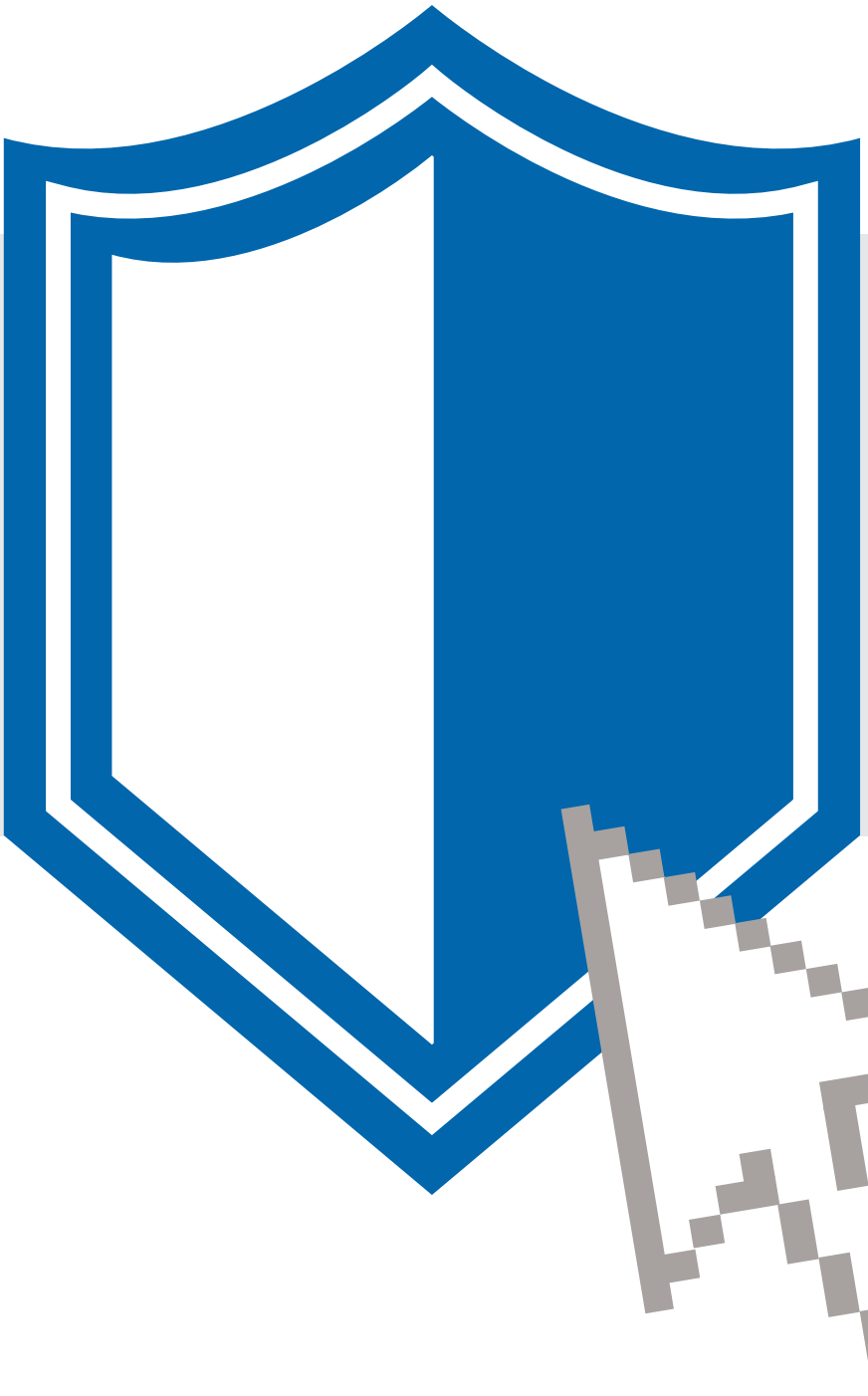
White Paper

IT-Security

Der Risikofaktor Mensch in der Informationssicherheit



H&D International Group

Inhalt

Einleitung

Die beste Leitlinie oder Sicherheitsmaßnahme zeigt sich schließlich wirkungslos, wenn niemand oder nur eine geringe Anzahl der Anwender darüber Kenntnis hat.

Informationssicherheit unterliegt zahlreichen Herausforderungen: Unternehmen sehen sich mit der fortwährenden Aufgabe konfrontiert, Usability und Sicherheitsvorkehrungen unter Berücksichtigung der Kernprozesse miteinander in Einklang zu bringen. Technischer Fortschritt und Innovationen erfordern eine kontinuierliche Auseinandersetzung mit neuen Bedrohungen und Lösungen. Zu geringe Aufwände für Informationssicherheit führen zu mangelhafter technischer Ausstattung, fehlender Sicherheitsinfrastruktur (Authentifizierung, Autorisierung, Malware-Schutz), geringen Personalkapazitäten oder unzureichendem Notfall-/Krisenmanagement. Am wenigsten kalkulierbar und damit ebenso kritisch wiegt zusätzlich der Risikofaktor Mensch. Denn die Mitarbeiter eines Unternehmens bedienen Systeme und Anwendungen. Sie entscheiden darüber, welche Daten in welcher Weise verarbeitet und verbreitet werden. Mitarbeiter sind es, die durch ihre Handlungen einen Informationssicherheitsvorfall verursachen können.

Im Verhältnis zum technischen Fortschritt der letzten 20 Jahre ist die Verantwortung jedes einzelnen Mitarbeiters exponentiell gestiegen. Die gesteigerte Komplexität vieler Systeme und ihre Anwendung über das Internet erhöht die Zahl möglicher Schwachstellen und Risiken. Der Trend hin zu Industrie 4.0[1] veranschaulicht nachvollziehbar, dass menschliche Fehlentscheidungen weitreichende Konsequenzen entlang einer kompletten Wertschöpfungskette haben können. Denn die Verknüpfung verschiedenster Systeme innerhalb einer selbstregulierenden Produktion ist darauf angewiesen, fehlerfrei bedient zu werden. Die Verantwortung, alle technischen Möglichkeiten im Sinne des Unternehmens zu nutzen und dabei die Informationssicherheit zu berücksichtigen, wird mehr denn je an die Mitarbeiter übertragen. Diese Verantwortung wird im Zuge der fortschreitenden Vernetzung stetig wachsen.

Awareness rückt in diesem Zusammenhang zunehmend in den Fokus von IT Dienstleistung. Die allgemeine Bedeutung des Begriffs (Bewusstsein, Erkenntnis, Sensibilisierung) hat sich im Umfeld von Informationssicherheit weiterentwickelt. Hier beschreibt Awareness alle Aktivitäten oder Maßnahmen, die die Mitarbeitersensibilisierung und -aufklärung rund um das Thema Informationssicherheit zum Ziel haben.[2] Die beste Leitlinie oder Sicherheitsmaßnahme zeigt sich schließlich wirkungslos, wenn niemand oder nur eine geringe Anzahl der Anwender darüber Kenntnis hat. Oftmals können gerade die kleinen Dinge eine schadensbringende Wirkung entfalten. So vermag zum Beispiel ein unbeabsichtigter Software-Download die ganze IT-Infrastruktur eines Unternehmens lahm legen. Eine durch Malware unwissentlich geschaffene Schwachstelle kann von externen Angreifern ausgenutzt werden, um Unternehmens- oder Kundendaten zu entwenden. Die Statistik zeigt, dass es sich hierbei keineswegs um Einzelfälle handelt. In den letzten zwei Jahren hat ca. ein Drittel aller deutschen Unternehmen einen Informationssicherheitsvorfall gemeldet[3], die Dunkelziffer wird deutlich darüber liegen.

[1] Die Plattform Industrie 4.0 definiert den Begriff folgendermaßen: „Im Zeitalter der Industrie 4.0 geben die Produkte selbst die Antwort und informieren die Maschinen, was mit ihnen passieren soll. Kurz: Die Objekte werden intelligent. […] Es entsteht ein Internet der Dinge und Dienste. Die physikalische Welt und die virtuelle Welt verschmelzen zu cyber-physischen Systemen." BITKOM (2015): Von smarten Objekten und Maschinen. [online] Homepage: http://www.plattform-i40.de/hintergrund/potenziale

[2] Der Diskurs zum Thema Mitarbeitersensibilisierung bzw. „Risikofaktor Mensch" beschäftigt Informationssicherheitsfachkräfte schon seit vielen Jahren und wird zunehmend breiter geführt. CIO (2005): Mitarbeiter als Gefahr für die IT-Sicherheit. [online] Homepage CIO. URL: http://www.cio.de/a/mitarbeiter-als-gefahr-fuer-die-it-sicherheit,807749; Lochmaier, Lothar (2007): Risikofaktor Mensch: Die Kunst des Social Engineering. [online] Homepage: ZDnet. URL: http://www.zdnet.de/39152145/risikofaktor-mensch-die-kunst-des-social-engineering/; WDR (2015): Forscher untersuchen IT-Sicherheit und den Risikofaktor Mensch. [online] Homepage: WDR. URL: http://www1.wdr.de/studio/bonn/nrwinfos/nachrichten/studios95098.html

[3] Vgl. BITKOM (2015): Digitale Angriffe auf jedes dritte Unternehmen. [online] Homepage: BITKOM. URL: http://www.bitkom.org/files/documents/BITKOM-Presseinfo_IT-Sicherheitsvorfaelle_in_Unternehmen_25_02_2015_v3(1).pdf

Standard-Szenarien

Bei der Betrachtung des „Risikofaktors Mensch“ gibt es zwei grundlegende Dimensionen. Die bewusste Beschädigung bzw. Umgehung der innerbetrieblichen Sicherheitsmechanismen entsteht meist aus Unzufriedenheit, krimineller Energie oder dient dem persönlichen Vorteil. Die unbewusste oder ungewollte Schädigung eines Unternehmens hingegen wird durch Unwissenheit oder Unachtsamkeit verursacht.

In beiden Fällen nimmt das betroffene Unternehmen Schaden, den es im Anschluss zu kompensieren gilt. Die Schadenshöhe ist hierbei von Art und Umfang des Incidents abhängig. Die eigentliche Ausführung einer Handlung, die zu einem Incident führt, ist zwar von jedem einzelnen Verursacher individuell abhängig, dennoch sind klare Muster und Szenarien vorhersehbar und durch die Praxis belegt.

Die unbewusste oder ungewollte Schädigung eines Unternehmens hingegen wird durch Unwissenheit oder Unachtsamkeit verursacht.

Bewusste Beschädigung

Mitnahme von Kundendaten und Unternehmensgeheimnissen

Selten verläuft der Austritt eines Mitarbeiters in beiderseitigem Einverständnis bzw. für beide Seiten gleichermaßen einvernehmlich. In einzelnen Fällen kopieren scheidende Mitarbeiter Kunden- oder Auftragsdaten für den neuen Arbeitgeber.

Absichtliches in-Kauf-nehmen von Risiken

Sie sind sich der Konsequenzen ihres Tuns in aller Regel bewusst, handeln dennoch (oder gerade deshalb) fernab der Sicherheitsrichtlinien.

Mitarbeiter, die gedanklich bereits mit ihrem Arbeitgeber abgeschlossen haben, handeln häufig nachlässig. Sie sind sich der Konsequenzen ihres Tuns in aller Regel bewusst, handeln dennoch (oder gerade deshalb) fernab der Sicherheitsrichtlinien. Dies zeigt sich beispielsweise in dem Besuch von unsicheren Internet-Seiten oder in dem Download und der Installation von Software aus nicht vertrauenswürdiger Quelle. Dadurch erleidet das Unternehmen beispielsweise eine Infizierung mit Malware[4].

Sabotage

In extremen Fällen entschließen sich Mitarbeiter aus Unmut gegenüber ihrem Arbeitgeber zur gezielten Sabotage, indem die unternehmenseigene IT-Infrastruktur lahmgelegt wird oder bestimmte Anwendungen bewusst blockiert und außer Kraft gesetzt werden. Sobald ein Mitarbeiter (intern) mit einem Angreifer (extern) zusammenarbeitet, sind bestehende Sicherheitssysteme in der Regel wirkungslos.

[4] Definition von Malware: Cisco (2015): What Is The Difference: Viruses, Worms, Trojans, and Bots? [online] Homepage: Cisco. URL: http://www.cisco.com/web/about/security/intelligence/virus-worm-diffs.html

Unbewusste Schädigung

Passwörter (Weitergabe, schwache Passwörter)

Das Opfer soll durch die Manipulation zu Handlungen veranlasst werden, die dem Angreifer Zugriff auf unternehmenseigene Daten ermöglichen.

Passwörter werden weitergegeben, um Kollegen einen schnellen Zugriff auf gemeinsam genutzte Systeme zu ermöglichen oder um personalisierte Anwendungen für einen kurzen Moment einer dritten Person zur Verfügung zu stellen. Vermeintliche Kleinigkeiten, dennoch handelt es sich bereits hier um klare Verstöße gegen den Datenschutz. Viele Mitarbeiter scheitern zudem an der Wahl starker Passwörter. Passwort-Richtlinien vieler Unternehmen lehnen „123456“ zwar mittlerweile ab, dennoch entscheiden sich viele Anwender für Kombinationen, die sie sich in erster Linie leicht merken können. Angreifern wiederum, die sich auf das Hacken von Passwörtern spezialisiert haben, steht heutzutage eine Reihe von Hilfsmitteln zur Verfügung, so dass logische Kombinationen oder Wörter aus dem Wörterbuch keine nennenswerte Hürde darstellen.[5]
Für viele Anwender besteht angesichts der Fülle der genutzten Systeme eine zusätzliche Herausforderung in der Zuordnung von Passwort und dazugehörigem System/Gerät. Die beliebteste Lösung ist nach wie vor das Notieren des Passworts auf einem Post-It, das dann unter den Rechner oder die Tastatur geklebt wird. Eine weitere, ebenso kritische Methode ist die Verwendung eines einzigen (schwachen) Passworts für alle Anwendungen und Systeme.

Download von Dateien mit Schadware, Viren, Trojanern

Im Internet kursiert eine Vielzahl an Schadware und Anwendungen, die auf ebenso zahlreiche Weise in das Unternehmen eintreten. Ein Installieren dieser Programme durch den Mitarbeiter ist mittlerweile meist nicht mehr notwendig. Sie sind so programmiert, dass sie sich von selbst im Zielsystem festsetzen und automatisiert ablaufen.

Reaktion auf Social Engineering-Aktivitäten[6]

Immer noch geben Mitarbeiter ihre Nutzernamen und Passwörter ohne Zögern an einen (angeblichen) Administrator weiter. Anhänge aus E-Mails werden ebenso leichtfertig geöffnet, da die Nachricht scheinbar von einem Kollegen versendet wurde. Besonders in großen Unternehmen sind dem einzelnen Mitarbeiter auch nicht alle Kollegen persönlich oder namentlich bekannt, so dass Gutgläubigkeit und Hilfsbereitschaft eine unglückliche Kombination erzeugen.
Social Engineering im Umfeld von Informationssicherheit beschreibt die gezielte Manipulation und Täuschung von Mitarbeitern, um an bestimmte Informationen wie beispielsweise Zugangsdaten oder Passwörter zu gelangen oder um versteckte Schadware zu installieren. Hierzu werden beispielsweise Mails (inkl. Hyperlinks oder Anhänge) versendet, die den Anschein erwecken, aus einer vertrauenswürdigen Quelle zu stammen (Spoofing). Gelegentlich wird Social Engineering auch mittels simpler Telefonanrufe betrieben, ebenfalls unter Vorspiegelung einer falschen Identität. Das Opfer soll durch die Manipulation zu Handlungen veranlasst werden, die dem Angreifer Zugriff auf unternehmenseigene Daten ermöglichen. Als Reaktion auf die zunehmende Sensibilisierung von Mitarbeitern, gehen Täter gleichermaßen geschickter vor (auch viele kleine Puzzlestücke ergeben ein Gesamtbild).

[5] Vgl.: Splashdata (2015): “123456” Maintains the Top Spot on Splashdata’s Annual “Worst Passwords” List. [online] Homepage: Splashdata. URL: http://splashdata.com/press/worst-passwords-of-2014.htm. Grundlage der Splashdata- Auswertung: 3,3 Mio. öffentlich gewordene Passwörter im WWW für das Jahr 2014.
[6] Definition von Social Engineering und weitere, anschauliche Beispiele: Bundesamt für Sicherheit in der Informationstechnik (2015): Social Engineering. [online] Homepage: Bundesamt für Sicherheit in der Informationstechnik. URL: https://www.bsi.bund.de/DE/Themen/ITGrundschutz/ITGrundschutzKataloge/Inhalt/_content/g/g05/g05042.html

Nicht-Melden von verdächtigen Ereignissen

Ausschlaggebend für die erfolgreiche Abwehr eines Angriffs ist die Kenntnis über den Vorfall. Mitarbeiter müssen explizit dazu aufgefordert werden, fragwürdige E-Mails oder verdächtige Vorfälle an die zuständigen Sicherheitsverantwortlichen zu melden. Nur so können präventive oder reaktive Maßnahmen eingeleitet werden. Existiert kein solcher Prozess, läuft das Unternehmen Gefahr, Bedrohungen nicht (rechtzeitig) identifizieren zu können. Für das dazu erforderliche Betriebsklima ist zwangsläufig eine gesunde Kommunikationskultur notwendig.

Installieren von nicht-autorisierten Anwendungen/Applikationen

Gerade Mitarbeiter mit Administrationsprivilegien installieren gerne eigene Anwendungen oder IT-Lösungen – in der Annahme, dass das, was am Heimrechner für einen bestimmten Zweck hervorragend funktioniert, auch am Arbeitsplatz eingesetzt werden kann. Damit wird jedoch ungeprüfte, nicht-autorisierte Software zum Einsatz gebracht. Schwachstellen sind auf diese Weise nicht kalkulierbar. Außerdem werden genannte Applikationen bei Sicherheitsüberprüfungen nicht berücksichtigt, da die Verantwortlichen keine Kenntnis von ihnen haben. Software-Lizenzen unterscheiden außerdem zwischen privater und gewerblicher Nutzung (durch ein Unternehmen), wobei der gewerbliche Einsatz in der Regel mit Lizenzgebühren verknüpft ist. Des Weiteren bergen Applikationen, die über das WWW frei verfügbar sind, immer das Risiko des Missbrauchs der zum Zweck der Anwendung übermittelten Daten.

Eine Variante des Bring-Your-Own-Device-Risikos ist der Missbrauch oder gar der Verlust eines privaten Speichermediums mit sensiblen Daten.

Verwendung von mitgebrachten Geräten oder Speichermedien

Bring-Your-Own-Device bezeichnet das Mitbringen von privaten Geräten wie Smartphone, USB-Stick oder externer Festplatte etc. zur Verwendung im Unternehmen. Die Gefahr besteht darin, dass das externe Gerät Zugang zum Unternehmensnetzwerk erhält und jeglicher installierter Schadware Einlass gewähren kann.
Eine Variante des Bring-Your-Own-Device-Risikos ist der Missbrauch oder gar der Verlust eines privaten Speichermediums mit sensiblen Daten. Unternehmensdaten sind nur im Sicherheitsrahmen des Firmennetzwerks geschützt, auf einem privaten Medium (z. B. für Homeoffice-Zwecke) unterliegen sie lediglich der Verantwortung des Mitarbeiters und sind daher ungeschützt.

Einsatz von präparierten mobilen Datenträgernn

Häufig werden mit Schad- oder Spyware präparierte Datenträger von Angreifern in der Nähe des Unternehmens platziert oder im Umfeld von Messen und Veranstaltungen verteilt. Der neugierige aber unwissende Mitarbeiter nimmt das Speichermedium an sich und schließt es – im besten Fall für die Angreifer – sogleich an den firmeninternen Rechner an, um die Inhalte abzurufen. Hierdurch können Angreifer nicht-autorisierten Zugriff auf unternehmensinterne Daten bekommen oder das Unternehmensnetz infizieren.[7]

[7] Vgl.: Knoke, Felix (2011): Finger weg von gefundenen USB-Sticks. [online] Homepage: Spiegel Online. URL: http://www.spiegel.de/netzwelt/web/netzwelt-ticker-finger-weg-von-gefundenen-usb-sticks-a-802443.html

Folgen eines Incidents und Gegenmaßnahmen

Interne Angriffe stellen mittlerweile eine ernstzunehmende Bedrohung dar: ca. zwei Drittel aller in Deutschland gemeldeten Angriffe wurden von einem Mitarbeiter des betroffenen Unternehmens initiiert.[8] Die Verantwortung zur Vermeidung solcher Incidents liegt in der Mitarbeiterzufriedenheit bzw. ist im Umfeld von Mitarbeiterführung verankert. Jedoch können Unternehmen Maßnahmen ergreifen, um den potentiellen Schaden so gering wie möglich zu halten. Funktionierende Informationssicherheitssysteme können einen böswilligen, internen Angriff nicht abwehren, sie können es einem mutwilligen Verursacher jedoch erschweren.[9] In der reaktiven Behandlung eines Incidents besteht für ein Unternehmen zusätzlich die Option, auf Grundlage forensischer[10] Ermittlungen und Beweise rechtlich gegen den Verursacher vorzugehen[11], da es sich nicht nur um einen Verstoß gegen interne Informationssicherheitsrichtlinien, sondern um die Verletzung arbeitsvertraglicher Vereinbarungen handelt. Datenschutzrichtlinien, Social-Media-Guidelines oder auch Sicherheitsleitfäden sollten aus diesem Grund fester Bestandteil von Einstellungsprozessen sowie Mitarbeiterbelehrungen sein.

Die Verantwortung zur Vermeidung solcher Incidents liegt in der Mitarbeiterzufriedenheit bzw. ist im Umfeld von Mitarbeiterführung verankert.

Die Folgen eines Security-Incidents wiegen auf unterschiedliche Weise schwer. Um den operativen Betrieb schnell wieder aufnehmen zu können oder die Sicherheitslücke zu schließen, müssen kostspielige Maßnahmen ergriffen werden. Die Kosten für den Austausch von Geräten oder das Aufspielen einer neuen Software sowie Lohnkosten, zeitlicher Aufwand und die durch Systemausfälle entstandenen Verluste addieren sich entsprechend. So entstehen dem Unternehmen hohe Kosten. Veröffentlichte Produkt- oder Produktionsdaten bedeuten einen Verlust an Know-how an die Konkurrenz und damit einen Wettbewerbsnachteil.

Im Fall von gehackten Kundendaten wird ein Incident auch um eine rechtliche Dimension erweitert. Insbesondere Kundendaten und/oder persönliche Daten unterliegen einem besonderen gesetzlichen Schutz und dürfen nur unter strengen Auflagen verarbeitet werden.[12]
Zusätzlich bedeutet das öffentliche Bekanntwerden eines Incidents immer einen Reputationsverlust. Es muss die Frage nach der Ursache beantwortet werden. Zudem wird es nur mit großem Aufwand möglich sein, verlorenes Vertrauen in die unternehmerische Integrität zurückzugewinnen.[13]
Zusammenfassend liegt der Abwehr von Angriffen eine einfache Logikkette zugrunde: Risikoanalyse, Prävention, Identifizierung, Reaktion und Lessons Learned. Alle genannten Beispiele eint zudem, dass es technisch nur begrenzte Möglichkeiten gibt, einem Angriff oder einer Aktion im Vorfeld entgegenzuwirken. Auf die Mitarbeiter jedoch kann durchaus Einfluss genommen werden. Mitarbeitersensibilisierung ist eines der verlässlichsten Mittel der präventiven Abwehr von Incidents. Analog zum Handeln im privaten Umfeld ist bewusstes Agieren und gesundes Misstrauen am Arbeitsplatz unerlässlich.

[8] Vgl.: Bundesamt für Verfassungsschutz (2015). Sicherheitslücke Mensch – Der Innentäter als größte Bedrohung für die Unternehmen. [online] Homepage: Bundesamt für Verfassungsschutz. URL: http://www.verfassungsschutz.de/de/download-manager/_faltblatt-2014-04-sicherheitsluecke-mensch.pdf
[9] Ein effizientes Echtzeit- Access- und Identity Management kann beispielsweise dafür sorgen, dass Berechtigungen für Systeme, Zugriffs- oder Zutrittsberechtigungen prozesskonform verwaltet und organisiert sind und im Falle eines Austritts oder Abteilungswechsels umgehend angepasst werden.
[10] IT-Forensik beschreibt die Erfassung, Analyse und Auswertung digitaler Spuren im Zusammenhang mit Incidents und der dazugehörigen Ermittlung detaillierter Handlungsabläufe und Verursachern, z. B. zur Ermittlung von Verantwortlichen eines Incidents.
[11] Im Hinblick auf die öffentliche Wahrnehmung ist eine Strategie situationsbedingt festzulegen (Eingeständnis des Vorfalls oder Schadensbegrenzung oder Schadensersatzforderung).
[12] Vgl.: Bundesministerium der Justiz und für Verbraucherschutz (2015). Bundesdatenschutzgesetz. [online] Homepage: juris GmbH: URL: http://www.gesetze-im-internet.de/bdsg_1990/index.html
[13] Eines der jüngsten Beispiele, vgl.: Spiegel Online (2015): Umstrittener Fahrdienst: Datenleck bei Uber. [online] Homepage: Spiegel Online. URL: http://www.spiegel.de/netzwelt/web/uber-datenleck-beim-umstrittenen-fahrdienst-a-1021091.html. Besonders spektakulär war der Datenklau bei Sony, der Millionen von Kundendaten betraf – vgl.: Heise Online (2011): Angriff auf Playstation Network: Persönliche Daten von Millionen Kunden gestohlen. [online] Homepage: Heise. URL: http://www.heise.de/newsticker/meldung/Angriff-auf-Playstation-Network-Persoenliche-Daten-von-Millionen-Kunden-gestohlen-1233136.html

Lösung: Awareness!

Awareness-Maßnahmen zur Verbesserung der Informationssicherheit sind nicht Teil der Wertschöpfungskette eines Unternehmens. Besonders in Zeiten von schmalen IT-Budgets werden sie häufig unterpriorisiert. Die Aufwendungen für eine regelmäßige Mitarbeiterschulung stehen allerdings in keinem Verhältnis zum potentiellen Schaden bei Eintritt eines Incidents. Grundsätzlich ist Awareness eine Maßnahme wie viele andere Sicherheitsvorkehrungen auch. Der Einsatz eines Virenscanners oder einer Firewall erschließt sich vielen Entscheidern jedoch offenbar noch unmittelbarer als die Weiterbildung ihrer Mitarbeiter. Im Detail ist zu definieren, welcher Anwenderkreis angesprochen werden soll. Ein IT-Administrator benötigt andere Schulungsinhalte als ein Backoffice-Supporter oder ein Produktionsmitarbeiter. Awareness-Verantwortliche müssen dabei immer bedenken: Der Mensch ist ein „Gewohnheitstier“ und geht gerne den Weg des geringsten Widerstandes. Es ist eine Herausforderung, Überzeugung und Motivation im Hinblick auf bereits vermittelte Inhalte über einen längeren Zeitraum aufrechtzuerhalten. Besonders wenn es darum geht, unbequeme oder unpraktische Handlungsweisen (lange Passwörter, Verifizierung von Absendern oder Anrufern etc.) im Alltag umzusetzen, sinkt die Moral proportional zum zeitlichen Abstand zur Schulung. Eine Ersteinweisung in unternehmenseigene Richtlinien und Sicherheitsleitfäden gehört vielfach schon zum standardisierten Onboarding neuer Mitarbeiter. Hier darf Sensibilisierung nicht aufhören. Abgesehen von der Vermeidung grundsätzlicher Bedrohungen, wissen geschulte Mitarbeiter auch zukünftig umsichtig und verantwortungsbewusst zu agieren.

Awareness-Verantwortliche müssen dabei immer bedenken: Der Mensch ist ein „Gewohnheitstier“ und geht gerne den Weg des geringsten Widerstandes.

Fazit

Ob und in welchen Intervallen eine Schulung oder eine Awareness-Kampagne sinnvoll ist, muss jedes Unternehmens-Management für sich selbst entscheiden. Angesichts der Risiken, die sich aus ungeschultem Personal in Kombination mit den wachsenden und zunehmend professionellen Angriffsmethoden ergeben, ist eine regelmäßige Schulung jedoch dringend empfehlenswert. Awareness bietet grundlegende Orientierung für die tagtägliche Umsetzung von Informationssicherheit sowie ihren zahlreichen Herausforderungen und trägt dadurch maßgeblich zu einem stabilen, wettbewerbsfähigen Unternehmen bei.

Verfasser: Robert Philipp Bock

Ansprechpartner

Jan Schendel
Service Line Manager IT-Security
Tel: +49 5361 308560
E-Mail: jan.schendel@hud.de

H&D International Group

August-Horch-Straße 1
38518 Gifhorn

Tel: +49 5371 960 0
E-Mail: kommunikation@hud.de
www.hud.de