Netzwerk war, ist es dort unbekannt, das Konto wird zumindest gesperrt und die Maschine kann am Netz nicht in Betrieb genommen werden. Fertig. Das ist so ein typischer Fall wo die Sicherheitsinteressen vielleicht den betrieblichen Interessen kurzfristig im Wege stehen. Aber auch dafür gibt es Lösungen das relativ zeitnah dann abzuarbeiten.

I: Ja, okay. Gut, ja dann würde ich gern so den nächsten Teil einleiten und zwar geht es mir jetzt nochmal speziell um die, wir haben jetzt über die Systeme gesprochen, über die Umsetzung, die Techniken, die Technologien, jetzt würde ich gern nochmal zum Schluss auf die Nutzer an sich zu sprechen kommen, also sozusagen auf die, wenn man es so nennen mag, menschliche Komponente bei der ganzen Geschichte. Und da einfach mal nachfragen, wo jetzt die Benutzer in Berührung kommen mit Authentifikation an sich, mit den eigentlichen Verfahren und wie sich da so die Bedienbarkeit gestaltet der Verfahren, also aus Nutzerperspektive sozusagen.

B: Ja. Also das ist relativ unkompliziert. Also wie eingangs schon gesagt ist der primäre Zugang die lokale Windows-Anmeldung, das heißt also jemand der früh morgens sein Gerät einschaltet, der wird gezwungen sich erstmal an der Windows-Domäne zu authentifizieren. Das ist der erste Schritt. Gelingt diese Anmeldung, stehen alle entsprechend zugewiesenen Ressourcen sofort offen. Also der Mann kann, oder der Mitarbeiter kann natürlich sofort loslegen und der muss sich nicht drum kümmern, ob da ein Drucker eingerichtet ist oder irgendwas. Also seine Welt ist erstmal damit komplett verfügbar. #

I: Okay.

B: Im Einzelfall kann es Momente geben, wo dann eine erneute Authentifizierung notwendig ist, beispielsweise wenn jemand der an der Firewall nicht bekannt ist ins Internet möchte. Dann stößt er natürlich auf ein Sicherheitsfenster und wird gebeten sich zu authentifizieren. Kann er das, kann er weiter arbeiten, kann er das nicht, dann war es das. Dann bleibt es bei dem Versuch ins Internet zu gehen, beispielsweise. Nein, üblicherweise wird die Eingangsauthentifizierung führt dazu, dass alle windowsgestützten Systeme dort quasi dem Benutzer zur Verfügung stehen. Also eine wiederholte Passworteingabe ist eigentlich nicht notwendig. Es sei denn Benutzer müssen sich auf spezielle Server begeben, die also nicht sag ich mal unmittelbar an das Windows-Domänen- und an die Windows-Benutzer-Verwaltung angeschlossen sind. Im Allgemeinen sind das spezielle Rechner, die zuständig sind für die Steuerung von Prozessabläufen in der Produktion. Die stehen so ein bisschen außerhalb dieses Systems.

I: Okay.

B: Ganz einfach weil dort die Verbindungen der Rechner untereinander und auch zum Prozess anderen Regeln gehorchen müssen. Das heißt also da ist nicht der Benutzer ausschlaggebend sondern da unterhalten sich die Maschinen miteinander und die kommunizieren in diesem Bereich im allgemeinen über ihre IP-Adressen. Das heißt also selbst wenn das Domänen-Benutzer-System also ausfallen würde, der Domänenserver ist, keine Ahnung, ist down und würde keine Authentifizierung mehr entgegen nehmen und verarbeiten, würden solche Systeme weiterlaufen.

I: Okay.

B: Aber das ist dann der Bereich nicht der Datensicherheit sondern der Prozesssicherheit, der da den Vorrang hat. Also da gelten etwas andere Regeln. Aber auch da gilt, der Zugang zu den Systemen ist wiederrum über zumindest eine Passwortabfrage Benutzerpasswort eingegrenzt.

I: Ja. Um nochmal kurz die Sache aufzugreifen, dass in der Regel die einmalige Anmeldung sag ich mal morgens ausreicht, um die Welt des Benutzers quasi zu öffnen. Gibt es da eventuell Abkürzungen im System? Also ist es irgendwie dadurch vielleicht auch dem Nutzer möglich das System irgendwie auszutricksen oder sich das Leben ein bisschen einfacher zu machen?

B: Grundsätzlich nicht, nein. Und selbst wenn der Benutzer seinen Rechner nicht ausschalten würde, also durchlaufen lassen würde, greift dieser, wei heißt das hier, Bildschirmschoner, die Technik greift dann und erzwingt nach einer bestimmten Zeit eh eine neue Anmeldung oder respektive eine neue Mitteilung des Passworts. Ne, ich wüsste nicht wie die Benutzer da rumkommen. Das wäre mir nicht bekannt.

I: Okay. Genau. Und sehen Sie dann in der Richtung dann auch so keinen direkten Bedarf, also Sie halten da was die Benutzerkomponente angeht das System dann schon für sicher?

B: Gut, die Schwachstelle sollte oder dürfte der Benutzer selbst sein in dem Fall.

I: Mhm, okay.

B: Also da wird zwar drauf hingewiesen, auf die Verwendung von sicheren Passwörtern, auf den Umgang mit Passwörtern selbstverständlich auch. Es gibt da ein Informationsblatt, was der Benutzer unterschreiben muss, das heißt also vom Benutzer wird durchaus abverlangt die Kenntnisnahme und auch quasi die Übernahme von Verantwortung an der Stelle. Das gilt also natürlich für die Weitergabe von Passwörtern an Dritte und so weiter.

I: Ja.

B: Also da ist schon denke ich mal viel dafür getan worden auch an der Stelle, die Benutzer sensibel zu halten, dass sie ihr Passwort nicht unter die Tastatur schreiben oder dergleichen mehr oder womöglich an den Bildschirm kleben, so wie es also früher auch schonmal zu beobachten war. Gut, ich bin jetzt nicht derjenige der durch die Büros geht und das nachprüft. Aber möglicherweise findet man oder sagen wir so, ich bin überzeugt man findet dort eigentlich wenig Nachlässigkeit in der Hinsicht. Weil man muss auch dazu sagen, das ist zum Glück schon Jahre her, aber wir hatten schon Ereignisse, die durchaus geeignet waren den Anwendern oder überhaupt den Mitarbeitern hier klar zu machen, wie gefährlich eigentlich auch Datentechnik werden kann, wenn sie dazu führt oder

wenn Missbrauch dazu führt, dass eben Systeme komplett lahm gelegt werden. Und wir haben hier also durchaus schon eine Virenattacke erlebt, die also spürbare Folgen hatte.

I: Okay.

B: Also ich glaube spätestens danach war allen klar, dass jeder selbst auch seinen Teil an Verantwortung und Bemühen dazu beitragen mussten, um die Systeme wirklich sicher zu machen am Ende. Ne aber unmittelbar Verbesserungsbedarf an der Stelle sehe ich nicht. Auch die Einführung von was weiß ich hier Fingerprints und dergleichen kann man nutzen, wird uns an einzelnen Stellen auch aber nicht zwingend und ich glaube auch nicht, dass es wirklich ein Muss ist im Moment. Es ist einfach so, wenn alle mitmachen und die vorgegebenen Regeln beachten, dann denke ich schon haben wir einen recht guten Stand hier in der Firma.

I: Sie sprachen da gerade schon die Verantwortung der Nutzer also das Bewusstsein der Nutzer sozusagen was die Sicherheit angeht an. Also schätzen Sie da das Bewusstsein der Nutzer auch so ein, dass da die Sicherheit gewährleistet wird?

B: Bewusstsein ändert sich. Also ich würde es als relativ hoch einstufen, weil, doch, nachdem was ich erlebt habe haben die Benutzer selbst, fühlen sich durchaus als Teil von irgendwas. Also das soll jetzt nicht pathetisch klingen oder irgendwas, die stehen auch nicht morgens zum Appell da und halten sich die Hand dann irgendwo hin. Nein, aber einfach vom Bewusstsein, ich habe hier einen Platz in der Firma und der Platz der soll also tunlichst nicht ins Chaos abgleiten. Dazu gehört eben ein bisschen Ordnung im rein physikalischen Sinne, dass also die Arbeitsplätze einer gewissen Ordnung unterliegen. Und das setzt sich dann auch durch bis an die IT-Systeme, dass auch da Regeln gelten, die akzeptiert sind und die also durchaus auch allen geläufig sind. Ich glaube wenn jemand in einer Bürogemeinschaft, die vielleicht aus zwei drei oder vier Mitgliedern besteht, da aus der Reihe fallen würde, der würde durchaus von den Übrigen getroffen gewiesen werden. Ich denke da ist schon ein allgemeines Verständnis und auch ein Commitment in der Richtung zu beobachten. Mein Eindruck.

I: Okay. Ja, um das Ganze noch abzurunden, die letzte Frage geht mir nochmal speziell jetzt um Schulungsmaßnahmen. Sie sprachen eben schon kurz von Sensibilisierung der Nutzer und das Infoblatt von dem Sie kurz gesprochen haben. Einfach nur mal um auf die Schulungsmaßnahmen zu kommen, gab es da in der Vergangenheit in Richtung Authentifikation, in Richtung Bewusstsein der Nutzer was die IT-Sicherheit angeht, was die Identitätssicherheit angeht, die Datensicherheit angeht, gab es da in der Vergangenheit schon Bestrebungen oder ist da noch was in der Umsetzung oder ist da noch was geplant?

B: Also Veranstaltungen, die sagen wir mal den Charakter von Schulungen Fortbildungen und dergleichen haben, sind meines Wissens nach oder konzentrieren sich darauf, Fachkenntnisse zu vermitteln. Also wir haben durchaus ein anspruchsvolles Fortbildungsprogramm oder Weiterbildungsprogramm, das aber abzielt auf, was weiß ich, Kenntnisse jetzt Excel-Erweiterungen oder dergleichen, also sprich fachliche datenverarbeitende Kenntnisse vermittelt. Ich bin mir aber im Moment nicht ganz sicher, ob in den Führungsebenen an der Stelle Bewusstsein geschult wird. Ich könnte es mir vorstellen. Aber dann wäre der Kreis der Teilnehmer eher Personen mit Personalführung von denen dann natürlich erwartet wird, dass sie die Gedanken im persönlichen Gespräch mit den Mitarbeitern weitervererben jetzt oder weitergeben halt. Also für die breite Masse der Anwender selbst werden Schulungen im Allgemeinen nur dann aufgelegt, wenn es um die Einführung neuer Systeme geht. Also ich kann mich erinnern wir sind irgendwann mal umgestiegen ich glaube von NT auf XP oder so etwas, da wurde dann im breiteren Sinne geschult um halt an

neue Oberflächen heranzuführen. Wobei da natürlich auch die sag ich mal neuen Sicherheits-Features eine Rolle spielen selbstverständlich. Aber dass jetzt gesagt würde hier so im Sinne von Feuerwehrübung, wir üben jetzt mal Sicherheit, das habe ich noch nicht erlebt. Das ist auch ein bisschen, ist auch nicht ganz so einfach damit eine bestimmte Zeit zu füllen auch.

I: Mhm.

B: Weil die wenigen Schritte, die der Benutzer durchführen muss und die wenigen Regeln, die er beachten muss, die sind relativ schnell erklärt. Zumal sie sich ja auch über die Systemgrenzen einheitlich fortsetzen. Beispielsweise gibt es innerhalb der Anwendungen nach der Windows-Authentifizierung, da muss ich die, ja da müssen Sie jetzt das entsprechend ergänzen, beispielsweise Anwendung SAP, die über eine eigene Benutzerverwaltung verfügen, wo dann natürlich der Benutzer sich erneut ausweisen muss. SAP wäre also eine Anwendung, die nicht durchgängig quasi ins Windows integriert ist.

I: Gibt es da noch Unterschiede, fallen Ihnen da noch Unterschiede ein? Was wir vielleicht bis jetzt noch nicht so besprochen hatten? Um jetzt nochmal auf SAP zu sprechen zu kommen.

B: Also ich bin jetzt kein SAP-Anwender selbst aber so vom Hörensagen was ich so mitbekomme sind die Mechanismen relativ ähnlich. Ich weiß nicht ob sich die Anzahl der Zeichen die Mindestzeichen im Passwort eben unterscheiden muss in beiden Systemen. Aber ich meine es sind relativ gleiche Muster, die dort vom Benutzer verlangt werden. Ich glaube die Lebensdauer der Passwörter ist ähnlich groß, auch das Verhalten bei Nicht-Anmeldung, der Verfall von Passwörtern und Benutzerkonten oder die Deaktivierung, das entspricht sich fast. Also da muss der Benutzer sage ich mal gedanklich nicht umschalten von einem zum anderen System.

I: Okay. Um nochmal auf die Schulungen zurück zu kommen kurz, sehen Sie denn da noch Bedarf aktuell? An gewissen Stellen, da vielleicht nochmal gezielt zu informieren, zu sensibilisieren vielleicht?

B: Gut, prinzipiell sollte sowas denke ich schon in Abständen aufgefrischt werden. Zum Einen gibt es da eine Fluktuation innerhalb der Mitarbeiterschaft, manche Leute scheiden aus, da kommen neue nach. So dass da auch vielleicht, naja Wissen jetzt verloren geht so will ich es nicht beschreiben aber vielleicht im Sinne wieder einer, um einen einheitlichen Stand zu schaffen durchaus von Zeit zu Zeit solche Schulungen sinnvoll sind. Ich will mich jetzt nicht festlegen in welchen Abständen man das tun sollte. Also oft ist es ja so, dass es bestimmter Ereignisse bedarf um festzustellen aha, es könnte mal wieder was notwendig sein. Und so lange nichts Schlimmes passiert sieht man vielleicht auch nicht unmittelbar den Bedarf dafür.

I: Mhm. Ja, okay. Das war es von meiner Seite. Wenn Sie nicht noch was haben, was Ihnen noch auf dem Herzen liegt, was Sie vielleicht nochmal unterstreichen wollen, dann wären wir jetzt am Ende.

B: Gut, was kann man noch sagen? Also ich weiß, dass Sicherheit natürlich auch mit oder der erreichbare Stand von Sicherheit auch irgendwas damit zu tun hat, wie viel man bereit ist in dem Bereich zu investieren. Und was das angeht kann ich guten Gewissens sagen, da wird von unserer Firma hier von DEW Stahl nicht wenig investiert. Sicherheit hat immer einen großen Stellenwert gehabt und da wo man Sicherheit hinzu kaufen muss, sei es jetzt im Bereich Virenschutz, sei es im Bereich Abschottung der Netze, sei es überhaupt im Bereich Tools für Netzwerksicherheit und dergleichen mehr, ist eigentlich nie gespart worden und die Entscheidungsträger waren bei uns

sicher immer der Meinung, dass das Geld was dort investiert wird nicht an der falschen Stelle investiert wurde. Und da hat unsere IT-Leitung also immer genug finanzielle Mittel zur Verfügung gestellt.

I: Mhm, ja. Ja okay, dann bedanke ich mich recht herzlich für das Interview.

B: Gerne.

A4

Interviewtranskript – Firma G.I.B mbH – 17.11.2014

I: Schönen guten Morgen, Herr Theis. Dann fangen wir mal an. Einleitend möchte ich Sie gerne fragen wo hier in Ihrer Firma, also hier im Unternehmen, Authentifikation eingesetzt wird, in welcher Form auch immer, und welche Technologien dafür verwandt werden, welche Mechanismen, welche Techniken?

B: Ja also ganz klassisch natürlich die Authentifizierung lokal am Notebook des Mitarbeiters, das ist dann auch gleichzeitig, insofern Netzzugang besteht, auch die Authentifizierung bei uns im Active Directory. Dann natürlich bei der Einwahl in das Firmennetzwerk, da nutzen wir eine SSL-VPN-Verbindung für Homeoffice, Kundentermine und so weiter und sofort. Und das ist dann auch eine lokale Authentifizierung an unserer Firewall, die also gleichzeitig dann das VPN-Gateway ist. Dann, jetzt muss ich ehrlich gesagt selber überlegen, in Richtung WLAN haben wir ja eigentlich keine Authentifizierung, das ist ja dann mehr die Verschlüsselung. Das war es ja wahrscheinlich, wo authentifiziert wird. Natürlich an den SAP-Systemen, klar. Da haben wir weitestgehend auch personalisierte Benutzer und vereinzelnd Programmier-Admin-User, die irgendwo doppelt genutzt werden, aber ansonsten weitestgehend personalisiert. Die restlichen Computer, also alle Anwendungen, sei es jetzt ein Ticketsystem, eine Passwortverwaltungssoftware, die Passwörter verschlüsselt ablegt für unsere Kundenverbindungen, das ist auch alles personalisiert, ein CRM-System. Also alles da, wo man auch wirklich einen personlisierten Zugang für benötigt, der auch natürlich abgesichert werden soll, findet auch eine Authentifizierung statt.

I: Mhm. Wir haben jetzt primär über interne Prozesse, über interne Kommunikation gesprochen mit den Mitarbeitern untereinander, mit den verschiedenen Systemen. Gibt es da auch extern gewisse Authentifikationen, die getroffen werden müssen? Also sei es jetzt mit Kunden oder mit anderen Firmen.

B: Ja klar. Also wir haben oder versuchen zu all unseren Kunden auch eine Remote-Verbindung zu bekommen, das ist in den meisten Fällen auch möglich. Und da haben wir eigentlich, unsere Wunschverbindung ist da eine Router-zu-Router-Verbindung, wo ja erstmal in dem Sinne keine Authentifizierung des Benutzers stattfindet sondern wo eben die Verschlüsselung und Authentifizierung dann zwischen den Maschinen stattfindet. Aber dann spätestens wenn man eben auf das SAP-System der Kunden natürlich zugreifen möchte oder muss, spätestens da ist natürlich dann auch die Authentifizierung erforderlich. Wenn das jetzt die Frage war. Ansonsten, also das klar, da haben wir natürlich auch die Authentifizierung. Ansonsten fällt mir jetzt so in diesem Zusammenhang extern wenig zu ein.

I: Gibt es da noch Besonderheiten, wenn man die externe Kommunikation betrachtet, also in der Umsetzung? Also welche Technik da zum Einsatz kommt?

B: Ja wie gesagt, also wir haben eigentlich eine, wie soll ich sagen, eine Vorlage, an die wir versuchen unsere Kunden zu binden. Das wäre halt eben einmal eine Kommunikation über einen sogenannten SAP-Router, die kommunizieren dann direkt miteinander, die Verschlüsselung erfolgt dann auch über SNC, also auch über Zertifikate, oder eben über eine VPN-Verbindung, die aufgebaut wird. Aber eben Router zu Router, also nicht irgendwo Client zu Client oder Client zu Router oder sowas, so dass wir da eigentlich mit unseren Authentifizierungmethoden überall gleich unterwegs sind. Wir haben natürlich auch Kunden, die uns versuchen oder es auch erfolgreich schaffen deren Verbindungsvarianten aufzudrücken sag ich mal, das heißt das wären dann auch

irgendwelche Client-Verbindungen. Und da gibt es dann auch die unterschiedlichsten Authentifizierungsmethoden, also das geht von einem Hardware-Token, also hier One-Time-Password, das geht dann über Software-Token, wo auch irgendwo ein Programm im Hintergrund läuft, über SMS-Token, also da gibt es die verschiedensten Varianten, die dann die Kunden nutzen. Da haben wir halt aktuell noch immer einige dieser Varianten im Umlauf, die meisten sind sicherlich dann das klassische Hardware-Token, was dann eben nochmal ein Passwort generiert. Aber wie gesagt, das versuchen wir eben weitestgehend abzublocken, weil das aus unserer Sicht oder für unseren Betrieb sehr schlecht zu handlen ist. Wir müssen ja Support leisten für unsere Software, die beim Kunden läuft, haben inzwischen ein recht großes Support-Team, wir haben Support-Zeiten vierzehn Stunden am Tag. Das heißt lange Zeit viele Leute, wo es dann eben administrativ sehr schwierig ist, diese verschiedensten Client-Lösungen am laufen zu halten und auch allen Support-Mitarbeitern zur Verfügung zu stellen. Also wenn wir jetzt das klassische Hardware-Token nehmen, was dann ein kleines Gerät ist was irgendwo liegt und wir haben Kollegen, die irgendwo aus dem Home-Office arbeiten oder spät abends früh morgens auf das System müssen, die brauchen ja wirklich Zugang zu diesem Token. Und da ist es dann eben für uns schwer zu handlen, deswegen wollen wir eben auf diese Router-zu-Router-Kommunikation, dass also der Client oder der Benutzer an sich mit der Sache garnichts zu tun hat. Der Verbindungsaufbau geschieht im Hintergrund und erst wenn er sich am SAP-System authentifizieren muss dann kommt eben der Client, der User wieder ins Spiel, der dann sein Kennwort eingeben muss.

I: Okay, gut. Ich sage mal die notwendigen Eigenschaften, die ein Nutzer nachwiesen muss, also die Anforderungen, die gestalten sich dann so wie gerade beschrieben, also dass es im Endeffekt auf Benutzername Passwort hinausläuft.

B: Genau.

I: Oder gibt es da noch tiefere Anforderungen an die Identität von gewissen Personen? Verschärfende Maßnahmen eventuell noch? Also dass jemand zum Beispiel gewisse Eigenschaften nachweisen muss, bevor er sich wirklich erfolgreich authentifizieren kann, also neben Passwort.

B: Wäre mir nicht bekannt. Also um ein Kennwort oder einen Zugang zu beantragen, da gibt es dann sicherlich verschiedene Wege wieder. Das geht dann über ich sag jetzt mal Geheimhaltungserklärungen, die wir zentral von der Firma aus unterschreiben können, die gilt dann für die komplette Firma. Andere Kunden wollen das auch personenbezogen, also da muss dann jeder Kollege, der irgendwie Zugang auf das SAP-System haben möchte oder haben muss, um diesen Benutzer zu beantragen irgendwo nochmal was unterschreiben, wirklich mit dem Kulli. Aber wenn der Zugang eigentlich dann existiert dann haben wir eben nur das klassische SAP-Logon und das ist dann ganz klassisch Username und Passwort. Also da haben wir eigentlich nichts anderes.

I: Okay. Dann möchte ich gerne noch als nächstes zu sprechen kommen auf gewisse Vorgaben. Gibt es im Unternehmen Vorgaben, was in Richtung IT-Security passieren muss, was jetzt speziell Authentifikation betrifft und wenn, wir werden die umgesetzt innerhalb des Unternehmens?

B: Also was jetzt ganz rein die Authentifizierung betrifft eigentlich nur was mir jetzt spontan einfällt, dass eben unser Domänen-Kennwort für die Active Directory, da muss ich ehrlich gestehen müsste ich nachgucken, aber eine gewisse Zeit lang regelmäßig abläuft, dass also die Benutzer gezwungen werden das Kennwort zu ändern und dann ganz klassische Kennwortrichtlinien, wobei da ist jetzt aktuell auch eine Baustelle, die wir aktuell haben. Wir haben die Richtlinien sehr gering gehalten, also ich glaube es sind wirklich nur acht Zeichen und Zahlen, also jetzt nicht irgwendwo

noch mit Sonderzeichen oder Groß- und Kleinschreibung oder sowas. Das werden wir aber in Zukunft ändern, weil wir gerne diese Active-Directory-Authentifizierung auch an die Firewall anbinden möchten, so dass sich also wirklich um hier ins Firmennetzwerk zu kommen, wo momentan eben nur eine Https-Seite aufgerufen wird und dann User und Kennwort aber ansonsten keine weitere Authentifizierung, und da möchten wir dann wenn wir das nutzen auf jeden Fall auch sichere oder sicherere Kennwörter verwenden, also da nicht nur sechs Zeichen das wars oder acht Zeichen sondern schon irgendwo nochmal mit Groß- und Kleinschreibung und dergleichen. Und da überlegen wir auch mit Zertifikaten zu arbeiten, so dass also bei dem Kollegen, der sich einwählt, auch tatsächlich ein Zertifikat installiert sein muss. Das ist aber jetzt aktueller Stand noch Zukunftsmusik, was heißt Zukunftsmusik, also wir wollen es schon gerne ich sag mal in dem nächsten Quartal irgendwo realisieren, in den nächsten drei vier Monaten, aber haben wir halt aktuell noch nicht. Und diese Zertifikate eben, um so ein bisschen auch zu steuern, welche Geräte sich bei uns einwählen, also momentan ist es wirklich so, dass Kollegen, die einen PC irgendwo zu Hause stehen haben, der irgendwo nicht durch uns gewartet wird oder sowas, können die sich hier einwählen. Sie brauchen nur eben diese Https-Seite aufzurufen, User Kenntwort haben sie ja und das wars. Und wir planen das dann eben mit Zertifikaten zu regeln. Es gibt da wohl Zertifikate, die importiert aber dann auch nicht mehr oder nur mit sehr sehr großem Aufwand wieder exportiert werden können, so dass wir dann eben eine Übersicht haben, oder was heißt eine Übersicht, so ein bisschen in der Hand haben, welcher Benutzer wählt sich auch mit was für einem Client ein. Weil da haben wir momentan wirklich die Regelung, dass wir hier Arbeiten im Firmennetzwerk, es gibt wie überall natürlich immer Ausnahmen, aber weitestgehend nur mit Firmen-Notebooks auch realisiert werden sollen und um da so ein bisschen auch das zu kontrollieren wollen wir das so machen.

I: Um gerade nochmal kurz auf die Umsetzung zu sprechen zu kommen, wie sähe da so ein Ablauf aus? Also wenn jetzt neue Vorgaben definiert würden, von wo würde das gesteuert beziehungsweise wie würde dann die Umsetzung aussehen?

B: Also wir sind da jetzt so vom Unternehmen her eigentlich so strukturiert, dass wir da in der IT weitestgehend freie Hand haben was wir umsetzen oder auch was für Kennwortrichtlinien wir da vergeben zum Beispiel. Und das würde dann bei uns auch wirklich ganz, wie soll ich sagen, unkompliziert durchgesetzt, dass wir also dann zum Beispiel die Kennwortrichtlinien von heute auf morgen dann auch ändern können. Das ist natürlich vom Prinzip, vom Prozedere keine komplizierte Sache, ob mein Kennwort jetzt sechs Zeichen, acht oder fünfzehn sein muss oder soll, das kann man einstellen und gut ist. Wenn man dann natürlich das mit den Zertifikaten auch wirklich umsetzen möchte, da spielen natürlich noch andere Faktoren eine Rolle. Baut man eine eigene CA intern auf, um eben diese Zertifikate, die man ja im Prinzip nur für die interne Kommunikation benötigt, kann man die dann selber signieren oder ausstellen oder greift man dort auf mal vorsichtig ausgedrückt professionelle CAs zurück. Also das muss man dann irgendwo in einer Testphase sicherlich mal so ein bisschen eroieren, Kostenfaktor Nutzenfaktor ganz klassisch gegenüber stellen und dann wird das in einer Testphase mal so auf Alltagstauglichkeit getestet und dann auch umgesetzt. Also so die Reihenfolge.

I: Okay. Sie sprachen jetzt eben schonmal von den Zertifikaten, die Sie intern gedenken einzuführen. Fallen Ihnen da jetzt spontan noch weitere Technologien oder Systeme oder Techniken ein, die Sie sich vorstellen könnten, die Sie in Zukunft eventuell einsetzen möchten oder könnten.

B: Ja. Also schon so diese One-Time-Passwords, was weiß ich, jetzt auch wieder das klassische Hardware-Token ist auch bei uns natürlich im Gespräch. Ich sag mal sobald man ja den Zugang nur für Kollegen gewährleisten möchte ist das ja auch wirklich ein gangbarer Weg, jeder Kollege

bekommt so ein Teil in die Hand, was er dann an sein Schlüsselbund machen kann, wie auch immer. Das kann man ja handlen, das kann man ja auch administrieren. Wir haben natürlich was ich jetzt eben sagte, wo uns natürlich die Kunden diese Dinger aufs Auge drücken, wo wir als Lieferant das Problem haben das zu administrieren, so haben wir natürlich auch Lieferanten, die bei uns auf das System wollen oder müssen. Und denen wollen wir natürlich dann auch nicht irgendwo diese Tokens dann aufs Auge drücken, weil gerade wenn man Firmen hat, Liferanten hat, wo doch ein ganzes Team irgendwo an einem Projekt arbeitet, finde ich das jetzt nicht irgendwo alltagstauglich mit diesen Tokens. Weil wenn ich eben fünf Leute habe muss ich denen auch wieder fünf Tokens in die Hand drücken. Also deswegen suchen wir da an einer Möglichkeit da ein bisschen drum rum zu kommen oder ob man eben sagt naja gut, der Lieferant bekommt ja eh nur einen temporären Zugang, der braucht dann von mir aus nur User und Kennwort und der Kollege, der dauerhaften Zugang benötigt, der muss eben User Kennwort plus OTP eingeben. Also sowas, eine Mixform wäre da denkbar. Aber ansonsten wollen wir es natürlich auch irgendwo versuchen nicht zu kompliziert zu halten, dass man da erst nochmal hier anrufen muss und sich stimmlich authentifizieren oder weiß der Henker was. Also da wollen wir natürlich schon irgendwo auch so alltagsfreundlich bleiben, dass man das nicht irgendwie unnötig verkompliziert. Also unterm Strich User, Kennwort, Zertifikat und maximal dann noch einen Token dabei, also so ein OTP. Das wäre noch sicherlich denkbar für die internen Kollegen.

I: Okay. Darauf aufbauend, wie zufrieden sind Sie mit der aktuellen Lage, also mit der aktuellen Umsetzung? Gibt es da in Ihren Augen Lücken?

B: Ja gut ich sag mal so, für die interne Authentifizierung, was ich jetzt eben mit den AD-Kennwörtern, da sind wir vielleicht sicherlich nicht so up-to-date. Da gibt es sicherlich schon Kennwortrichtlinien, die ein bisschen sicherer sind, wobei wir da aktuell sagen okay, jemand der jetzt wirklich über dieses Kennwort hier ins Netzwerk gelangen möchte, braucht ja erstmal physikalischen Zugang zu unseren Räumlichkeiten, weil wir eben aktuell noch bei der Firewall-Authentifizierung doch höhere Kennwortrestriktionen haben. Spätestens dann, wenn wir das verknüpfen wollen, Stichwort Single-Sign-On oder eben ein User ein Kennwort für alle Zugänge, spätestens dann werden wir auf jeden Fall da was anpassen müssen, welche zusätzlichen Authentifizierungmaßnahmen wir noch dazu nehmen sei mal außen vor. Aber gerade mal das reine Kennwort, das werden wir also auf jeden Fall noch verschärfen müssen, wenn wir das wollen. Ansonsten, wie gesagt die Remote-Einwahl, das wäre ja dann auch mit ein Angriffspunkt, wo man wirklich so ein bisschen mal drauf achten sollte. Da fahren wir unserer Meinung nach ganz gut, weil wir eben da eine relativ hohe Kennwortsicherheit irgendwo auch etablieren. Aber es wird sich immer was anpassen in Zukunft und da müssen wir halt irgendwo auch mit der Zeit gehen, klar.

I: Ja. Also wenn Sie jetzt einfach mal spontan sagen müssten, wie in Ihren Augen so die optimale Lösung aussehen würde, also jetzt mal losgelöst vom Unternehmen oder von der ganzen Struktur oder der Umsetzbarkeit. Fällt Ihnen da spontan was ein was Sie gerne hätten?

B: Tja, also unabhängig von der Umsetzbarkeit finde ich es immer ganz gut, wenn man weiß welche Personen sich in das Firmennetz einwählen. Also ich beziehe mich jetzt auch da primär auf die Einwahl im Firmennetz. Wie gesagt, intern haben wir auch eine Unternehmensgröße, wo das glaube ich auch von unserer Struktur überschaubar ist, die Gefahren, die jetzt irgendwo vom internen Netz ausgehen, also von extern, da sind wir natürlich wie jeder andere auch betroffen, deswegen da der Schwerpunkt drauf. Also wenn man sich da was wünschen dürfte, ich persönlich finde es immer ganz gut, wenn man wirklich weiß welche Personen sich einwählen und welche Geräte sich einwählen. Also ich sage mal Stichwort Bring-Your-Own-Device oder sowas in der Art, dass man da jetzt irgendwo die Türen offen macht für alle Geräte, soweit, mal vorsichtig

ausgedrückt, sind wir halt bei uns noch nicht. Also da finde ich es immer ganz gut, das Notebook wählt sich ein, da bin ich mir sicher da ist ein aktueller Virenscanner drauf, da bin ich mir sicher da sind die aktuellsten Betriebssystem-Patches drauf auf dem Rechner. Und wenn man eben sowas abfangen kann, das wäre halt ganz gut. Und natürlich irgendwo von der Authentifizierung diese Geschichte, dass ich da wirklich sagen kann okay, nur der der das Zertifikat im Bauch hat darf sich pauschal hier einwählen, der kommt überhaupt erst auf die Login-Maske. Oder eben alternativ das One-Time-Password, dass ich jetzt sage okay, das ist auch nochmal mit einer erhöhten Sicherheit, weil es eben nur ein paar Sekunden gültig ist, was weiß ich. Also das sind so die Dinge, aber die glaube ich auch, also da geht meine Phantasie auch von der Realisierbarkeit glaub ich nicht weit auseinander. Also da würde ich mir nichts utopisches wünschen, das ist auch glaube ich alles zu realisieren.

I: Okay. Darauf nochmal aufbauend, auch auf alternativen Systemen oder Mechaniken, könnten Sie sich vorstellen an Stelle von herkömmlichen Authentifizierungmethoden, wie sie jetzt im Moment noch eingesetzt werden oder im Einsatz sind, dass man so eine Art Netz aufbaut, in dem sich Nutzer, also im Endeffekt Mitarbeiter oder auch Kunden oder wer auch immer jetzt beteiligt ist an dem Netz, dass die sich gegenseitig authentifizieren beziehungsweise gegenseitig ihre Identität bestätigen, also dass das Ganze mehr auf Vertrauen basiert? Also dass jetzt meinetwegen Mitarbeiter A sagt ja, ich kenne Mitarbeiter B also ist der vertrauenswürdig.

B: Also da fehlt mir jetzt gerade so der Praxisbezug ehrlich gesagt, wie das jetzt gemeint ist. Also was heißt jetzt der Mitarbeiter A...?

I: Also ein Beispiel wäre die Firma kennt jetzt meinetwegen Lieferant A und Lieferant A wiederum sagt aber hier, Lieferant B oder Mitarbeiter B den kenne ich, ich verifiziere seine Identität also vertraut die Firma oder das Unternehmen automatisch auch diesem Mitarbeiter. Würde sich das irgendwo umsetzen lassen?

B: Also spontan muss ich sagen fällt mir da jetzt so wie gesagt nicht so der Praxisbezug ein. Wir haben natürlich auch Kunden, die irgendwo vernetzt sind, ich sage mal wir haben auch einige Konzerne in unserem Kundenbereich, wo man sicherlich auch sagt man nutzt die Infrastruktur des Kunden A um eben auf die Systeme des Kunden B zuzugreifen. Wenn das jetzt in die Richtung geht, weiß ich jetzt nicht. Das ist sicherlich aus unserer Sicht auch denkbar, sowas in der Art. Wobei wir ja im Prinzip zum größten Teil immer ausgehende Verbindungen haben zu unseren Kunden. Und ich sage mal so, wenn ich jetzt im Kundennetz bin und komme über Kunden A auf die Systeme von Kunden B, dann ist mir das ja egal über welche Systeme ich dann gehe, weil die Verbindung aus unserer Sicht primär nur ausgehend ist. Gut, sicherlich kann auch da der Hacker an sich, der kann vielleicht auch mit den Verbindungen was anfangen aber ich sage jetzt erstmal klassisch ist es nur einseitig. Ich würde mir sicherlich mehr Gedanken darüber machen, wenn wir auch eingehende Verbindungen auf unsere Systeme hätten. Und wenn jetzt dort eben unser Lieferant A, ohne dass wir das jetzt irgendwo steuern oder controllen können, auf einmal einem unbekannten Lieferanten B den Zugang auf unsere Systeme gewährt, dann muss ich sagen so spontan wäre ich dann sicherlich ein bisschen skeptisch. Wobei, ich persönlich kann das jetzt nicht so pauschalisieren ehrlich gesagt. Mir fällt jetzt spontan auch da ein Beispiel ein, dass wir jetzt sicherlich in Zukunft irgendwann ein Projekt haben, wo eben zwei Lieferanten für uns arbeiten und wir einen Lieferanten jetzt schon kennen, Lieferant B durch Lieferant A empfohlen wurde, wo ich dann natürlich als Unternehmen dann auch sage okay, wenn die beiden sich kennen ist da schon mal eher pauschal sicherlich eine höhere Vertrauensstellung da als wenn man den Lieferanten jetzt garnicht kennen würde. Das stimmt schon, aber ob ich dem jetzt wirklich da jetzt direkt den Zugang gewähren würde nur weil ich jetzt den Lieferanten A kenne, das weiß ich ehrlich gesagt nicht. Also wenn die Fragen jetzt in

die Richtung zählen, wobei wie gesagt da fehlt mir so ein bisschen der Praxisbezug, um da jetzt was zu sagen zu können.

I: Also sehen Sie da schon Probleme bei der ich sage mal unternehmerischen Umsetzung?

B: Ja wie gesagt, also aus jetziger Sicht kann ich der Sache entspannt entgegen sehen, weil wir eben primär Verbindungen ausgehend haben und dann sehe ich das immer so, dann muss sich eben der Kunde darum kümmern, dass ich nicht auf irgendwelche Systeme drauf komme auf die ich nicht drauf kommen soll. Bei eingehenden Verbindungen, dann bin ich ja der, der vielleicht irgendwo geschädigt werden kann, dann muss ich mich halt drum kümmern und da wäre ich dann schon etwas skeptisch, wenn ich nicht genau irgendwo wüsste wer auf unsere Systeme zugreifen kann.

I: Mhm. Gut, wenn wir gerade mal vielleicht die Brücke schlagen zur internen Kommunikation, dass man das vielleicht unter Mitarbeitern einführt oder auch unter Besuchern? Wenn jetzt meinetwegen ein Mitarbeiter Interessenten oder Kunden oder Besucher mitbringt und sagt jawoll, der ist vertrauenswürdig, würde man da differenzieren ob man jetzt intern kommuniziert oder ob es dann halt wirklich um Externe also um Lieferanten geht oder um Kunden oder was auch immer?

B: Gegenfrage, das heißt jetzt in dem Beispiel kann ich mir jetzt die Frage so vorstellen, wir haben, keine Ahnung, morgen einen Interessenten bei uns im Haus zu einem Workshop, keine Ahnung. Da sind jetzt Kollegen mit im Raum anwesend und die erlauben jetzt hier in unserem Schulungsraum, dass sich jetzt der Interessent hier in das Netzwerk reinhängt. Ist das jetzt in die Richtung gemeint oder wie ist jetzt ...?

I: Ja, grob schon. Also im Endeffekt würde es dann so aussehen, dass meinetwegen der Mitarbeiter dann sagt jawoll, jetzt mal in IT gesprochen, ich signiere so und so, dass die Identität von dem Interessenten in dem Fall jetzt oder er ist vertrauenswürdig und dass dadurch dann automatisch seitens des Unternehmens gesagt würde okay gut, wenn der das sagt, dann darf der auch auf das System. Also es würde natürlich immer noch vom Unternehmen abhängig sein aber das wäre jetzt so ein Beispiel.

B: Ja. Also da muss ich ehrlich sagen, das weiß ich nicht, ob das jetzt irgendwo so praktikabel ist. Wenn ich mir das jetzt wirklich so praktisch vorstellen kann, dass jetzt der Interessant, der besagte sich jetzt hier ins Netzwerk hängt und der Kollege muss das dann freischalten, das ist sicherlich momentan bei uns in der Praxis so gehandhabt, weil wie ich das eben schonmal sagte, hier intern haben wir keine großen Sicherheitsrichtlinien. Also wenn jetzt hier ein Interessent Zugang zu unseren Räumlichkeiten hat und der hängt sich jetzt hier in das Netzwerk, dann ist der im Netzwerk drin. Also der muss sich hier im Netzwerk nicht mehr authentifizieren.

I: Okay.

B: So, deswegen haben wir ja sowas noch nicht mal, dass wer jetzt irgendwas freischalten muss. Aber wenn man jetzt mal weiter denkt und man hätte jetzt irgendwo in der Praxis die Situation, dass der Kollege erstmal den Zugang freischalten muss für diesen Kunden oder Interessenten und das Unternehmen ist so aufgestellt, dass man den Zugang darüber kontrollieren möchte, dann fände ich es einen nicht-praktikablen Weg, weil wenn ich ein Unternehmen bin, was eben solchen Zugängen misstraut und nur, dass jetzt derjenige sich kennt oder sonstwas, dieser Zugang freigeschaltet wird, der weiß ja garnicht was nutzt der für Hardware, was nutzt der für Client-Software was weiß ich, die jetzt hier irgendwo Schaden anrichten kann. Also wie gesagt nochmal vielleicht, wir haben diese Sicherheitsrichtlinien sowieso nicht, wenn jemand Zugang zu unseren Räumlichkeiten hat, der hat

Zugang auch zum Netzwerk. Deswegen trifft das bei uns jetzt eh glaube ich nicht so zu aber wenn wir das restriktieren würden und man müsste sich authentifizieren, wenn man hier irgendwo das Patch-Kabel einsteckt, dann würde ich es schon so machen, dass man entweder einen Gastzugang hier irgendwo etabliert, wo man jetzt nichts Böses anstellen kann oder sowas, aber dass jetzt da ein Kollege, der jetzt irgendwo das entsprechende Know-How garnicht sowas zu bewerten, dass der das jetzt irgendwie freischaltet, da hätte ich jetzt glaube ich ein ungutes Gefühlt bei.

I: Ja okay. Dann möchte ich gerne als Nächstes noch auf einen anderen nicht ganz davon losgelösten Themenbereich, aber den würde ich gerne nochmal gezielt beleuchten, und zwar das Ganze aus Nutzersicht. Also wenn wir uns jetzt wirklich mal so den Faktor Mensch sag ich mal angucken in der ganzen Situation, also im ganzen Authentifizierungs- und IT-Sicherheitsprozess. Gut, wir haben schon darüber gesprochen, wo die Nutzer im Endeffekt damit in Berührung kommen, aber wie gestaltet sich aus Ihrer Sicht die Anwendung dieser eingesetzten Methoden? Also wie schätzen Sie die Anwendbarkeit, die Usability im Endeffekt ein? Gibt es da Probleme, zum Beispiel bei der Nutzung? Also wie gestaltet sich da so die Nutzerperspektive?

B: Ja also, wie gesagt jetzt auch da Ist-Zustand bei uns, was vielleicht so ein bisschen ein Kritikpunkt des Anwenders sein kann, wo man Optimierungsbedarf hätte, ist sicherlich so das Stichwort Single-Sign-On. Ja, dass ich jetzt irgendwo sage okay, morgens komme ich hier hin, ich muss mich dann natürlich irgendwo einmal authentifizieren, dass ich auch der bin der ich vorgebe zu sein mag. Und dann kann man sicherlich da irgendwo einen Automatismus einrichten, dass ich mich nur einmalig anmelde und auf allen anderen Systemen, die ich während meines Arbeitstages nutze, wird dann eben dieses Login weitergereicht. Sowas in der Art kann man sicherlich bei uns auch optimieren aber ich glaube im Vergleich zu anderen Unternehmen, größeren Unternehmen, die auch irgendwo kritischere Anwendungen vielleicht haben, haben wir was das Stichwort Authentifizierung angeht jetzt keine unnötige Verkomplizierung, so dass jetzt sicherlich bei uns der Anwender ich sage mal so ganz salopp sich nicht beschweren kann. Also wir sind da schon sehr anwenderfreundlich glaube ich. Was wir jetzt eben schonmal sagten eben diese Authentifizierungmethoden, die wir vielleicht in Zukunft noch einführen werden, weil auch da sicherlich die Anforderungen immer wieder sich ändern, da ist dann irgendwo klar, wenn ich mich einwähle und muss immer nochmal mein Token ablesen, keine Ahnung, was eine fünfzehnstellige Zahl ist oder sowas, das ist dann vielleicht irgendwo noch geht natürlich in Anwenderunfreundlichkeit. Aber auf der anderen Seite ist das glaube ich noch vertretbar. Wenn ich jetzt irgendwo sagen muss okay, ich muss jetzt hier erst auf der Firma anrufen und sagen schaltet mich frei und dann muss ich nochmal einen Token eingeben und noch fünf mal auf Enter drücken und sieben mal auf irgendwas, dann hat man irgendwann die Stufe erreicht wo man sagt das steht jetzt vielleicht nicht mehr in einer Relation zu einem Unternehmen, was jetzt vielleicht nicht unbedingt in der Rüstungsindustrie tätig ist oder sowas. Die haben vielleicht berechtigterweise ein bisschen höhere Anforderungen was die Authentifizierung angeht. Wir haben zum Beispiel einen Kunden das ist die Bundesdruckerei, die also das Geld drucken und die Personalausweise herstellen. Da haben wir natürlich keinen Systemzugang auf deren Systeme. Die haben natürlich ganz andere Anforderungen. Da bin ich persönlich auch froh, dass wir da keinen Zugang haben, weil mein Personalausweis da auch gedruckt wird und ich auch gerne möchte, dass die da sensibel mit den Daten umgehen. Also die haben dann vielleicht wirklich ein berechtigtes Interesse, dass dann wirklich niemand auf das System kommt. Auf der anderen Seite haben wir Kunden, die irgendwas 0815-Produkt herstellen sag ich mal. Da ist das vielleicht dann wieder ein bisschen zu überspitzt. Also da muss man halt einfach gucken was mach ich in meinem Unternehmen, was kann bei mir überhaupt geklaut werden, vor was muss ich meine Systeme schützen. Aber da sind wir jetzt hier glaube ich auf einem ganz guten Weg was ich jetzt mal behaupte.

I: Daraus abgeleitet, also sehen Sie auch nicht gewisse Risiken, dass es gewisse Abkürzungen in der Authentifizierung gibt, also dass Nutzer vielleicht dazu neigen, das irgendwie zu umgehen oder auszuhebeln, um es halt im Endeffekt gemütlicher zu haben?

B: Ja klar. Also das mag durchaus so sein, wenn ich jetzt eben auch nochmal an meine klassische Kennwortrestriktion denke. Wir haben das eben alle paar Monate muss das Kennwort geändert werden, viele nutzen das dann eben, dass sie dann was weiß ich an das Kennwort noch hinten eine Ziffer dran packen und diese Ziffer jedes mal hochzählen. Aus meinem Grundkennwort Spinat wird dann Spinat eins zwei drei fünf X was weiß ich, was man dann vielleicht irgendwo auch umgehen kann über irgendwelche Restriktionen. Und je mehr ich natürlich von einem Kennwort irgendwo abhängig mache, Stichwort Single-Sign-On, desto komplizierter muss ich natürlich mein Kennwort machen um eben dem vorzugreifen, dass meine Kollegen da versuchen das irgendwie zu umgehen. Auf der anderen Seite, wenn ich ja irgendwo eine Authentifizierung einrichte im Unternehmen als Administrator, dann muss sich mein Kollege ja dran richten. Wie gesagt, was mir jetzt so bei diesem Aushebeln nur spontan einfällt ist, dass man natürlich irgendwo versucht die Kennwort oder den Sinn dieser Kennwortrestriktionen zu umgehen.

I: Ja.

B: Indem man jetzt sagt naja, ich muss zwar jedes Mal mein Kennwort ändern aber ich zähle einfach nur die Zahl hoch, was ja dann dem Kennwortändern entspricht aber eigentlich vielleicht dem Grundgedanken nicht, dass man vielleicht sein Kennwort auch zumindest mal alle paar Mal komplett ändern sollte. Aber ansonsten fällt mir da jetzt spontan nichts ein, was in die Richtung geht.

I: Vielleicht nach außen hin? Fällt Ihnen da spontan irgendwas ein oder halten Sie die Lösung was die Nutzer angeht schon für relativ sicher?

B: Tja, also es gibt immer was sichereres. Es gibt immer was, was man besser machen kann. Wo wir halt auch regelmäßig natürlich irgendwo versuchen auch Dinge, die irgendwo unserer Meinung nach Sinn machen, auch umzusetzen. Also ich kann nicht verhindern, dass jetzt ein Kollege sein Kennwort, was dann vielleicht laut Richtlinie aus fünfzehn Zeichen besteht, aus groß und klein das sicherste Kennwort dieser Welt ist, aber ich kann halt nicht verhindern, dass der sich es auf ein Blatt Papier schreibt und an den Monitor heftet. Was will ich machen, kann ich nicht. Kann ich dann natürlich irgendwo sagen naja, es ist zwar schon schlimm genug, dass er es macht, aber wenn ich eben mein One-Time-Password habe dann soll von mir aus der böse Kunde, der dann das Kennwort irgendwo sieht oder der Dieb, der mein Notebook klaut und das Kennwort am Monitor hängen hat, der soll das dann von mir aus klauen aber er brauch ja noch mein fünfzehnstelliges Token. Von daher habe ich das so ein bisschen ausgehebelt. Also das sind sicherlich so Punkte, wo auch bei uns eben dieser Optimierungsbedarf da ist oder Optimierungspotential da ist. Aber irgendwo, ja, ab und zu greift ja auch das Stichwort die Intelligenz sitzt vor dem Computer, also irgendwo muss ich dann auch an die Sensibilität der Kollegen dann auch appellieren, dass ich dann irgendwo sage ja gut, bitte geht auch sensibel mit euren Kennwörtern um. Aber sicherlich, Username und Kennwort als alleinige Authentifizierung ist optimierungsbedürftig, das haben wir auch bei uns erkannt, also wie ich schon eben mal erwähnt habe, das werden wir auch irgendwo in Zukunft ändern bei uns. Und dann ist aber auch gut, also wie gesagt da noch tiefere Sachen zu gehen also das wollen wir bei uns vermeiden.

I: Sie sprachen jetzt gerade schon die Sensibilität oder die Sensibilisierung der Nutzer an. Wie schätzen Sie denn so allgemein den Umgang der Nutzer mit dem ganzen Thema IT-Sicherheit,

digitaler Sicherheit, also wie schätzen Sie das Bewusstsein der Nutzer ein?

B: Potential nach oben ist vorhanden.

I: Okay, ja.

B: Nein, also das ist halt auch glaube ich durch die ganzen Medien, die ganzen Nachrichten, die in dieser Hinsicht kommen, dass Accounts gehackt werden und so weiter und sofort, das sensibilisiert schon die Leute, ganz klar. Aber ich glaube eben, dass dort auf jeden Fall Potential nach oben besteht, nicht nur bei der GIB oder den Mitarbeitern der GIB sondern bei wahrscheinlich einem Großteil der Bevölkerung, die irgendwo mit IT zu hat ob privat oder geschäftlich. Weil das erleben wir also tatsächlich, dass Kollegen die Kennwörter auf der Tastatur liegen haben, am Monitor kleben haben, irgendwo in einer Excel-Tabelle, ein Kollege hatte auch immer sein Notepad, sein Text-File wo er die ganzen Zugänge abgespeichert hat. Dann sagte ich auch überlege doch mal ob das so sinnvoll ist. Ja er hat es aber auch ganz versteckt irgendwo abgelegt. Ja sage ich, dann lass mich mal gucken und ich bin kein Hacker und man konnte halt ganz normal ganz klassisch über zuletzt geöffnete Dokumente und dann hatte man sehr schnell diese ganz versteckt abgelegte Datei geöffnet. Also da ist sicherlich noch Potential nach oben und da müssen wir als IT-Abteilung natürlich auch Hilfestellung geben, wie zum Beispiel diese passwortgeschützte Datenbank die wir haben, wo unsere Zugänge dann abgelegt werden, wo jeder Kollege einen einzelnen eigenen Bereich hat, wo auch nur er Zugriff hat, wo er also seine privaten Kennwörter von mir aus sogar oder eben seine Firmenaccounts pflegen kann. Also so versuchen wir dann immer auch Hilfestellung den Kollegen zu geben und das halt auch so einfach wie möglich zu machen, dass man also diese Datenbank dann auch mit einem Smartphone abrufen kann, wenn man gerade beim Kunden ist und garnicht erst in Verlegenheit kommt oder garnicht erst auf die Idee kommt, sein Kennwort in einer Excel-Tabelle im Klartext abzulegen, weil er jederzeit eben auf diese gesicherte Datenbank Zugriff hat. Also so versuchen wir sicherlich auch unsere Kollegen zu sensibilisieren, auch regelmäßig nochmal darauf hinzuweisen hier, wenn ihr den Arbeitsplatz verlasst, dann sperrt doch gerade mal euer Computerkonto. Oder gerade wenn ihr beim Kunden seid, sperrt doch gerade mal eure Computerkonten damit man halt da einfach das Bewusstsein schafft. Aber wie ich eben gerade sagte, also da ist sicherlich Luft nach oben, also da könnten auch wir sicherlich mehr tun an der Stelle. #

I: Das als Überleitung mal genommen, abschließend noch das Thema Schulungen, also Schulungsmaßnahmen jetzt gerade im Bereich Authentifikation aber auch übergeordnet sage ich mal IT-Security. Wie sieht es da aus mit den Schulungen, also wurde da in der Vergangenheit schon was realisiert oder ist vielleicht was in der Planung oder ist da nicht so ganz der Bedarf?

B: Der Bedarf sicherlich schon. Also das sicherlich schon, es ist aber schulungsmäßig noch nichts gelaufen in der Richtung. Wir machen das immer so am Arbeitsplatz des Kollegen. Sagen wir mal als Beispiel, wenn die Kollegen Software installiert haben, wobei wir das auch aktuell einschränken, dass also die Kollegen auch nichts mehr installieren können auf den Notebooks, weil es da in der Vergangenheit auch passiert ist, wenn man mal ein kleines Freeware-Tool installiert, jeder kennt das, da werden wieder acht neue Suchleisten im Internetexplorer installiert, so dass die Kollegen nur noch ein Fenster von fünf mal fünf Zentimeter frei haben, weil der Rest nur noch aus Suchleisten besteht. Also da versuchen wir dann direkt im direkten Kontakt mit dem Kollegen zu sensibilisieren und zu sagen hier hör mal, du kannst dir auch durchaus mal irgendwas installieren, was nicht so gut ist. Was wir halt machen ist sicherlich, wir haben im vier Wochen, oder was weiß ich sechs acht Wochenrhythmus unsere Mitarbeiterversammlungen, wo wir immer mal wieder auch mal kurz sagen hier Leute denkt daran, wählt sichere Kennwörter, was ist ein sicheres Kennwort, so

diese Punkte. Das ist aber nicht wirklich irgendwo mit einem Konzept dahinter, das machen wir dann, wenn wir irgendwo feststellen, meistens wenn wir feststellen oh da hat wieder ein Kollege sein Kennwort irgendwo im Klartext abgelegt und dann werden wir bei der nächsten Mitarbeiterversammlung nochmal kurz aufstehen und sagen hier Leute, denkt doch bitte daran legt es in der Passwortdatenbank ab, weil da ist es verschlüsselt und so weiter. Aber da machen wir jetzt nichts irgendwie regelmäßig oder sowas, also da ist sicherlich von unserer Seite auch ein bisschen Optimierungsbedarf.

I: Mhm. Gibt es da schon konkrete Pläne?

B: Nein.

I: Noch garnichts?

B: Nein garnichts. Also das ist, lediglich in dem Zusammenhang wird das vielleicht auf die Tagesordnung kommen was ich mehrmals jetzt schon sagte, dass wir eben an den Authentifizierungsrestriktionen, an den Passwortrestriktionen was ändern werden, das wird also so passieren. Und in dem Zusammenhang könnte das sicherlich mal auf die Tagesordnung kommen. Aber so konkret geplant ist da noch nichts.

I: Und sehen Sie konkret jetzt da Bedarf? Also wie wäre das nach Ihrer Meinung am Besten zu gestalten?

B: Also wenn wir da nur mal der kompletten Überschrift IT-Security, wie gesagt da sind wir aktuell dabei die Computerkonten auf den Laptops so einzuschränken, dass man zum Beispiel eben nichts mehr installieren kann ohne ein Administratorpasswort zu haben. Das setzen wir momentan um, das hilft uns auch meiner Meinung nach stark weiter. Einmal natürlich was die Gefährdung angeht, Viren, Malware, Phishingware was weiß ich was. Aber natürlich auch was unseren Supportaufwand angeht. Also wir haben sicherlich ein Großteil unserer Kollegen ist IT-affin sag ich mal, das sind halt alles irgendwo ITler, wir sind halt ein IT-Dienstleister. Das heißt wo wir in der Vergangenheit auch den Bedarf nicht hatten großartig was aus unserer IT-Abteilung zu verteilen, irgendwelche Restriktionen, weil wir eben viele Kollegen haben die auch selber IT-Spezialisten sind. Aber inzwischen haben wir immer mehr Kollegen die auch bei uns im Innendienst arbeiten, das ist jetzt nicht negativ gemeint, also Kollegen die bei uns in der Verwaltung arbeiten, im Vertrieb arbeiten, die halt einfach Anwender sind. Das ist echt wirklich nicht negativ gemeint. Die müssen sich nicht mit IT-Security auskennen, zumindest nicht in dem Maße wie wir es müssen. Und da wird sicherlich der Bedarf immer mehr, dass man da auch Schulungen anbietet, dass man da auch Sachen vorgibt indem man eben nicht alles installieren darf oder nicht ohne irgendwelche Abfragen irgendwas machen darf. Das kommt in Zukunft bei uns sicherlich und da ist auch der Bedarf da, aber da haben wir momentan noch nicht wirklich viel getan in der Richtung.

I: Mhm. Ja gut, von meiner Seite wärs das dann, wenn Sie nicht noch irgendwas haben was Sie nochmal betonen möchten oder was Sie noch ansprechen möchten spontan.

B: Mir fällt jetzt nichts ein. Ich sag mal so zusammenfassend, ich kannte ja jetzt auch die Fragen noch nicht im Vorfeld, kann man schon sagen, dass glaube ich jedes Unternehmen immer wieder die im Einsatz befindlichen IT-Sicherheitsmaßnahmen beleuchten muss, weil das ist halt in der IT so, das ändert sich täglich vielleicht nicht aber regelmäßig. Und da muss man sich immer wieder hinterfragen ist das immer noch State of the Art was man da tut oder ist da halt noch Optimierungsbedarf, ohne die Benutzer so dermaßen einzuschränken und zu beschneiden, dass es

keinen Spaß mehr macht mit der IT zu arbeiten, die man im Unternehmen hat. Also es ist immer sicherlich ein wichtiger Aspekt. Und wir haben, das erkennen wir aber auch selber, an den ein oder anderen Stellen Optimierungsbedarf. Wir haben immer Glück, dass wir viele IT-Spezialisten auch haben als Kollegen, so dass wir das sicherlich nicht so extrem wie vielleicht andere Unternehmen sehen. Aber Luft nach oben ist immer.

I: Gut, dann bedanke ich mich recht herzlich für das Interview.

B: Sehr gerne.

A5

Interviewtranskript – Firma Mennekes GmbH – 20.11.2014

I: Also, Herr (anonym), um einfach mal einzusteigen in die ganze Geschichte würde ich Sie ganz gerne mal einleitend fragen, wo hier in der Firma, in welchen Bereichen Authentifikation eingesetzt wird, also Authentifikationsverfahren, Mechanismen und welche Technologien in welcher Form auch immer dazu eingesetzt werden?

B: Zum Einen setzen wir hier ein Active Directory ein von Microsoft, wo halt jeder Rechner irgendwo, wenn er denn dann gestartet wird, einer Authentifizierung bedarf, sprich ein Benutzername, ein Passwort, womit er sich dann anmelden kann und entsprechende Ressourcen wie sein Outlook, seine Dinge, die er für das tägliche Arbeiten brauch nutzen darf. Dann gibt es natürlich Authentifizierung noch gegenüber Programmen, im Speziellen zum Beispiel SAP, wo dann im Moment bei uns kein Single-Sign-On aktiv ist, wo sich dann auch der entsprechende Benutzer, wenn spezifische Programme genutzt werden müssen, dann auch entsprechend authentifizieren muss. Mechanismus oder Technik, die da hinter steckt, ist natürlich zum Einen programmintern, da gibt es keine, kann ich jetzt nicht sagen was da genau hinter steckt. Zum Anderen das Active Directory. Dann gibt es noch Authentifizierung von Extern, quasi wenn ein Mitarbeiter ein mobiles Gerät hat oder vom Home Office aus arbeitet, dass er dann auch entsprechend über eine VPN beziehungsweise über ein Portal Applikationen starten darf beziehungsweise dann die Ressourcen hier im Haus nutzen darf und da ist dann eine Authentifizierung bei einer VPN über ein RSA-Secure-ID-Authentication-Manager notwendig mit der entsprechenden Secure-ID-Karte beziehungsweise dann mit dem entsprechenden Software-Token, was wir seit kurzem einsetzen auf Mobiltelefonen. Wo dann das Handy halt eine PIN generiert oder einen Token-Code mit einer dazugehörigen PIN, die sich der Benutzer selbst vergeben darf, dann hier am Netzwerk anmelden darf. Des Weiteren in dem Zusammenhang, in diesem Portal ist es auch möglich nur Applikationen zu nutzen, das setzen wir zum Beispiel ein bei Tochterfirmen im Ausland, die hauptsächlich über veröffentlichte Applikationen hier auf unseren Systemen arbeiten. Diese authentifizieren sich nicht mit RSA sondern über MAC-Adressen, die wir hier dann von den Client-Rechnern, wo die halt den Zugriff hier auf das System machen, hinterlegen und dementsprechend dann der Rechner mit dem entsprechenden Passwort dann auch Zugriff erhält hier.

I: Mhm.

B: Was haben wir noch für Authentifizierung hier im Haus? Authentifizierung auf Ebene Zutritt, das hat jetzt nichts mit Computern zu tun aber räumliche Zutrittsauthentifizierung über die Stempelkarten, die jeder Mitarbeiter hier hat. Da können entsprechende Berechtigungen über unser Zeiterfassungssystem Interflex gesetzt werden, wo dann auch an Türen zum Beispiel so RFID-Leser sind und wenn der Benutzer dann mit seiner Karte davor steht und die Karte davor hält kommt er entweder rein oder kommt nicht rein. Das ist auch so eine Authentifizierung die wir hier haben. Ansonsten fällt mir jetzt in dem Bereich nichts mehr ein.

I: Sie sprachen jetzt primär von Mitarbeitern oder der internen Authentifizierung beziehungsweise der Authentifizierung zwischen Ihnen und Tochterunternehmen. Gibt es da eventuell Unterschiede, wenn Sie mit Kunden kommunizieren? Gibt es da eventuell Authentifizierungsmaßnahmen?

B: Mit Kunden. Kunden haben Zugriff auf Bestände hier im Haus, also Lagerbestände. Da gibt es

eine Authentifizierung über ein Webportal, wo dann der Kunde sich einloggen kann um dann Bestände von Artikeln hier abzufragen. Ist aber auch gegenüber dem AD sogar geregelt, oder gegen eine Webseite, ich weiß nicht was da für eine Technologie hinter steckt. Das macht das Marketing mehr oder weniger. Kunden an sich kommen hier, also was wir hier noch haben sind unsere Handelsvertretungen. Das sind ja auch quasi Kunden. Die kommen hier auf ein SAP-Portal aber dann auch über den Weg MAC-Adressen-Authentifizierung und Zugang zum Portal mit den entsprechenden Ressourcen. Also da ist jetzt auch nicht getrennt zwischen ich sag mal eigener Mitarbeiter oder Handelsvertretung. Das ist jetzt von dem Mechanismus, von der Technologie nicht unterschieden.

I: Okay. Um gerade mal auf die Vorgaben innerhalb der Firma in Richtung Authentifizierung oder IT-Security zu kommen, wie gestalten sich da die Vorgaben beziehungsweise wie werden die gesteuert oder umgesetzt?

B: Ja, ehrliche Meinung oder...?

I: Gerne.

B: Ich weiß nicht wo das hier veröffentlicht wird.

I: Okay. Also können Sie mir was über den Prozess sagen, wenn jetzt meinetwegen neue Richtlinien eingeführt werden oder neue Vorgaben eingeführt werden?

B: Generell gibt es grundsätzlich Richtlinien für Mitarbeiter, die hier quasi Zugriff auf IT-Systeme haben, die den Umgang mit IT-Technik regeln, mit Daten regeln und unter anderem auch regeln, wie die ihr Passwort quasi wählen sollen. Also das sie quasi schon ein komplexeres Passwort wählen sollen und das auch entsprechend ändern sollen, wobei wir jetzt im Moment noch nicht vorgeben, dass das Passwort nach vier, weiß ich nicht, vier sechs Wochen abläuft oder geändert werden muss. Also wir überlassen das im Moment dem Mitarbeiter, das selbstständig zu tun. Von daher haben wir jetzt da nicht ganz strikte Regelungen. Einzige strikte Regelung die es ist, halt wer hier mit VPN auf das System zugreifen will braucht diesen RSA-Security-Token. Das ist Vorgabe hier im Haus.

I: Okay. Einfach mal jetzt aus Ihrer Sicht, wenn Sie beschreiben sollten wie zufrieden Sie so mit der aktuellen Lage sind hier im Haus, was die Authentifizierung angeht. Wie schätzen Sie die Umsetzung ein?

B: Aus IT-Sicht sind wir nicht zufrieden.

I: Okay.

B: Weil wir da sicherlich noch Bedarf haben, das noch zu verstärken beziehungsweise dann auch Authentifizierung zu vereinfachen beziehungsweise Single-Sign-On zu nutzen für die Applikationen, die dann nach dem Active-Directory-Login kommen. Um damit dann auch zu verbinden, eine Passwortrichtlinie quasi dann einzusetzen, zu sagen ihr müsst alle vier acht Wochen euer Passwort entsprechend ändern und das Passwort muss eine entsprechende Komplexität haben. Also da wollen wir sicherlich noch hinkommen. Von daher sind wir nicht nicht, wir wissen, dass wir noch Defizite haben.

I: Okay. Sie sprachen gerade schon von Single-Sign-On, wo Sie drüber nachdenken oder was Sie

für sinnvoll halten. Fallen Ihnen noch andere Technologien oder Systeme ein?

B: Zertifikate ist sicherlich ein Thema, wo man Authentifizierung mit machen kann.

I: Okay.

B: Wo wir auch schonmal drüber überlegt haben, das zum Beispiel für mobile Rechner oder Außendienstler oder sowas zu nutzen im Rahmen von neuen Windows-Versionen, die dann entsprechende Zertifikate Authentifizierung mit sich bringen, wo man dann halt einen transparenten Login zum Firmennetzwerk hat. Setzen wir aber so im Moment nicht ein.

I: Okay, darauf jetzt mal aufbauend. Aus Ihrer Sicht, wie würden Sie sich eine optimale Lösung vorstellen?

B: Optimale Authentifizierungslösung?

I: Ja. Also jetzt mal abgesehen von Umsetzbarkeit, einfach nur mal aus dem Bauch raus.

B: Es wäre sicherlich schon irgendwas wo wir wissen, dass wirklich der Client auch unser Client ist, der sich hier authentifizieren möchte. Sprich eine Zertifikatslösung vielleicht abhängig von einem Client zu schaffen, dass man genau weiß aha der Client der darf hier rein. Dann entsprechend eine Passwortrichtlinie aufzubauen, die dann entsprechend ist und halt das Single-Sign-On, was dann dahinter steckt, dass Transparenz da ist zum Login, zu anderen Applikationen. Also dass quasi der Anwender sich ein Passwort merken muss und dann dementsprechend in allen Applikationen, die ihm zur Verfügung gestellt werden oder wofür er berechtigt ist dann drauf zugreifen darf. Ich denke eine Schwierigkeit ist im Moment, ja gut mit der MAC-Adresse haben wir das eigentlich so wobei MAC-Adressen sich auch fälschen lassen aber das wollen wir jetzt mal nicht jedem unterstellen, dass er das tut und auch die MAC-Adresse muss auch erstmal bekannt sein. Aber ich denke sowas könnte ich mir vorstellen, also dass es erstmal einfacher wird für den Benutzer und nachvollziehbar beziehungsweise kontrollierter für die IT.

I: Mhm, okay. Um dann noch kurz mal in eine andere Richtung zu gehen. Könnten Sie sich vorstellen, entweder an Stelle oder in Kombination mit den aktuell eingesetzten Techniken oder Verfahren, was die Authentifikation angeht, könnten Sie sich vorstellen da eine Art Netz aufzubauen, in der sich Nutzer gegenseitig authentifizieren beziehungsweise dass Nutzer sich gegenseitig die Identität bestätigen? Also dass das Ganze nicht mehr zentral gesteuert ist sondern dass das auf Vertrauen basiert? Könnten Sie sich da vorstellen, dass das einsetzbar wäre?

B: Also quasi dass wenn ich, um das jetzt zu verstehen, also wenn ich jetzt einem Benutzer die Authentizität bestätige, dass der dann auch wiederum anderen Benutzern diese bestätigen darf? In so einem Schneeballverfahren dann mehr oder weniger, also dass ich dann...?

I: Das wäre so eine Ausprägung und dass er wiederum dadurch, dass Sie ihm die Identität bestätigen, dann dass ihm dann bestimmte Rechte eingeräumt werden, dass die Nutzer das unter sich mehr oder weniger aushandeln, was dann flexibel wäre.

B: Ja, ich sag mal so ein ähnliches Prinzip planen wir jetzt einzusetzen auf File-Ebene.

I: Okay.

B: Ist irgendwie so eine Authentifizierungs, ja, dass man bestimmten Benutzern erlaubt auf einen bestimmten Bereich zuzugreifen. Im Moment steuern wir das hier zentral von der IT aus, dass wir die Berechtigungen vergeben oder die Benutzer in die entsprechenden Berechtigungsgruppen reinsetzen und das ist geplant, dass wir halt da ein Berechtigungsmanagementsystem aufsetzen wo wir quasi dann, wie heißen die nochmal, Data-Owner definieren in Form einer Person, die dann für einen bestimmten Bereich zuständig sind und dort die Berechtigungen auch selber vergeben dürfen. Das ist ja quasi so ein Authentifizierungsprinzip. Also das ist so der Schritt aber jetzt zu sagen grundsätzlich, wenn ich jemandem vertraue, dass der dann automatisch dazu berechtigt ist anderen denen er vertraut das freizugeben, nicht in jedem Bereich. Also das würde ich jetzt mal nicht machen wollen. Zum Beispiel, nein, das wäre ja schon, weiß ich nicht,...

I: Gut, das ließe sich ja theoretisch auch ein bisschen eingrenzen. Aber fallen Ihnen da jetzt Bereiche ein wo das aus Ihrer Sicht nicht machbar wäre? Oder wo sehen Sie Probleme bei der Sache?

B: Es hört sich zwar jetzt doof an aber man darf nicht jedem vertrauen, dem ein Mann automatisch auch vertraut. Ich habe jetzt andere Freunde als der (anonym) Freunde hat und ob ich jetzt automatisch seinen Freunden vertrauen würde weiß ich nicht, dafür kenne ich die Leute zu wenig und wenn ich verantwortlich für den Bereich wäre und sagen würde alle deine Freunde sind auch meine Freunde, hätte ich jetzt ein Problem mit ganz ehrlich gesagt. In bestimmten Bereichen nicht oder in bestimmten Ebenen nicht. Wenn ich jetzt zum Beispiel dieses Berechtigungsmanagement sehe da ist der Data-Owner dann schon eine verantwortliche Stellung hier im Haus, eine Person, die eine entsprechende Position auch hat. Wenn die den Leuten diese Person freischaltet, auch vertraut, dann ist das in Ordnung, aber er wird ja nicht sagen dann alle von Mitarbeitern, also wenn er es runter deligiert auf den Mitarbeiter und der sagt dann ich habe tausend Freunde, die will ich auch alle mit da rein lassen, das sind ja meine Freunde, dann kann ich mir nicht vorstellen, dass das funktioniert und hinterher auch noch den Richtlinien der Firma entspricht.

I: Also sehen Sie da so im betrieblichen Umfeld Probleme?

B: Ich denke schon, ja.

I: Und wenn Sie das mal vergleichen mit dem privaten Umfeld?

B: Ich wüsste jetzt nicht so den Anwendungsfall. Was ist so der Anwendungszweck im Privaten wenn ich jetzt sagen würde, ich bin nicht so in Social Medias unterwegs, hab ich nicht so viel mit zu tun. Weiger ich mich so ein bisschen beziehungsweise sehe die Notwendigkeit auch nicht da. Von daher hätte ich da auch wahrscheinlich im privaten Umfeld, ich jetzt für mich persönlich, ein Problem zu sagen, ich habe einen Freund, du bist mein Freund und wenn du tausend Freunde mitbringst denen vertraue ich auch. Da hätte ich wahrscheinlich auch ein Problem mit, weil ich die Freunde nicht kenne und auch nicht weiß, wie die ticken, wie die umgehen mit bestimmten Informationen. Also hätte ich ein Problem mit. Muss ich ganz ehrlich sagen. Es muss ja nicht jeder wissen was ich meinem Freund erzähle, dann muss er ja nicht seinen tausend anderen Freunden auch noch erzählen, weil das erzähle ich meinem Freund und nicht den tausend anderen Freunden.

I: Ja, okay. Fallen Ihnen denn spontan, wenn Sie einfach mal drüber nachdenken, fallen Ihnen denn gewisse Gruppen ein, wie man das Ganze clustern könnte oder wie man das Ganze aufteilen könnte? Also was jetzt die Authentifikation angeht.

B: Jetzt in diesem Netzwerk?

I: Ja genau. Dass man das vielleicht unterteilen könnte, separieren könnte?

B: Ich denke es ist immer abhängig von den Informationen, die ich verbreiten möchte.

I: Okay.

B: Ich müsste die Informationen klassifizieren. Ich müsste sagen die Information, die darf jetzt jeder des Freundes Freunde wissen, dann kann der die weiter geben. Aber wenn ich sage das ist eine private vertrauliche Information, dann soll auch nur der Freund die wissen und nicht die tausend Freunde von dem Freund. Ich denke das muss man irgendwie anhand der Information oder des Zugriffs wodrauf man zugreifen möchte klassifizieren. Ich denke das ist mehr der Ansatz. Und dann kann ich es auch noch vielleicht gruppieren, zu sagen die Information ist ganz privat, die ist halb privat und öffentlich, irgendwie sowas. Aber um da jetzt die Gruppen zu gruppieren, weiß ich nicht, tue ich mich schwer. Ich denke es hängt an der Information.

I: Okay. Um jetzt mal in eine andere Richtung zu gehen würde ich gerne noch zu sprechen kommen auf die Nutzerebene, also auf die Authentifikation und die IT-Sicherheit-Aspekte aus der Nutzersicht. Wo kommen denn die Nutzer aktiv in Berührung mit den eingesetzten Verfahren und wie gestaltet sich da die Bedienbarkeit?

B: Also, wie gesagt, morgens beim Hochfahren des Rechners ist die eine Authentifizierung, Passwort eingeben, anmelden, alles gut. Applikation noch anmelden. Ich denke, der Benutzer muss einfach in der Lage sein, da auch den Benutzernamen und das Passwort einzugeben, das ist so jetzt bei den internen Rechnern die Authentifizierung. Extern halt über die RSA-Security-Token, da entsprechend dann halt den Token abzulesen, die PIN zu wissen, den Benutzernamen zu wissen und das Netzwerkkennwort zu wissen, das ist da in dem Umfeld. Bedienbarkeit denke ich mal ist in Ordnung. Es hat eine gewisse Komplexität aber es ist noch relativ handhabbar würde ich jetzt mal als IT-technischer sagen. MAC-Adressen-Authentifizierung ist auch Benutzername Passwort, der da eigentlich nur, die MAC-Adresse wird dann entsprechend hier hinterlegt, da hat der Benutzer eigentlich nichts mit zu tun, also von daher auch handhabbar. Was hatten wir noch? Gut, Zutritt hier, Zutrittskontrollen, Zutrittsauthentifizierung, Karte vor halten Tür öffnet sich oder Tür bleibt zu ist eigentlich auch relativ einfach zu handhaben.

I: Fallen Ihnen denn spontan Probleme ein oder haben Sie schon von Problemen gehört, die bei der Nutzung von gewissen Technologien auftreten könnten?

B: Ist benutzerabhängig, ja.

I: Okay ja, aus Benutzersicht.

B: Wenn der Benutzer sich einloggt auch schonmal seinen Benutzernamen nicht weiß, wenn dann jemand anderes sich am Rechner angemeldet hat zum Beispiel. Das kann schonmal passieren, dass man einfach nicht, wenn man das jeden Morgen macht, nicht darauf achtet welcher Name drin steht sondern einfach sein Passwort eintippt. Es kann auch schonmal passieren, dass Passwörter schonmal vergessen werden, auch dann zurückgesetzt werden müssen, dass das Konto gesperrt wird oder falsch eingegeben wird. Ein anderes Problem kann natürlich sein beim Security-Token, beim RSA-Token, dass der verloren geht. Da kann er sich auch entsprechend nicht mehr einloggen, beziehungsweise muss dann hier anrufen um dann einen Emergency-Code sich generieren zu lassen, mit dem er sich dann einloggen kann von extern. Aber ansonsten sind das so die einzigen

Probleme.

I: Fallen Ihnen denn dazu spontan Abkürzungen im System ein? Also ist es aus Ihrer Sicht möglich, dass Nutzer an gewissen Stellen dazu verleitet werden das System zu umgehen oder zumindest versuchen zu umgehen oder auszutricksen?

B: Ist eigentlich nicht,... Wüsste ich nicht, nein. Also ich muss ja irgendwo ein Passwort haben, wenn ich es nicht habe komme ich nicht rein.

I: Ja.

B: Wenn ich meinen Rechner nicht freigeschaltet habe mit der entsprechenden MAC-Adresse oder die nicht gefaked habe oder wie auch immer komme ich auch nicht hier rein. Also dann funktioniert es einfach nicht. Also von daher, umgehen...

I: Oder um sich den Alltag ein bisschen zu erleichtern.

B: Nein, wüsste ich nicht. Normalerweise haben die Kollegen hier im Haus auch nur Standardberechtigungen auf den Rechnern, wenn ich es jetzt mal auf die Rechner runterbreche, und damit keine administrativen Rechte und damit können die eigentlich so, sollten sie eigentlich nicht viel machen können an den Dingern. Es gibt sicherlich schonmal kriminelle Energie in manchen Leuten aber es ist natürlich auch, es hängt ein bisschen von der IT auch ab wie sicher die Systeme dann sind. Das ist ja unsere Verantwortung mehr oder weniger dann auch sicherzustellen, dass die Leute nicht viel machen können mit Ihren Systemen. Oder auch diese Möglichkeit nicht haben. In dem Bereich Authentifizierung ist ja auch irgendwie Device-Management, Device-Pro, ist auch Authentifizierung was wir hier einsetzen, womit dann bei bestimmten Leuten dann bestimmte Ports oder Schnittstellen am Rechnernotebook freigeschaltet werden. Wenn wir natürlich nicht sicherstellen, dass die Ports zu sind die zu sein sollen, dann ist natürlich auch immer ganz schnell das iPhone hier eingesteckt im Rechner und wird dementsprechend ausgelesen und genutzt. Ob jetzt bewusst oder unbewusst von dem Mitarbeiter, der dann da das versucht und dann auch vielleicht erfolgreich Daten rauslesen kann, aber ich denke das ist so.

I: Okay. Um auf das Bewusstsein der Nutzer zu sprechen zu kommen, wie schätzen Sie das ein hinsichtlich Authentifikation aber auch hinsichtlich der IT-Sicherheit im Unternehmen?

B: Ist noch nicht so weit, dass man sagen würde jedem wäre bewusst, was man mit dem Benutzernamen und dem dazugehörigen Passwort alles anrichten kann. Ich denke das Bewusstsein ist noch nicht wirklich da. Weil teilweise sind die Passwörter hier im Unternehmen nicht wirklich komplex gewählt, teilweise auch mehreren Personen bekannt, vertretungstechnisch dann, dass man einfach seinen Benutzernamen Passwort dann an die Kollegin weitergibt, die dann falls der eine Kollege dann nicht da ist da an den Rechner gehen kann, die E-Mails prüfen kann oder weiterleiten kann. Ich denke so richtig das Bewusstsein ist noch nicht und das Verständnis auch für manche Technologien einfach auch nicht von den Benutzern. Dass die auch wirklich wissen was alles entweder an Informationen hier raus genommen werden können aus dem System beziehungsweise irgendwelche Informationen verändert werden unter bestimmten Kontoinformationen, die man dann besitzt, oder halt auch Viren hier eingeschleust werden können zum Beispiel jetzt bei dem Device-Management-System. Und das Bewusstsein ist noch nicht da.

I: Okay.

B: Noch nicht so ganz ausgeprägt, sagen wir es mal so.

I: Also sehen Sie da durchaus Probleme, die auftreten können?

B: Es können schonmal, es treten schonmal Probleme auf, dass ohne dieses Bewusstsein halt bestimmte Viren zum Beispiel hier rein geschleust werden, dass Viren auftreten. Aber sonst, dass jetzt Missbrauch damit betrieben wird, dass einer das Passwort kennt, wäre mir jetzt unbekannt.

I: Mhm. Also basiert auf der Nutzerebene schon relativ, also herrscht viel Vertrauen.

B: Es herrscht viel Vertrauen, ja.

I: Okay, würden Sie denn sagen, dass sich das denn schon ein bisschen gewandelt hat, das Bewusstsein, oder sehen Sie da im Moment eher Stagnation?

B: Nein, es ändert sich schon. Also früher war es noch lascher sag ich mal, mittlerweile hat man schon so ein kleineres Bewusstsein dafür gekriegt aber es ist wirklich noch nicht so, dass man vollstes Verständnis für bestimmte Dinge, die man dann, zum Beispiel wenn wir jetzt sagen würden alle vier Wochen ändert euer Passwort. Da hätten die Benutzer im Moment noch nicht das Verständnis für. Wobei sie sicherlich schon jetzt dahingehen, um zu sagen ich brauche jetzt ein anderes Passwort anstelle meines dreistelligen Passwortes, was ich sonst immer hatte. Was dann aus den drei ersten Buchstaben des Alphabetes bestand. Das Bewusstsein ist jetzt schon da, dass diese Passwörter vielleicht schon komplexer sein müssen aber das Bewusstsein jetzt dafür zu sagen ich muss alle vier Wochen mein Passwort ändern, das ist noch nicht da.

I: Okay. Würden Sie sagen, dass da unterschieden werden kann zwischen dem Privatleben sag ich mal und der Arbeit? Dass da vielleicht Unterschiede herrschen?

B: Ich denke, dass im Privatleben das gleiche Nicht-Bewusstsein da ist für die Konten, die man sich anlegt, dass man dafür dann meistens auch irgendwelche einfachen Passwörter nimmt so wie man es hier im Unternehmen auch macht oder versucht zu machen. Ich denke, dass das Bewusstsein das gleiche ist. Vermute ich mal. Dass man das Bewusstsein aus dem Privaten mit hier rein nimmt und im privaten Umfeld denke ich mal hat nicht jeder eine Passwortdatenbank zu Hause mit seinen Passwörter und seinen zehn kryptischen, nicht-alphabetischen Zeichen, die er dann da im Passwort hinterlegt. Würde ich jetzt mal so sagen.

I: Okay. Als letzten Punkt würde ich gerne mal noch zu sprechen kommen auf Schulungsmaßnahmen in Richtung IT-Sicherheit, also jetzt auch Authentifikation aber vielleicht auch übergeordnet die IT-Sicherheit. Wie sieht das da aus, also wurden da schon Schlungen in der Richtung vollzogen oder ist da eventuell irgendwas in Planung?

B: Also Schulungen IT-sicherheitstechnisch erfolgen dann, wenn der Mitarbeiter vielleicht eine passende Frage an den Supportler stellt, der gerade bei ihm am Rechner steht. Aber eine generelle Schulung für alle Mitarbeiter ist nie gemacht worden und ich weiß nicht ob es geplant ist. Es ist geplant im Rahmen des Berechtigungsmanagement da vielleicht mal eine Schulung zu machen oder eine Einweisung für die bestimmten Data-Owner oder für einen bestimmten Personenkreis. Aber ich denke nicht, dass wir alle Kollegen hier im Haus schulen werden. Also, das ist sicherlich noch ein Thema, da muss man sich Gedanken zu machen, ob das vielleicht sinnvoll ist solche Themen auch dann mal zu schulen. Aber ich denke es wird eher dann ein Thema werden, wenn wir hier sei es mit Zertifikaten, Zukunftsmusik, oder sei es mit strikteren Passwortregeln hier vielleicht neue

Richtlinien schaffen, wo dann die Leute auch das entsprechende Verständnis für haben müssen. Und da macht vielleicht eine Schulung dann Sinn.

I: Halten Sie es denn generell für sinnvoll, die Mitarbeiter zu sensibilisieren was die Sicherheit angeht?

B: Auf jeden Fall. Das auf jeden Fall. Man sollte schon gucken, dass die Leute, das haben wir jetzt zuletzt noch gemacht, hat jetzt mit Authentifizierung nichts zu tun aber mit dubiosen E-Mails. Da werden dann Telekom-Rechnungen verschickt, wie es ja auch in allen Medien steht, und werden trotzdem noch hier im Haus quasi geöffnet, der Link wird geöffnet, ein entsprechender Virus ist dann auf dem Rechner drauf und daraufhin haben wir versucht nochmal mit einer E-Mail die Leute ein bisschen zu sensibilisieren und zu sagen hey, passt ein bisschen auf wenn irgendwas dubioses in eurem Postfach ist, nicht sofort alles anklicken, aufmachen oder sonstiges wobei es dann auch den Fall gab, einen Tag nachdem diese E-Mail rumgeschickt worden ist hat ein anderer Kollege genau das offen gemacht was er nicht offen machen sollte also von daher ist es auch ein bisschen schwierig. Dafür wäre vielleicht so eine Schulung auch nochmal gut.

I: Also denken Sie, dass das in Zukunft durchaus mehr werden könnte?

B: Das denke ich schon, weil ich denke mal die Daten oder gewisse Daten werden kritischer, die man auch nicht jedem zur Verfügung stellen sollte und gewisse Informationen einfach auch hier das Haus nicht verlassen sollten oder gewisse Dinge auch entsprechend geschützt werden müssen, von daher auch die Leute sensibilisiert werden müssen, wie sie mit den Informationen umzugehen haben. Weil ich denke, dass das vielleicht in Zukunft mehr kommt, ja, zumindest die Sensibilisierung der Kollegen.

I: Ja okay, das wars erstmal von meiner Seite, wenn Sie nicht noch was haben, was Sie gerne nochmal erwähnen würden. Okay. Dann bedanke ich mich recht herzlich für das Interview.

B: Ja, gerne.