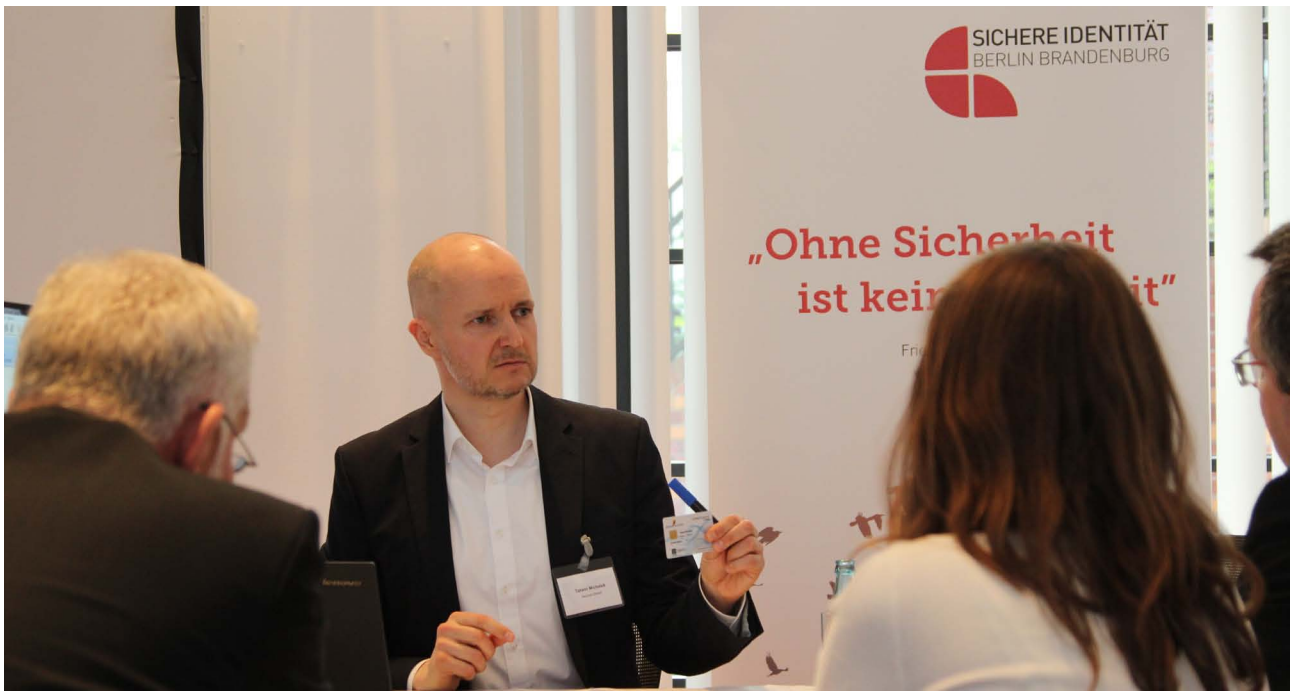
„Wenn wir uns nicht intensiver mit Informationssicherheit befassen, nutzen uns die digitalen Chancen wenig.“



Sicherheit im digitalen Wandel – Dokumentation einer Dialogveranstaltung im Hause Bundesdruckerei

Am 11.05.2017 fand ihn den Räumen der Bundesdruckerei die Dialogveranstaltung „Sichere Identitäten“ statt.

Ausgewählte Experten und rund 40 Gäste diskutierten in einem sog. World Café aktuelle Herausforderungen der Digitalisierung. Die Themen umfassten u.a. das Vermeiden von Medienbrüchen in digitalen Geschäftsprozessen, rechtliche Entwicklungen oder auch Sicherheitslücken in IT-Systemen, die durch die aktuelle ransomeware „WannaCry“ offengelegt wurden. Den Rahmen für die angeregten Diskussionen bildeten fünf Themenblöcke:

- Digitalisierung von papierbasierten Prozessen mit E-Signatur
- Datenschutz 2.0 – Neues aus der EU ab Mai 2018 (EU-DSGVO)
- IT-Sicherheit – eine Hürde für die Umsetzung der Digitalisierung in Unternehmen?
- ID Management – Identitäten ohne Passwort
- Vertrauliche E-Mails – Neues zum Wirtschafts- und Knowhow-Schutz

Ziel des gemeinsamen Nachmittags war es, Ansprechpartner für individuelle Fragen zu identifizieren sowie dringende Problemfelder zu benennen und erste Lösungen zu erarbeiten. Organisiert vom Verein Sichere Identität Berlin-Brandenburg e.V., in Kooperation mit den Unternehmensverbänden Berlin-Brandenburg e.V. und der Mittelstand 4.0 Agentur Kommunikation, war die Veranstaltung vor allem auf einen konstruktiven Dialog zwischen den Beteiligten ausgerichtet. Das Format „World Café“ bot dafür den idealen Rahmen.

Mittelstand 4.0
Agentur Kommunikation

UVB
Unternehmensverbände Berlin-Brandenburg

SICHERE IDENTITÄT
BERLIN BRANDENBURG

Einstieg in einen spannenden Nachmittag

Sehr herzlich möchte ich Sie im Namen des Vorstandes und der Geschäftsführung unseres Vereines „Sichere Identität Berlin-Brandenburg e.V.“ begrüßen.

Die historischen Räume der Bundesdruckerei bezeugen die lange Tradition mit der hier, im Mittelpunkt der Hauptstadtregion, Personalausweise, Pässe und Führerscheine, die sicheren Identitäten der realen Welt, geschaffen werden. Seit 20 Jahre werden hier am Standort durch die D-TRUST GmbH auch sichere elektronische Identitäten in Form von digital signierten Zertifikatsdateien erzeugt. In dieser Kombination bildet dieses ein einzigartiges Kompetenzzentrum in Europa.

Das Entstehen neuer Kommunikationsmittel und -technologien, die zunehmende interaktive Nutzung des Internets und der Siegeszug von Social Media führen zu einem veränderten Umgang mit Identitätsdaten. Gleichzeitig bieten immer mehr Unternehmen und Behörden Dienstleistungen über elektronische Kanäle an. Diese Entwicklungen erzeugen einen neuen Bedarf an Konzepten und Lösungen für den sicheren Umgang mit Identitätsdaten.

Viele unserer Mitglieder arbeiten intensiv an diesen Themen. Aus diesem Grund haben wir uns besonders gefreut, mit den Experten von secrypt, der Bundesdruckerei GmbH, der Freien Universität Berlin, dem Hasso-Plattner-Institut und der Zertificon Solutions GmbH in einem interaktiven Format, dem „World Café“, über Herausforderungen und mögliche Lösungen im Bereich „Sichere Identitäten“ zu diskutieren. Ich lade Sie hiermit herzlich ein, diese spannende Diskussion in Form der vorliegenden Broschüre nachzulesen.

Arno Fiedler, Vorstand Sichere Identität Berlin-Brandenburg e.V.

Die Region Berlin-Brandenburg entwickelt sich kontinuierlich zu einem der führenden Digital-Standorte in Europa. Gerade für die kleinen und mittleren Unternehmen in der Hauptstadtregion ist das erfreulich, bringt aber auch eine Reihe von Fragen und Herausforderungen mit sich. Wer die Chancen der Digitalisierung erfolgreich nutzen will, darf bei der Sicherheit kein Auge zudrücken.

Darum haben wir Führungskräfte aus KMU und Experten ins Gespräch gebracht. Welche datenschutzrechtlichen Aspekte müssen bedacht werden, wenn die Bürokommunikation digital funktioniert? Welche Konsequenzen hat die Einführung digitaler Unterschriften? Welche Gesetze und Normen sind in diesem Bereich relevant und wie werden sie ausgelegt?

Im Rahmen eines sogenannten World Café wurden diese und andere Fragen angeregt diskutiert. Bei dieser Methode gibt es keine wortgewaltigen Menschen „da vorne“ oder gar „da oben“, die nacheinander Reden halten. Die Veranstaltung war vielmehr eine gleichberechtigte Debatte, in die alle ihre Erfahrungen einbringen konnten.

Im Namen der Mittelstand 4.0 Agentur Kommunikation, dem Verein Sichere Identität Berlin-Brandenburg e.V. und den Unternehmensverbänden Berlin-Brandenburg UVB laden wir Sie herzlich ein, die Themen und Ergebnisse dieses spannenden Nachmittags Revue passieren zu lassen.

Anne-Sophie Braun, Geschäftsführerin Sichere Identität Berlin-Brandenburg e.V.

Prof. Dr. Thomas Thiessen, Rektor der BSP Business School Berlin, Konsortialleiter der Mittelstand 4.0 Agentur Kommunikation

Sven Weickert, Geschäftsführer Vereinigung der Unternehmensverbände in Berlin und Brandenburg e. V.

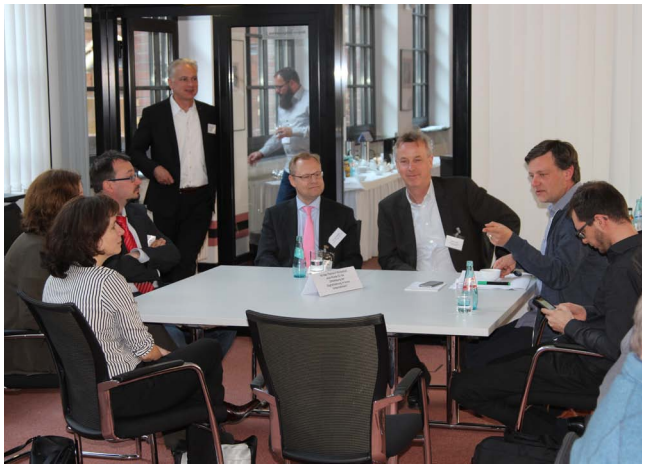
Aus Gründen der besseren Lesbarkeit wird auf eine geschlechtsneutrale Differenzierung (z. B. Mitarbeiterinnen / Mitarbeiter) verzichtet. Entsprechende Begriffe gelten im Sinne der Gleichbehandlung grundsätzlich für beide Geschlechter. Die verkürzte Sprachform hat nur redaktionelle Gründe und beinhaltet keine Wertung.

Workshop-Methode „World Café“ – Was ist das und wie geht es?

In der Regel findet die strategische Ausrichtung eines Unternehmens in einem engen Führungskreis statt und wird von ökonomischen Aspekten bestimmt. Um zusätzliche Innovationspotenziale zu erschließen, bemühen sich viele Unternehmer, die Impulse ihrer Mitarbeiter einzubeziehen und sie zur aktiven Mitgestaltung von Innovationsprozessen zu motivieren. Die Methodik des World Café bietet hierfür eine innovative Kommunikationsplattform.

Alle Teilnehmer eines World Café werden gebeten, sich nach dem Zufallsprinzip an Tischen zu gruppieren und zu einer vorgegebenen Fragestellung ins Gespräch zu kommen. Idealerweise finden sich an jedem Tisch 4 – 6 Personen sowie ein Moderator zusammen. Als Diskussionszeitraum werden etwa 15 – 20 Minuten festgelegt, in denen die Gesprächspartner Fragen stellen, Wissen teilen und gemeinsam neue Lösungen und Ideen entwickeln, die auf Papiertischdecken oder separaten Flipchart-Postern stichpunktartig notiert werden.

Nach Ablauf der vereinbarten Frist wechseln die Gesprächspartner an andere Tische und diskutieren die dort vorgegebenen Fragestellungen. Im abschließenden Plenum werden die gesammelten Ergebnisse von den Thementisch-Moderatoren vorgestellt.



Thementisch 1: Digitalisierung von papierbasierten Prozessen mit E-Signatur

Worum ging es?

Im Zuge der Transformation des Geschäftsalltages in die digitale Sphäre hat die Daten- und Dokumentensicherheit massiv an Bedeutung gewonnen.

Mehr und mehr Organisationen sind bestrebt, Dokumente und zugehörige Unterschriften in digitaler statt in Papierform zu verarbeiten und zu archivieren – und das bei einem möglichst hohen Beweiswert, gegebenenfalls über einen mehrjährigen Aufbewahrungszeitraum hinweg. In diesem Zusammenhang rücken Verfahren für elektronische Signaturen, mit denen sich Authentizität (Urhebernachweis) und Integrität (Manipulationsschutz) sicherstellen lassen, in das Zentrum der Aufmerksamkeit von IT-Strategie, Compliance und gesellschaftlichem Diskurs.

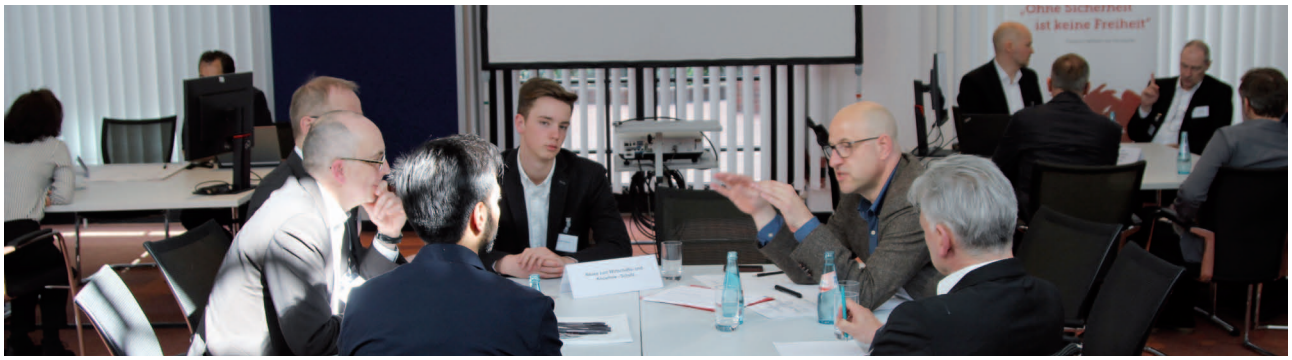
Wesentliche Aspekte der Diskussion:

Mit der Umsetzung digitaler Geschäftsprozesse und dem Einsatz elektronischer Unterschriften sollen Medienbrüche (ausdrucken, unterschreiben und einscannen von Dokumenten) vermieden werden. In der Runde haben sich die typischen Faktoren, die die Einführung solcher Technologien maßgeblich beeinflussen, bestätigt: Betroffene Mitarbeiter müssen motiviert, überzeugt und geschult werden. Älteren Mitarbeitern muss die Angst genommen werden. Ein hoher Komfort bei der Benutzbarkeit kann hier wesentliche Überzeugungsarbeit leisten. Dabei ist die nahtlose Integration der E-Signatur in den Dokumenten-Workflow, der beispielsweise durch ein Dokumenten-Management-System gesteuert wird, entscheidend. Nicht zuletzt müssen die Kosten den zu erwartenden Nutzen rechtfertigen.

FAZIT: Das Thema Digitalisierung ist allen Teilnehmern sehr bewusst. Einige nutzen die elektronische Signatur bereits aktiv in ihren Geschäftsprozessen. Die überwiegende Anzahl sieht hohes Potential und großen Nutzen der vorgestellten Lösung bei der Optimierung ihrer Geschäftsprozesse und wird sich mittelfristig intensiv damit auseinandersetzen. Dies hat auch eine Minibefragung unter den Teilnehmenden bestätigt: Es waren insgesamt 21 Organisationen (vom mittelständischen Unternehmen bis zum Großverband) vertreten, 19 (ca. 90%) habe sich bereits mit der Digitalisierung beschäftigt, 11 (ca. 52%) setzen bereits die elektronische Unterschrift in der einen oder anderen Form ein.

Impulsgeber: Dipl.-Ing. Tatami Michalek, Geschäftsführer secrypt GmbH
tatami.michalek@secrypt.de

Thementisch 2: Datenschutz 2.0 – Neues aus der EU ab Mai 2018 (EU-DSGVO)



Worum ging es?

Die neue Datenschutz-Regulierung der EU tritt ab 25. Mai 2018 in Kraft. Sie ersetzt in den 28 EU-Mitgliedsstaaten die bis dahin geltende Datenschutzrichtlinie 95/46/EG aus dem Jahre 1995 und die auf dieser Basis erlassenen nationalen Umsetzungsgesetze.

Der Datenschutz wird innerhalb der EU auf diese Weise auf eine einheitliche rechtliche Grundlage gestellt. Die Datenschutz-Regulierung der EU sorgt für gleiche Wettbewerbsbedingungen für alle Unternehmen, die Waren oder Dienstleistungen auf dem europäischen Markt anbieten und gilt zusätzlich auch für den gesamten öffentlichen Bereich. In Vorbereitung auf die Regulierung gilt es, eine Reihe von Maßnahmen in Unternehmen zu treffen. Hierzu gehören u.a. die Installation eines Datenschutz-Managementsystems sowie die Sensibilisierung der verantwortlichen Abteilungen für die Veränderungen. Die angeregte Diskussion verlief entlang der folgenden 2 Fragestellungen:

1. Welche Anforderungen sind gegenüber dem BDSG neu?

2. Was muss in Vorbereitung auf die Regulierung getan werden?

Wesentliche Aspekte der Diskussion:

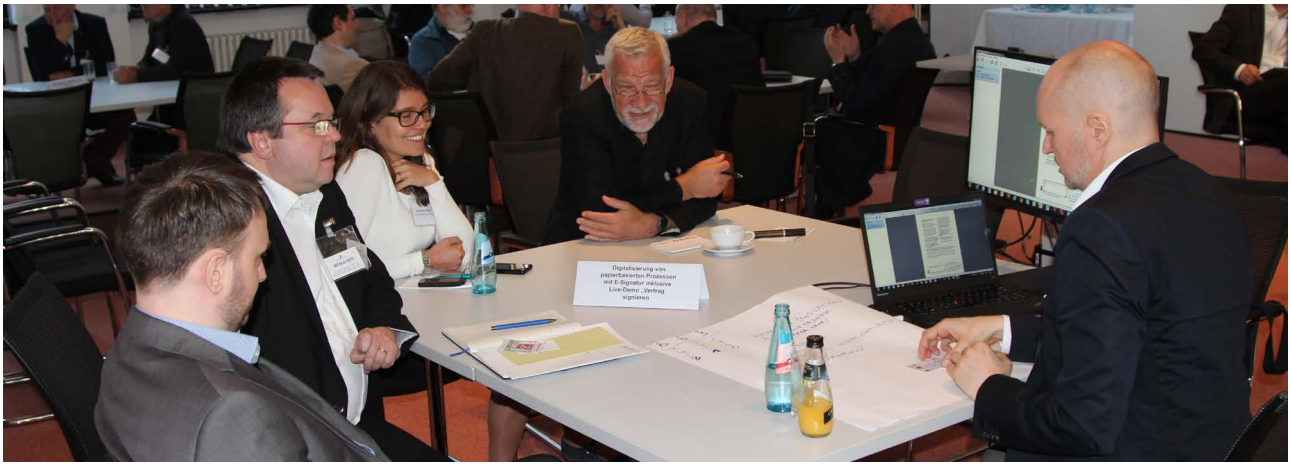
Die Grundsätze des Bundesdatenschutzgesetzes (BDSG) bleiben auch nach Inkrafttreten der Regulierung bestehen. Dies betrifft u.a. die Gebote der Zweckbindung und Transparenz sowie das Gebot der Datenvermeidung und Datensparsamkeit. Neu gegenüber dem BDSG ist für Unternehmen u.a. die Pflicht zu verbraucher- und datenschutzfreundlichen Voreinstellungen z. B. bei elektronischen Geräten. Neu für Unternehmen ist auch die Pflicht zur Datenschutzfolgeabschätzung, die immer dann greift, wenn eine Form der Datenverarbeitung wahrscheinlich ein hohes Risiko verursacht. Mit der neuen Regulierung ändern sich auch die Vorgaben zur Datensicherheit in Unternehmen. Dies betrifft sowohl technische als auch organisatorische Maßnahmen. Neue Verfahren müssen etabliert und Prozesse entsprechend der Verordnung angepasst werden. Aufgrund der umfangreichen Änderungen, die durch die Datenschutz-Regulierung entstehen, sollte dringend ein Datenschutz-Managementsystem installiert werden. Interne Verarbeitungsübersichten, mit Begründungen der Zulässigkeit und eindeutigem Zweck des Verfahrens, sollten erstellt werden. Bestehende Verträge müssen überprüft und Datenschutzfolgeabschätzung durchgeführt werden.

!

FAZIT: Bei den KMU ist das Bewusstsein für die DSGVO vorhanden, die Informationsbedarfe, insbesondere mit Blick auf die Datenschutzfolgeabschätzungen sind jedoch noch sehr groß. Da ab Inkrafttreten der DSGVO empfindliche Strafen bei Nichteinhaltung drohen, müssen KMU frühzeitig die Umsetzung und Einhaltung organisieren und zeitnah offene Fragen klären. Weil nicht nur die Bestimmungen der DSGVO eingehalten, sondern auf Nachfrage auch ihre Einhaltung demonstriert werden muss, müssen interne Prozesse klar dokumentiert werden. Bei diesen Schritten brauchen KMU sachkundige Unterstützung. Weitere Veranstaltungen und Beratungsangebote zu diesem Thema sind dringend erforderlich.

Impulsgeber: Dirk Clemens, Datenschutzbeauftragter der Bundesdruckerei
Dirk.clemens@bdr.de

Thementisch 3: IT-Sicherheit – eine Hürde für die Umsetzung der Digitalisierung in Unternehmen?



Worum ging es?

Teilnehmer aus KMU, Branchenvertreter und IT-Firmen diskutierten angeregt an 5 Thementischen. Die Vielfalt der Argumente war riesig. Allen Beteiligten ist bewusst, dass die Digitalisierung ein wichtiger Schritt für die Zukunft der kleinen und mittleren Unternehmen in der Region ist. Dies zeigte sich am deutlichsten bei dem Thema Internetpräsenz. KMU die sich nicht im Internet präsentieren haben schon heute Probleme, qualifizierte Mitarbeiter zu finden oder Neukunden zu akquirieren. Wachstumschancen, Wettbewerbsvorteile und eine erhöhte Kundenbindung werden ganz konkret mit Digitalisierungsvorhaben in Zusammenhang gebracht. Auf diesem Weg gibt es eine ganze Reihe von Fragen und großen Informationsbedarf seitens der KMU. Sie betreffen vor allem die Bereiche Kosten für IT-Sicherheit sowie Zukunftsfähigkeit der IT-Dienstleistungen und Komponenten. Die Schulungsbedarfe im Bereich der IT-Sicherheit sind groß.

Wesentliche Aspekte der Diskussion:

Die für die Digitalisierung benötigten Kosten können von den Verantwortlichen in KMU nur schwer abgeschätzt werden. Häufig wurden im Gespräch die anfallenden Kosten deutlich zu hoch eingeschätzt. Auch die Folgekosten konnten aufgrund fehlender Erfahrungen nur schwer kalkuliert werden. Der Bereich der Zukunftssicherheit betrifft vor allem Fragen nach Standards und Normen, die Komponenten und Dienstleistungen über längere Zeiträume hinweg vernetzbar machen. Kann meine gerade teuer bezahlte Maschine in fünf Jahren noch mit den anderen Komponenten in meiner Fertigung „reden“? Auch die technischen Aspekte der IT-Sicherheit wurden intensiv diskutiert. Der große Informationsbedarf in diesem Bereich ist klar erkennbar. Als mögliche Lösungen wurden vor allem Cloud-Angebote identifiziert, die auf der einen Seite die Kosten für die Digitalisierung deutlich reduzieren können, aber auch ein Mindestmaß an IT-Schutzangeboten bieten.

FAZIT: Eine Lösungsorientierte Auseinandersetzung mit den genannten Themen ist für Unternehmen essentiell notwendig, wenn das Thema IT-Sicherheit nicht zu einem Hemmnis für die Digitalisierung werden soll. Trotz der angeregten und aufgeschlossenen Diskussion ist ein gewisses Unbehagen bei KMU spürbar. Kosten können (noch) nicht zuverlässig eingeschätzt und die Konsequenzen der Einführung von digitalen Komponenten gerade im Hinblick auf die Datensicherheit noch nicht umfassend abgeschätzt werden.

Impulsgeber: Prof. Dr. Marian Margraf, Institut für Informatik, Fachbereich Mathematik und Informatik, (FU Berlin), marian.margraf@fu-berlin.de

Thementisch 4: ID Management

Worum ging es?

Ein Mensch existiert in der realen Welt exakt ein Mal. Seine Identität kann durch den Personalausweis oder Führerschein bestätigt werden. Diese Dokumente enthalten eine Handvoll Identitätsattribute wie den Namen und die Anschrift. Im Gegensatz dazu hat ein durchschnittlicher Bürger in der digitalen Welt ca. 26 Identitäten. Eine digitale Identität zeichnet sich normalerweise durch einen Account bei einem digitalen Dienst wie z. B. Amazon oder Facebook aus. Für eine Authentifizierung in der digitalen Welt wird in der Regel eine Verbindung von Benutzername und Passwort benötigt. Derzeit werden ca. 6.750.000 digitale Identitäten pro Monat von Cyberkriminellen gestohlen, z. B. durch Attacken gegen Amazon-Serverfarmen. Ein sicheres Identitätsmanagement wird durch die Vielzahl an unterschiedlichen digitalen Identitäten erschwert. Zu den 26 passwortgeschützten Accounts hat ein durchschnittlicher Nutzer nur fünf unterschiedliche Passwörter. Was kann man tun, um die eigenen digitalen Identitäten vor Missbrauch durch Cyberkriminelle zu schützen?

Wesentliche Aspekte der Diskussion:

Die Mehrheit der Teilnehmer zieht eine sichere digitale Identität vielen verschiedenen Identitäten vor. Aus der Diskussion im World Café ergaben sich die folgenden fünf Aspekte, die eine sichere Identität mindestens beinhalten sollte:

- Unterstützung von allen digitalen Diensten und diversen digitalen Geräten
- flexible und mobile Nutzung
- große Verbreitung
- Vertrauen
- sichere Datenspeicherung (in Europa/Deutschland)

Es existiert die grundsätzliche Bereitschaft für eine sichere, einheitliche digitale Identität zu bezahlen, wenn diese allen erläuterten Ansprüchen entspricht. In Bezug auf Unternehmensidentitäten gelten die gleichen Ansprüche. Sie werden aber deutlich sensibler und damit schützenswerter eingeschätzt, schließlich kann der Identitätsdiebstal eines kleinen oder mittleren Unternehmens im WWW schnell das Aus für das gesamte Unternehmen bedeuten.

FAZIT: Fast alle Teilnehmer haben sich bereits mit dem Thema beschäftigt. Der Großteil würde eine sichere digitale Identität vielen Identitäten vorziehen. Die Mehrzahl der Teilnehmer nutzt einen Passwortmanager und fühlt sich damit ausreichend sicher, denkt aber nicht an Backups. Die Frage nach der Sicherheit des Passwortmanagers stellen die meisten nicht. Hier gibt es deutlichen Aufklärungsbedarf. Die Sicherheit von digitalen Identitäten von Unternehmen wird als sehr wichtig, aber noch zu wenig thematisiert, eingeschätzt.

Impulsgeber: M.Sc. Tatiana Gayvoronskaya, Team Security Tech, Hasso-Plattner Institut
Tatiana.Gayvoronskaya@hpi.de

Thementisch 5: Vertrauliche E-Mails – Neues zum Wirtschafts- und Knowhow-Schutz

Worum ging es?

E-Mails sind und bleiben auf absehbare Zeit das Medium für formelle und informelle Kommunikation. Werden E-Mails nicht verschlüsselt oder wird nur ein verschlüsselter Transportweg genutzt, muss man davon ausgehen, dass die Inhalte mitgelesen und ausgewertet werden können.

Im Zusammenhang mit dem Wirtschaftsschutz wird oftmals übersehen, dass es beim Schutz vor dem Zugriff Dritter nicht nur um die eine wichtige E-Mail geht, die einen Vertrag enthält oder das Angebot, das einem potentiellen Mitbewerber nicht in die Hände fallen darf. Es geht auch um die Möglichkeit der Massenauswertung aller E-Mails aller Mitarbeiter. Der Schutz der eigenen IT-Systeme über Firewalls und VPN (Virtual Private Network) ist nicht mehr ausreichend, denn längst haben Hacker die Möglichkeit, sich unter Ausnutzung von bisher unbekannten Sicherheitslücken Zugang zu den internen Systemen zu verschaffen. Die Ransomeware „WannaCry“ ist ein alarmierendes Beispiel hierfür.

Wesentliche Aspekte der Diskussion:

Die Diskussion hat gezeigt, dass nur ca. 10% der Teilnehmer ihren E-Mail-Verkehr verschlüsseln, viele davon nur selektiv – also nur die eine wichtige E-Mail.

Alle Diskutanten haben bestätigt, dass es nach ihren bisherigen Erfahrungen vom normalen Endanwender oder Mitarbeiter nicht zu leisten ist, die Verschlüsselungstechnologien mit Benutzerinteraktion zu verwenden. In vielen Fällen wurde deswegen aufgegeben, zu verschlüsseln, auch wenn man sich den Gefahren bewusst war. Dies deckt sich mit Ergebnissen von Befragungen, die in der deutschen Wirtschaft durchgeführt wurden.
Einem Großteil der Teilnehmer war die Existenz von automatisierten Systemen zur E-Mail-Verschlüsselung unbekannt. Die meisten Fragen ergaben sich aus der Übertragung von Erfahrungen aus dem privaten in den geschäftlichen Zusammenhang. Vielen waren die doch erheblichen Unterschiede dieser beiden Sphären nicht bewusst.

FAZIT: Jede Person und insbesondere jedes Unternehmen muss sich fragen, ob es sich leisten kann, Informationen preiszugeben. Verfügt man über schützenswerte Informationen, deren Verlust potentiell schädlich ist, sollte man diese Informationen schützen. Dieser Schutz kann u.a. durch E-Mail Verschlüsselung gewährleistet werden. Damit dies flächendeckend funktioniert, müssen eine Reihe von Kriterien erfüllt werden. Am wichtigsten ist es, dass Endbenutzer nicht mit der Verschlüsselung belastet werden. Alle notwendigen Technologien müssen automatisch und zentral im Hintergrund betrieben werden. Auch die Aushandlung des jeweils höchsten Schutzniveaus mit dem Kommunikationspartner muss automatisch erfolgen. Die Automatisierung ist auf allen Ebenen des Verschlüsselungsprozesses möglich und ist der Garant für die Absicherung der Kommunikation vor unberechtigtem Zugriff.

Impulsgeber: Dipl. Verw.-wiss. Andreas Nold, Chief Commercial Officer Zertificon Solutions GmbH
a.nold@zertificon.com

Gesamtfazit der Veranstaltung

Umgeben von Begriffen wie Cloud Computing, Smart Home, Industrie 4.0 und geprägt durch täglich neue Nachrichten über Computerkriminalität, ist das Bewusstsein für IT-Sicherheit und vor allem sichere Identitäten bei kleinen und mittleren Unternehmen sehr ausgeprägt. Im digitalen Zeitalter ist Vertrauen eine grundlegende Voraussetzung für verlässliche und erfolgreiche Geschäftsprozesse. Nur wenn in der digitalen Kommunikation davon ausgegangen werden kann, dass der Ansprechpartner tatsächlich derjenige ist, als der er sich ausgibt, sind langfristige Geschäftsbeziehungen denkbar.

Die Workshop Methode World Café war die richtige Wahl, um die Teilnehmer der Veranstaltung zu diesem komplexen Thema miteinander ins Gespräch zu bringen, sich zu vernetzen und aktuelle Herausforderungen in einer wertschätzenden und offenen Atmosphäre zu diskutieren. Da alle Veranstaltungsteilnehmer über ein ausgeprägtes Bewusstsein rund um das Thema Sichere Identitäten und IT-Sicherheit verfügen, konnte schnell und konstruktiv an ersten Problemlösungsszenarien gearbeitet werden.

Die Mehrheit der Teilnehmer hat die Unternehmens-IT bereits als differenzierten Wettbewerbsfaktor verstanden. Vor allem nicht ausreichende oder unklare rechtliche Rahmenbedingungen wurden als wesentlicher Grund für mangelnde IT-Sicherheit benannt. Die DSGVO wird hier Klarheit bringen, KMU aber auch vor große Umsetzungsherausforderungen stellen. Finanzelle Fragen in Bezug auf IT-Sicherheit waren für die Teilnehmer ebenso virulent. Eine gewisse Scheu vor Beratung war jedoch spürbar. Kostenfreie Informationsprogramme für KMU zu den diskutierten Themen in Blended Learning- und Micro Learning-Formaten erscheinen daher als gute Kompromisslösung um Kompetenzen zeit- und ortsunabhängig aufzubauen.

Insgesamt kann gesagt werden: Die Gewährleistung sicherer Identitäten ist für KMU ein wesentlicher Faktor für erfolgreiche Geschäftsbeziehungen. Das Interessen und die Informationsbedarfe rund um das Thema sind riesig. Dem Wunsch nach Vernetzung und vertrauenswürdiger Kommunikation mit Experten konnte durch die Veranstaltung entsprochen werden. Die konstruktive und freundliche Atmosphäre des World Café hat geholfen Berührungsängste abzubauen und strategische Partnerschaften anzubahnen.

Gemeinsam mit dem Sichere Identität Berlin- Brandenburg e.V., der Vereinigung der Unternehmensverbände in Berlin und Brandenburg e.V. und der Mittelstand 4.0 Agentur Kommunikation sind weitere Veranstaltungen dieser Art geplant.

Kontakt

Sichere Identität Berlin-Brandenburg e.V.

http://www.sichere-identitaet-bb.de/

Ansprechpartnerin: Anne-Sophie Braun

Kommandantenstr. 18
10969 Berlin
Telefon: +49 30-2515 077
Telefax: +49 30-2598 1008
E-Mail: info@sichere-identitaet-bb.de

SICHERE IDENTITÄT
BERLIN BRANDENBURG

Vereinigung der Unternehmensverbände in Berlin und Brandenburg e. V.

http://www.uvb-digitallabor.de
http://www.hauptstadtregion.digital

Ansprechpartner: Sven Weickert

Am Schillertheater 2
10625 Berlin
Telefon: +49 30 31005-0
Telefax: +49 30 31005-166
E-Mail: uvb@uvb-online.de

UVB
Unternehmensverbände
Berlin-Brandenburg

Mittelstand 4.0 Agentur Kommunikation

http://kommunikation-mittelstand.digital/

Ansprechpartner: Prof. Dr. Thomas Thiessen

Mittelstand 4.0-Agentur Kommunikation
Sirius Business Park Potsdam
Wetzlarer Straße 30
14482 Potsdam
Telefon: +49 331-982225-09
Telefax: +49 30 - 76683753-19
E-Mail: info@kommunikation-mittelstand.digital

Mittelstand 4.0
Agentur
Kommunikation