
COMPUTERWOCHE
VON IDG

Hackerangriff von Innen

So wird man zum Innentäter

von Dennis Buroh

Foto: turlakova - shutterstock.com

Inhalt

Hackerangriff von Innen

So wird man zum Innentäter

von Dennis Buroh

Die Furcht vor Hackerangriffen greift im Unternehmensumfeld schon länger um sich. Dabei geht die Gefahr - bewusst und unbewusst - oft von den eigenen Mitarbeitern aus.

Viele Unternehmen betreiben einen hohen technischen Aufwand, um die IT-Schutzziele zu erreichen. In der Praxis orientiert sich die angestrebte Informationssicherheit im Rahmen des IT-Sicherheitsmanagements [1] an verschiedenen internationalen Standards, wie der ISO/IEC 2700-Reihe [2]. Dabei verlässt man sich inzwischen auf immer ausgeklügeltere Techniken.

Regelmäßig unterschätzt, wenn es um IT-Sicherheit geht: der Faktor Mensch.
Foto: turlakova - shutterstock.com

1 http://www.computerwoche.de/a/wie-wird-man-it-security-profi,2520172
2 http://www.computerwoche.de/a/nis-richtlinie-und-neue-tools-fuer-den-mittelstand,3313854

Es wäre jedoch illusorisch anzunehmen, dass alleine durch technische Maßnahmen, wie Firewalls [3], Zugriffbeschränkungen oder ein Privileged Identity Management (PIM), hundertprozentige Sicherheit gewährleistet werden kann. Die Erfahrungen der verschiedensten Unternehmen zeigen, dass insbesondere der Faktor Mensch [4] häufig stark unterschätzt wird. Vor allem bei kritischen Infrastrukturen gibt es eine Vielzahl von Nutzern und beteiligten Personen, die nicht immer direkt durch technische Maßnahmen überwacht werden können.

[Hinweis auf Bildergalerie: Top 10: Diese Mitarbeiter gefährden Ihre IT-Sicherheit] gal1

Innentäter: Status Quo

Laut einer Studie des deutschen Verfassungsschutzes [5] aus dem Jahr 2014 wurden mehr als 30 Prozent der öffentlich gewordenen Hackerangriffe [6] durch Innentäter ausgelöst. Die Dunkelziffer liegt wesentlich höher. Innentäter können ihr Wissen um die Strukturen des Unternehmens und dessen Sicherheitsschwachstellen jederzeit ausnutzen. Hinzu kommt, dass die meisten Mitarbeiter über die nötigen Rechte verfügen, Firewalls und Zugriffsbeschränkungen zu umgehen, um ihre Regeltätigkeit ausüben zu können. Ein Innentäter [7] besitzt also ausreichend Informationen, um einem Unternehmen Schaden zuzufügen und seine Aktionen anschließend zu verschleiern.

Durch die notwendige Einbindung externer Fachkräfte oder Dienstleister in interne Arbeitsprozesse, um am dynamischen, nationalen und internationalen Markt zu bestehen, wird das Bedrohungsszenario wesentlich erweitert. Und bei einem externen Mitarbeiter liegt die Hemmschwelle wesentlich niedriger, wenn es darum geht Daten und Informationen des Kunden zu entwenden.

[Hinweis auf Bildergalerie: Die größten Cyberangriffe auf Unternehmen] gal2

Motive: So werden Mitarbeiter zur Bedrohung

Es gibt verschiedene Gründe, warum aus loyalen Mitarbeitern aktive Innentäter [8] werden. Laut Bundesverfassungsschutz und einschlägiger Studien zum Thema sind folgende Beweggründe und Indikatoren hervorzuheben:

- Unzufriedenheit am Arbeitsplatz, fehlende Identifikation mit dem Unternehmen
- Diskrepanzen im beruflichen Werdegang
- Fehlende Schulung am Produkt
- Unkenntnis über Arbeitsprozesse
- Auffällige Neugier
- Whistleblowing
- Nutzung von mobilen Datenträgern
- Überschreitung der Zugriffsberechtigung

[3] http://www.computerwoche.de/a/wirkungslose-it-sicherheits-massnahmen,3229874

[4] http://www.computerwoche.de/a/datenschutz-un-sicherheitsfaktor-mensch,3229132

[5] https://www.verfassungsschutz.de/de/aktuelles/zur-sache/zs-2015-001-maassen-im-audit-committee-quarterly-2014-04

[6] http://www.computerwoche.de/a/selbst-schuld,3327016

[7] http://www.computerwoche.de/a/der-blinde-fleck-der-it-sicherheit,3214236

[8] http://www.computerwoche.de/a/inside-jobs-was-unternehmen-tun-koennen,3324705

Es geht also nicht immer ums Geld. Enttäuschung, Frust am Arbeitsplatz [9] oder private Probleme spielen ebenso mit hinein, wie die einfache Unkenntnis über sensible Schwachstellen in Arbeitsabläufen. Amerikanische Studien gehen noch einen Schritt weiter. Wissenschaftler des "American Board of Professional Psychology [10]" (ABPP) beleuchten in ihrem forensischen Ansatz die psychologischen Risikofaktoren, die Mitarbeiter überhaupt erst anfällig für eine Innentäterschaft machen.

An erster Stelle steht natürlich die psychische und gesundheitliche Verfassung [11], die sich unmittelbar auf die Wahrnehmungs- und Urteilsfähigkeit des Mitarbeiters auswirkt, insbesondere auf dessen soziale Interaktion und Performance am Arbeitsplatz. Die daraus gebildete Persönlichkeit des Einzelnen, seine sozialen Fähigkeiten [12] und seine Vorgehensweise in der Entscheidungsfindung sind die Faktoren, die im Weiteren dessen Eigenwahrnehmung und dessen Wahrnehmung der Umgebung beeinflussen. Sie bestimmen die Wahrscheinlichkeit sozialer Konflikte und möglicher Isolation. Nach außen hin zeigt sich dies beispielsweise durch:

- Probleme in der Zusammenarbeit [13],
- Impulsivität,
- das Gefühl über den Regeln zu stehen,
- die Schwierigkeit bei der Übernahme von Verantwortung
- und der Tendenz, eher andere für Fehler verantwortlich zu machen.

Kommen persönliche Stressfaktoren wie finanzielle Schwierigkeiten oder Krankheiten und Zurücksetzung außerhalb des Arbeitswelt hinzu, können die beruflichen Stressfaktoren [14] (Ärger mit dem Vorgesetzten, drohende Entlassung oder unerfüllte Erwartungen) weiter verstärkt werden. Es droht zur Eskalation zu kommen. In jedem Fall festigt sich so eine verstimmte Grundhaltung, die in der Regel mehr und mehr offensichtlich zu Tage tritt. Interessant ist dabei die Umkehr der Wertewelt: Falsches Benehmen [15] und Vorteilsnahme werden als lohnend eingestuft, harte Arbeit nicht. Kollegen wollen einem eher schaden und müssen besiegt werden, so wie das ganze Unternehmen, das die eigenen Interessen nicht schützen will. Offensichtlicher Ärger [16] schlägt um in das Gefühl, provoziert zu werden und nun quasi zum Handeln gezwungen zu sein.

Sollten Unternehmen nun schon bei der Auswahl der Mitarbeiter möglichst all diese Kriterien einbeziehen und psychologische Integritätstests [17] durchführen? Wenn es danach ginge, müsste es zumindest eine Gruppe schwer haben: Laut begleitender empirischer Forschung der ABPP-Wissenschaftler ist der klassische Innentäter nämlich männlich, 37 Jahre alt und hat eine technische Position inne. Er kann Ingenieur, Wissenschaftler, Manager oder Programmierer sein. Die Mehrheit dieser Täter hat Vereinbarungen in Sachen geistiges Eigentum unterschrieben. Eine Compliance-Politik [18] allein reicht da wohl nicht aus.

9 http://www.computerwoche.de/a/die-acht-stressigsten-it-jobs,3223233
10 http://www.abpp.org/i4a/pages/index.cfm?pageid=3285
11 http://www.computerwoche.de/a/wenn-software-in-die-seele-des-bewerbers-schaut,3312154
12 http://www.computerwoche.de/a/die-elf-wichtigsten-soft-skills,1902818
13 http://www.computerwoche.de/a/wenn-kollegen-gift-fuers-teamwork-sind,3316012
14 http://www.computerwoche.de/a/jeder-mitarbeiter-leidet-anders-unter-stress,3260708
15 http://www.computerwoche.de/a/soforthilfe-fuer-peinliche-knigge-blackouts,1892144
16 http://www.computerwoche.de/a/das-laesst-softwareentwickler-austicken,3324531
17 http://www.computerwoche.de/a/die-psychologie-der-e-mail-scams,3067073

Allerdings müssen genannte Gründe oder Indikatoren nicht zutreffen, damit es zu einem gezielten "Datenverrat" kommt. Ein Mitarbeiter oder externer Dienstleister kann die Kontrolle über seinen User Account beispielsweise durch einen Hackerangriff [19], eine gezielte oder ungezielte Malware-Infektion [20] und ähnliches verlieren, so dass unter seinem Account (und damit mit seinen Mitarbeiterrechten) dem Unternehmen Schaden zugefügt wird. Ein gezielter Akt der Cyberspionage [21] (Advanced Persistant Threats) wird im Schnitt übrigens erst nach 243 Tagen entdeckt.

Hacker inside: So greifen Insider an

Das Bundesamt für Sicherheit in der Informationstechnik (BSI) hat die möglichen Angriffe durch Innentäter bereits 2013 beschrieben und dabei vor allem drei Handlungsmuster festgehalten:

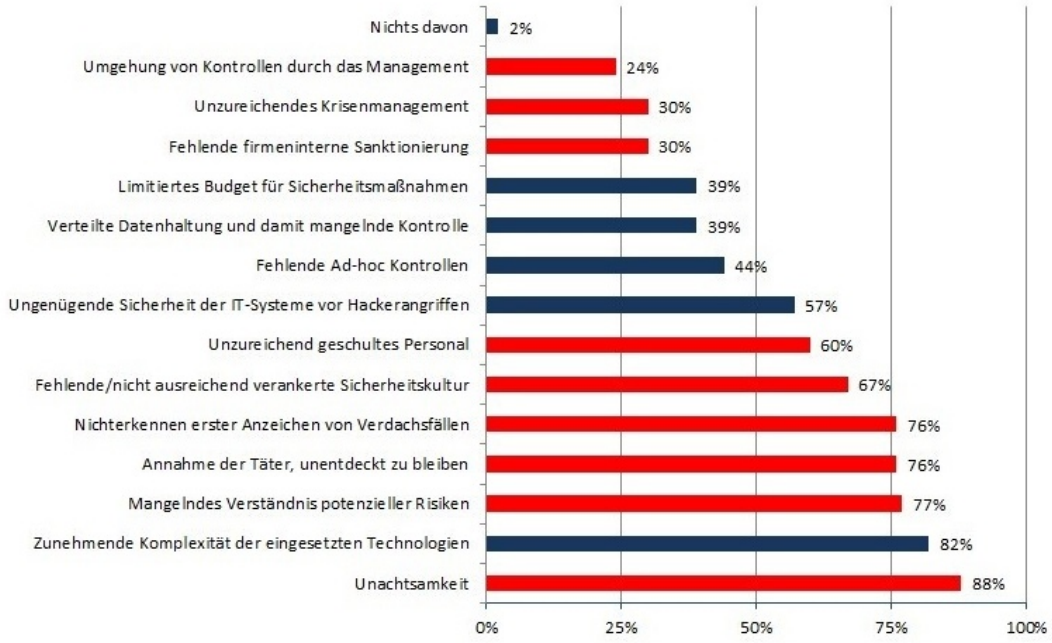
Data Leakage: Dieser Begriff umschreibt den Verlust, beziehungsweise den Diebstahl von Informationen durch Zugriffsmöglichkeiten auf Fileserver, Datenträger oder die IT-Systeme.

Social Engineering: Zwischenmenschliche Manipulation findet insbesondere zur Vorbereitung von Folgeangriffen statt, beispielsweise durch Ermittlung von Ansprechpartnern, Prozessbeschreibungen, IT-Architekturen oder Steuerprogrammen. Personen mit Zugang zu bestimmten Bereichen könnten zudem andere Mitarbeiter dazu verleiten, Software zu installieren, Konfigurationsänderungen vorzunehmen oder kryptografische Schlüssel herauszugeben. Das Ziel: die Eröffnung von Angriffspfaden.

Sabotage: Oftmals begründet durch politische oder wirtschaftliche Interessen ist dies eine Angriffsform, bei der eine erhöhte Bedrohung durch Innentäter ausgeht.

Dass sich bereits viele Unternehmen dieser Problematiken bewusst sind, zeigen zum Beispiel die Studienergebnisse von KPMG [22]: Acht von zwölf der meistgenannten Ursachen für Internetkriminalität sind demnach Innentätern zuzuordnen.

18 http://www.computerwoche.de/p/compliance-und-recht,3147
19 http://www.computerwoche.de/a/wenn-der-hacker-ueber-linkedin-kommt,3329602
20 http://www.computerwoche.de/a/woran-sie-merken-dass-sie-gehackt-wurden,2553914
21 http://www.computerwoche.de/a/hackerangriffe-worst-of-2016,3329101
22 https://home.kpmg.com/de/de/home/themen/2015/03/studie--e-crime---computerkriminalitaet-in-der-deutschen-wirtsch.html



Begünstigende Faktoren für Cyberkriminalität laut KPMG.
Foto: KPMG

Besonders hervorzuheben ist in diesem Zusammenhang auch das unbeabsichtigte Fehlverhalten von Mitarbeitern. In einer Umfrage [23] der vom BSI initiierten Allianz für Cybersicherheit war dies der meistgenannte Grund hinter "erfolgreichen" Hackerangriffen [24].

So brachte es beispielsweise ein technischer Mitarbeiter von Amazon zu unbeabsichtigtem "Innentäter-Ruhm" - und verursachte dabei einen Schaden von mehr als 150 Millionen Dollar. Was war passiert? Der Mitarbeiter führte eine routinemäßige Server-Wartung durch und beschloss zur Beschleunigung seiner Arbeitsaufgabe, mehr Server als üblich direkt in die Wartung zu setzen und mit neuer Software zu versorgen. Blöderweise verursachte diese Entscheidung eine Kettenreaktion durch die unzählige Webshops und Webdienste über Stunden nicht mehr erreichbar waren.

Fälle wie dieser sind in Unternehmen jeder Größe denkbar. Ebenso wie folgender Fall: Ein Mitarbeiter tauscht sich regelmäßig in verschiedenen Chats mit anderen Menschen über sein Hobby aus. Dort wird er von einem externen Hacker gefunden und kontaktiert. Ist erstes Vertrauen aufgebaut, schickt dieser eine infizierte Datei - und hört, beziehungsweise liest ab diesem Zeitpunkt mit. Diese Form des Social Engineering [25] führt nicht unmittelbar zu einer missbräuchlichen Folgehandlung. Der Täter wartet nun ab, bis der Mitarbeiter über sein Facebook-Profil beispielsweise seine Hochzeitsreise ankündigt. Nach der Abreise in die Flitterwochen folgt der "Zugriff". Mit den Zugangsdaten des Urlaubers kann der Hacker [26] nun voraussichtlich unbehelligt Daten stehlen.

[23] https://www.allianz-fuer-cybersicherheit.de/ACS/DE/_/downloads/cybersicherheitslage/umfrage2015_ergebnisse.pdf?__blob=publicationFile&v=4
[24] http://www.computerwoche.de/a/kriminelle-hacker-unterschaetzte-gefahr,3314112
[25] http://www.computerwoche.de/a/social-media-stairway-to-malware,3260667
[26] http://www.computerwoche.de/a/zehn-extrem-hacks,3316462

Häufig geht mit der Veröffentlichung von Hacks und Kompromittierungen durch Innentäter auch ein enormer Imageschaden für Unternehmen einher. Kein Wunder: Wer vertraut schon einem Webshop, der die eigenen Kunden beziehungsweise deren Accounts nicht schützen kann? Ebay durchlebte diese schmerzhafte Erfahrung bereits im März 2014. Damals wurden über gehackte Mitarbeiter-Konten [27] mehr als 145 Millionen Passwörter und E-Mail-Adressen gestohlen. Die Aktie des US-Unternehmens brach nach Bekanntwerden des Hacks massiv ein.

Fazit: So schützen sich Unternehmen

Compliance-Richtlinien alleine reichen nicht aus, um Innentäter beziehungsweise Hacks und Angriffe durch diese zu verhindern. Klare Verhaltensregeln - auch im Umgang von Kollegen und Führungskräften untereinander - sowie geeignete, interne Kontrollsysteme sind zusätzlich unabdingbar.

Die größte Herausforderung für die IT-Sicherheit [28] bleibt die (frühzeitige) Erkennung krimineller oder schädlicher Aktivitäten. Allerdings kann bereits das einfache Monitoring von Mitarbeiteraktivitäten auf kritischen Systemen bei einem Sicherheitsvorfall die Kapazitäten der IT-Security-Abteilung sprengen. Zudem kann ein solches Vorgehen bei den überwachten Mitarbeitern zu großem Unmut führen, da ihre gesamte Arbeitsleistung unter Generalverdacht steht. Ein generelles Aufzeichnen aller Aktivitäten des Mitarbeiters - ohne dass dabei eine konkrete Gefahr für das Unternehmen besteht - verstößt ohnehin gegen das Computergrundrecht [29].

Der Versuch, IT-Sicherheit [30] nur mit technischen Mitteln zu erreichen, ist sehr wahrscheinlich zum Scheitern verurteilt. Durch das Outsourcing von Abteilungen oder Dienstleistungen sinkt diese Wahrscheinlichkeit noch einmal. Denn weitere neue und ungeschulte Personen, die in die IT-Sicherheit einbezogen werden müssen, eröffnen zusätzliche Schwachstellen und Fehlerquellen im Unternehmen. Im Umgang mit kritischen Systemen [31] und im IT-Sicherheitsmanagement ganz allgemein nimmt der Faktor Mensch nun einmal die Hauptrolle ein.

Unternehmen sollten sich in jedem Fall aktiv mit dem Thema Innentäter auseinandersetzen. Ein einfaches Monitoring oder Fokussieren auf Log-Files ist hier nicht ausreichend und vermittelt darüber hinaus allzu oft ein falsches Gefühl von Sicherheit. Ein schlichtes Log-File-Management-Monitoring bildet zudem keinen kompletten Nachweis zur Sicherstellung der EU-Datenschutz-Grundverordnung [32] dar. Eine komplette Prozessabbildung durch Applikations-Log-Files wird nie möglich sein, zumal nicht sämtliche Prozessschritte der Anwender in einer einzelnen Applikation durchgeführt oder angezeigt werden können.

[Hinweis auf Bildergalerie: EU-Datenschutzreform 2016: Die wichtigsten Änderungen] gal3

27 http://www.computerwoche.de/a/sie-werden-gehackt-jetzt-gerade-tun-sie-etwas,3324414
28 http://www.computerwoche.de/a/prognosen-fuer-2017,3329201
29 https://de.wikipedia.org/wiki/Grundrecht_auf_Gew%C3%A4hrleistung_der_Vertraulichkeit_und_Integrit%C3%A4t_informationstechnischer_Systeme
30 http://www.computerwoche.de/a/it-sicherheit-im-arbeitsalltag,3330346
31 http://www.computerwoche.de/a/so-werden-industrielle-kontrollsysteme-sicher,3323105
32 http://www.computerwoche.de/a/der-neue-eu-datenschutz-ab-2018-alles-wichtige,3226704

Durch aktive Schulungsmaßnahmen [33] für die Mitarbeiter werden mögliche Fehlerquellen minimiert. Gleichzeitig erlaubt dieses Vorgehen eine Protokollierung der Mitarbeiter-Aktivitäten in der Produktionsumgebung. Beim Monitoring sollte weiterhin immer auf die Erfassung von Metadaten geachtet werden, so dass eine schnelle Auswertung und Datensparsamkeit gemäß BDSG gewährleistet werden kann. Die Kombination von Schulungs- und Monitoring-Applikationen ist somit ausdrücklich zu empfehlen. (fm)

[Hinweis auf Bildergalerie: Das Einmaleins der IT-Security] gal4

Bildergalerien im Artikel:

gal1 Top 10: Diese Mitarbeiter gefährden Ihre IT-Sicherheit

10. Die Charity-Organisation
Foto: Rawpixel.com - shutterstock.com

9. Der Cloud-Manager
Foto: Peshkova - shutterstock.com

8. Der befristet Beschäftigte
Foto: Dean Drobot - shutterstock.com

7. Der externe Partner
Foto: Ditty_about_summer - shutterstock.com

[33] http://www.computerwoche.de/a/wie-it-sicherheit-den-mitarbeitern-spass-macht,3323508

6. Der Social Media Manager
Foto: Aysezgicmeli - shutterstock.com

5. Der neue IT-Entscheider
Foto: Eugenio Marongiu - shutterstock.com

4. Der Ex-Mitarbeiter
Foto: Michal Kowalski - shutterstock.com

3. Der Security-Berater
Foto: Pressmaster - shutterstock.com

2. Die Assistenz der Geschäftsleitung

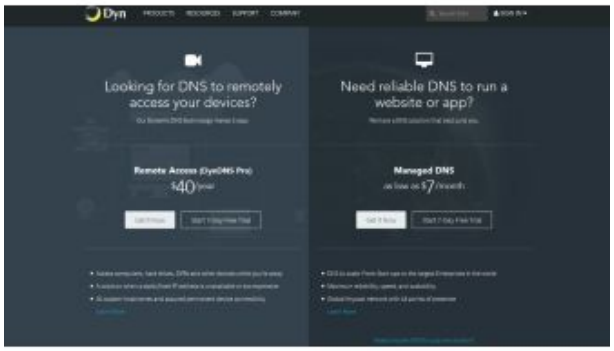
1. Der CEO
Foto: Syda Productions - shutterstock.com

Foto: Cressida studio - shutterstock.com

gal2Die größten Cyberangriffe auf Unternehmen

Die Top 15 Hacker-Angriffe auf Unternehmen
Unternehmen weltweit rücken seit Jahren in den Fokus von Hackern und Cyberkriminellen. Identitäts- und Datendiebstahl stehen bei den Anhängern der Computerkriminalität besonders hoch im Kurs - kein Wunder, dass Cyber-Risk-Versicherungen immer mehr in Mode kommen. Wir zeigen Ihnen 15 der größten Hacking-Attacken auf Unternehmen der letzten Jahre.
Foto: McIek - shutterstock.com

Yahoo
Erst im September musste Yahoo den größten Hack aller Zeiten eingestehen. Nun verdichten sich die Anzeichen, dass dieselben Hacker sich bereits ein Jahr zuvor deutlich übertroffen hatten: Bei einem Cyberangriff im August 2013 wurden demnach die Konten von knapp einer Milliarde Yahoo-Usern kompromittiert. Dabei wurden Namen, E-Mail-Adressen, Telefonnummern, Geburtsdaten und verschlüsselte Passwörter abgegriffen.
Mehr zur Attacke auf Yahoo (http://www.computerworld.com/article/3150901/security/yahoo-breach-means-hackers-had-3-years-to-abuse-user-accounts.html)
Foto: Kvitka Fabian - shutterstock.com



Dyn
Eine massive DDoS-Attacke auf den DNS-Provider Dyn sorgt im Oktober für Wirbel: Mit Hilfe eines Botnetzes – bestehend aus tausenden unzureichend gesicherten IoT-Devices – gelingt es Cyberkriminellen, gleich drei Data Center von Dyn lahmzule-

Cicis
Auch die US-Pizzakette Cicis musste Mitte 2016 einen Hackerangriff eingestehen. Wie das Unternehmen mitteilte, wurden die Kassensysteme von 130 Filialen kompromittiert. Der Diebstahl von Kreditkartendaten ist sehr wahrscheinlich. Wie im Fall von Wendy's und Target gelang es Hackern auch bei Cicis Malware in das Point-of-Sale-Kassensystem einzuschleusen. Erste Angriffe traten bereits im Jahr 2015 auf, im März 2016 verstärkten sich die Einzelattacken zu einer groß angelegten Offensive.

gen. Amazon, GitHub, Twitter, die New York Times und einige weitere, große Websites sind über Stunden nicht erreichbar.
Mehr zum Hackerangriff auf Dyn (http://www.computerwoche.de/a/internet-of-things-regulation-als-rettungsanker,3326410,2)

Nach eigenen Angaben hat Cicis die Malware inzwischen beseitigt.
Mehr zum Cyberangriff auf Cicis (http://www.trendmicro.com/vinfo/us/security/news/cybercrime-and-digital-threats/cicis-pizza-hit-by-credit-card-breach)
Foto: Michael Kan / IDG News Service

Wendy's
Anfang Juli 2016 wurde ein Hacker-Angriff auf die US-Fastfood-Kette Wendy's bekannt. Auf den Kassensystemen wurde Malware gefunden – zunächst war von weniger als 300 betroffenen Filialen die Rede. Wie sich dann herausstellte, waren die Malware-Attacken schon seit Herbst 2015 im Gange. Zudem ließ die Burger-Kette verlauten, dass wohl doch bis zu 1000 Filialen betroffen seien. Die Kreditkarten-Daten der Kunden wurden bei den Malware-Angriffen offenbar ebenfalls gestohlen. Wie im Fall von The Home Depot hatten sich die Hacker per Remote Access Zugang zum Kassensystem der Fast-Food-Kette verschafft.
Mehr zum Cyberangriff auf Wendy's (http://www.computerworld.com/article/3093003/security/wendys-hack-was-bigger-than-thought-and-exposed-credit-card-data.html)
Foto: Wendy's

Heartland Payment Systems
Noch heute gilt der 2008 erfolgte Cyberangriff auf das US-Unternehmen Heartland Payment Systems als einer der größten Hacks aller Zeiten wenn es um Kreditkartenbetrug geht. Heartland ist einer der weltweit größten Anbieter für elektronische Zahlungsabwicklung. Im Zuge des Hacks wurden rund 130.000.000 Kreditkarten-Informationen gestohlen. Der Schaden für Heartland belief sich auf mehr als 110 Millionen Dollar, die zum größten Teil für außergerichtliche Vergleiche mit Kreditkartenunternehmen aufgewendet werden mussten. Verantwortlich für den Hack war eine Gruppe von Cyberkriminellen. Deren Kopf, ein gewisser Albert Gonzalez, wurde im März 2010 wegen seiner maßgeblichen Rolle im Heartland-Hack zu einer Haftstrafe von 20 Jahren verurteilt. Heartland bietet seinen Kunden seit 2014 ein besonderes Security-Paket - inklusive "breach warranty".
Mehr zum Angriff auf Heartland (http://www.bloomberg.com/bw/stories/2009-07-06/lessons-from-the-data-breach-at-heartland-businessweek-business-news-stock-market-and-financial-advice)

Sony Playstation Network
Im April 2011 ging bei vielen Playstation-Besitzern rund um den Globus nichts mehr. Der Grund: ein Cyberangriff auf das digitale Serviceportal Playstation Network (PSN). Neben einer Ausfallzeit des PSN von knapp vier Wochen (!) wurden bei der Cyberattacke jedoch auch die Daten (Kreditkarteninformationen und persönliche Daten) von rund 77 Millionen PSN-Abonennten gestohlen. Sony informierte seine Nutzer erst rund sechs Tage über den Hack - und musste sich dafür harsche Kritik gefallen lassen. Die Kosten des PSN-Hacks beliefen sich auf circa 170 Millionen Dollar. Die Verantwortlichen wurden bislang nicht identifiziert.
Mehr zum PSN-Hack (https://en.wikipedia.org/wiki/2011_PlayStation_Network_outage)
Foto: gielmichal - shutterstock.com

Livingsocial.com
Die Online-Plattform Livinggsocial.com (inhaltlich vergleichbar mit Groupon) wurde im April 2013 Opfer eines Hacker-Angriffs. Dabei wurden die Passwörter, E-Mail-Adressen und persönlichen Informationen von circa 50 Millionen Nutzern der E-Commerce-Website gestohlen. Glücklicherweise waren die Finanzdaten von Kunden und Partnern in einer separaten Datenbank gespeichert. Die Verursacher des Security-Vorfalls wurden nicht identifiziert.
Mehr zur Cyberattacke auf Liviongsocial.com (http://bits.blogs.nytimes.com/2013/04/26/living-social-hack-exposes-data-for-50-million-customers/?_r=0)

Adobe Systems
Mitte September 2013 wurde Adobe das Ziel von Hackern. Circa 38 Millionen Datensätze von Adobe-Kunden wurden im Zuge des Cyberangriffs gestohlen - darunter die Kreditkarteninformationen von knapp drei Millionen registrierter Kunden. Die Hacker die hinter dem Angriff standen, wurden nicht gefasst.
Mehr zum Cyberangriff auf Adobe (http://www.computerwoche.de/a/hacker-erbeuteten-daten-von-38-millionen-adobe-kunden,2548967)
Foto: Ken Wolter - shutterstock.com

Target Corporation
Die Target Corporation gehört zu den größten Einzelhandels-Unternehmen der USA. Ende des Jahres 2013 musste Target einen Cyberangriff eingestehen, bei dem rund 70 Millionen Datensätze mit persönlichen Informationen der Kundschaft gestohlen wurden. Weitaus schwerer wog jedoch, dass unter diesen auch 40 Millionen Datensätze waren, die Kreditkarteninformationen und sogar die zugehörigen PIN-Codes enthielten. Für außergerichtliche Einigungen mit betroffenen Kunden musste Target rund zehn Millionen Dollar investieren, der damalige CEO Gregg Steinhafel musste ein halbes Jahr nach dem Hack seinen Hut nehmen.
Mehr zum Target-Hack (http://techcrunch.com/2014/01/10/targets-data-breach-gets-worse-70-million-customers-had-info-sto-

len-including-names-emails-and-phones/?utm_source=feed-burner&utm_medium=feed&utm_campaign=Feed%3A+Tech-crunch+%28TechCrunch%29&utm_content=Netvibes)
Foto: Ken Wolter - shutterstock.com

Snapchat
Ein kleiner Fehler führte Ende Dezember 2013 dazu, dass Hacker die Telefonnummern und Nutzernamen von 4,6 Millionen Snapchat-Usern veröffentlicht haben. Snapchat selbst geriet darauf ins Kritikfeuer von Nutzern und Sicherheitsforschern, denn wie so oft war die Ursache für die Veröffentlichung der Daten ein Mangel an Sicherheitsvorkehrungen. Die von Hackern verursachten Probleme sind jedoch meist weniger schlimm als der Schaden, der nach der Veröffentlichung folgt. Auch wenn man seinen Nutzernamen oder seine Telefonnummer nicht als großes Geheimnis ansieht – ein motivierter Angreifer wie ein Stalker oder ein Identitäts-Dieb könnten mit diesen Daten Übles anrichten. Dieser Hack zeigt wiederum, dass alle Daten wichtig sind - vor allem wenn sie den Nutzern gehören. Man kann mit Sicherheit davon ausgehen, dass die Entwickler von Snapchat diesen Sicherheitsfehler gerne vor den Hackern gefunden hätten.
Mehr zum Snapchat-Hack (http://techcrunch.com/2013/12/31/hackers-claim-to-publish-list-of-4-6m-snapchat-usernames-and-numbers/)
Foto: focal point - shutterstock.com

Ebay Inc.
Im Mai 2014 wurde Ebay das Ziel von Cyberkriminellen. Zwar wurden bei der Attacke keine Zahlungsinformationen entwendet - dafür aber E-Mail-Adressen, Usernamen und Passwörter von knapp 145 Millionen registrierten Kunden. Die Hacker erlangten scheinbar über von Ebay-Mitarbeitern gestohlene Logins Zugriff auf die Datenbanken des Unternehmens. Die Verantwortlichen wurden nicht identifiziert.
Mehr zum Ebay-Hack (http://www.computerwoche.de/a/alle-ebay-nutzer-sollen-ihr-passwort-aendern%2C3061999)
Foto: 360b - shutterstock.com

J.P. Morgan Chase
Mit J.P. Morgan rückte im Juli 2014 eine der größten US-Banken ins Visier von Cyberkriminellen. Rund 83 Millionen Datensätze mit Namen, Adressen und Telefonnummern von Kunden fielen den Hackern in die Hände. Zugang erlangten die Kriminellen offensichtlich über gestohlene Login-Daten eines Mitarbeiters. Allerdings musste sich J.P. Morgan den Vorwurf gefallen lassen, seine Systeme nicht ausreichend zu schützen. Inzwischen wurden in den USA und Israel vier Personen festgenommen, die mutmaßlich an diesem Hack beteiligt waren.
Mehr zum Cyberangriff auf J.P. Morgan Chase (http://dealbook.nytimes.com/2014/12/22/entry-point-of-jpmorgan-data-breach-is-identified/)
Foto: - shutterstock.com

The Home Depot
Die US-Baumarktkette The Home Depot wurde im September 2014 Opfer eines besonders hinterhältigen Hacks. Cyberkriminelle hatten es geschafft, Malware in das Kassensystem von über 2000 Filialen einzuschleusen. Die Folge davon: 56 Millionen Kreditkarteninformationen von Bürgern der USA und Kanada wurden direkt bei der Zahlung in den Home-Depot-Geschäften entwendet. Darüber hinaus fielen auch noch 53 Millionen E-Mail-Adressen in die Hände der Hacker. Der Schaden für das US-Unternehmen wird auf rund 62 Millionen Dollar beziffert.
Mehr zum Cyberangriff auf The Home Depot (http://www.computerwoche.de/a/riesiger-hackerangriff-bei-home-depot,3068221)
Foto: Niloo - shutterstock.com

Anthem Inc.
Anthem gehört zu den größten Krankenversicherern der USA. Im Februar 2015 gelang es Cyberkriminellen, persönliche Daten von circa 80 Millionen Kunden zu stehlen. Die Datensätze enthielten Sozialversicherungsnummern, E-Mail-Adressen und Anschriften. Darüber hinaus wurden auch Gehaltsinformationen von Kunden und Angestellten entwendet. Immerhin: Medizinische Daten sollen nicht betroffen gewesen sein. Verschiedenen Security-Experten zufolge führt die Spur des Hacks nach China.
Mehr zum Cyberangriff auf Anthem (http://www.nytimes.com/2015/02/06/business/experts-suspect-lax-security-left-anthem-vulnerable-to-hackers.html)

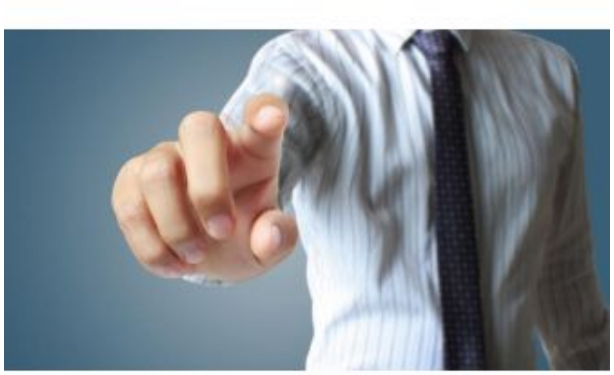
Ashleymadison.com
Anschriften, Kreditkartennummern und sexuelle Vorlieben von circa 40 Millionen Usern hat eine Hackergruppe namens Impact Team im August 2015 nach einem Cyberangriff auf das Seitensprung-Portal Ashley Madison öffentlich gemacht. Der Angriff bewies, dass Ashley Madison nicht – wie eigentlich versprochen – persönliche Informationen der Nutzer gegen eine Gebühr löschte. Das erbeutete 30-Gigabyte-Paket beinhaltete insgesamt 32 Millionen Datensätze, darunter 15.000 Regierungs- und Militäradressen von Nutzern. Auch Teile des Seitenquellcodes und interne E-Mails der Betreiber lagen dadurch offen. Aufgrund der intimen Nutzerdaten und der geheimnisvollen Natur von Ashley Madison ist dieser Hackerangriff besonders heikel. Dass die Betreiber persönliche Daten auch auf Wunsch nicht vernichtet haben, zeigt ein Problem von Unternehmen, die per-

sonenbezogene Daten auf verschiedenen Systemen verarbeiten. Aber auch solche Unternehmen müssen Nutzerinformationen gegen Gefahren schützen – ganz gleich, ob die Gefahr von externen Hackern, böswilligen Insidern oder zufälligen Datenverlusten ausgeht. Ein Ashleymadison-User hat inzwischen vor einem Gericht in Los Angeles Klage gegen Avid Life Media eingereicht. Der Vorwurf: fahrlässiger Umgang mit hochsensiblen Daten. Ein Antrag auf Sammelklage ist ebenfalls bereits eingegangen. Sollte das Gericht diesem folgen, könnten ALM Schadenersatzforderungen in Milliardenhöhe ins Haus stehen.
Mehr zur Cyberattacke auf Ashleymadison.com (http://meedia.de/2015/08/25/selbstmorde-erpressung-betrug-schadensersatz-chaos-und-verbrechen-nach-dem-ashley-madison-hack/)

gal3EU-Datenschutzreform 2016: Die wichtigsten Änderungen

Ein Gesetz für alle
EU-weit gelten die gleichen Datenschutzregeln. Das bedeutet auch eine gestiegene Verantwortung und Haftung für alle, die persönliche Daten verarbeiten.
Foto: Yvonne Bogdanski - Fotolia.com

"Recht auf Vergessen"
Wollen Nutzer ihre Daten nicht weiter verarbeitet sehen, werden diese gelöscht - vorausgesetzt, es spricht aus juristischer Sicht nichts dagegen.
Foto: Anson/Fotolia.com



"Opt-in" statt "Opt-out"
Sollen persönliche Daten verabeitet werden, müssen Nutzer aktiv zustimmen (und nicht aktiv widersprechen wie bisher).
Foto: violetkaipa - Fotolia.com

Recht auf Transparenz
Nutzer haben ein Recht auf Transparenz - sie dürfen erfahren, welche Daten über sie gesammelt und wie diese verarbeitet werden.
Foto: Kritchanut - www.shutterstock.com

Zugang und Portabilität
Der Zugang zu den bei Dritten über einen selbst gespeicherten Daten soll einfacher möglich sein. Zudem ist die Dartenportabilität zu gewährleisten - also sicherzustellen, dass persönliche Informationen leichter von einem Dienstanbieter zu einem anderen übertragen werden können.
Foto: Doc Rabe Media, Fotolia.com

Schnellere Meldung
Tritt ein Datenverlust auf, müssen Unternehmen und Organisationen im Regelfall binnen 24 Stunden, mindestens aber so schnell wie möglich ihrer behördlichen Meldepflicht nachkommen.
Foto: kantver/Fotolia

Weniger Behördenchaos
Unternehmen müssen sich nur noch mit einer einzigen Aufsichtsbehörde auseinandersetzen - und zwar dort, wo sie ihren Hauptsitz haben.
Foto: Firma V - Fotolia.com

Grenzübergreifend
Privatanwender dürfen jeden Fall von Datenmissbrauch an ihre nationale Aufsichtsbehörde melden - selbst dann, wenn die betroffenen Daten im Ausland verarbeitet wurden.
Foto: R. Schramm - Fotolia.com

Erweiterter Geltungsbereich
Die EU-Richtlinie gilt auch für Unternehmen, die keinen Sitz in der EU haben, sobald sie Waren oder Dienstleistungen in der EU anbieten oder auch nur Online-Marktforschung unter EU-Bürgern betreiben.
Foto: WavebreakMediaMicro - Fotolia.com

Höhere Bußgelder
Verstößt ein Unternehmen gegen die Datenschutzbestimmungen, droht ein Bußgeld in Höhe von bis zu vier Prozent des Jahresumsatzes.
Foto: rangizzz - Fotolia.com

Bürokratieabbau
Administrative Umstände wie Meldepflichten für Unternehmen, die persönliche Daten verarbeiten, entfallen.
Foto: Jochen Binikowski - Fotolia.com

Erst ab 16
Die rechtswirksame Anmeldung bei Internetnetservices wie Facebook oder Instagr.am soll Jugendlichen im Regelfall erst ab 16 Jahren möglich sein - weil sie erst ab diesem Lebensalter eine gültige Einwilligung in die Verarbeitung ihrer persönlichen Daten geben können. Nationale Gesetze sollen laut Datenschutzverordnung hier aber Ausnahmen möglich machen.
Foto: Sergey Novikov - shutterstock.com

Stärkung der nationalen Aufsichtsbehörden
Nationale Datenschutzbehörden werden in ihren Kompetenzen gestärkt, so dass sie die neuen EU-Regeln besser umsetzen können. Unter anderem dürfen sie einzelnen Unternehmen verbieten, Daten zu verarbeiten. können bestimmte Datenflüsse stoppen und Bußgelder gegen Unternehmen verhängen, die bis zu zwei Prozent der jeweiligen weltweiten Jahreseinkünfte betragen. Darüber hinaus dürfen sie Gerichtsverfahren in Datenschutzfragen anstrengen.

(Quelle: Forrester Research)
Foto: Martin Fally - Fotolia.com

gal4Das Einmaleins der IT-Security

Sichere Passwörter
IT-Sicherheit beginnt mit Sensibilisierung und Schulung der Mitarbeiter sowie mit einer klaren Kommunikation der internen Verhaltensregeln zur Informationssicherheit:

 Komplexe Passwörter aus Groß- und Kleinbuchstaben, Ziffern und Sonderzeichen, mindestens achtstellig.
Foto: wk1003mike - shutterstock.com

Passwortdiebstahl
Niemals vertrauliche Daten weitergeben oder/und notieren.
Foto: Brian A Jackson - shutterstock.com

E-Mail-Sicherheit
E-Mails signieren, sensible Daten verschlüsseln, Vorsicht beim Öffnen von E-Mail-Anlagen und Links.
Foto: ra2studio - shutterstock.com

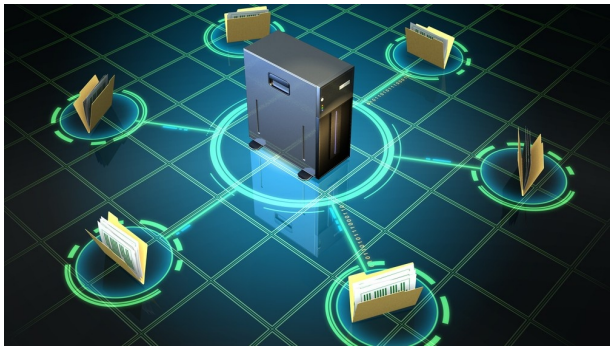
Soziale Manipulation
Bewusst mit vertraulichen Informationen umgehen, nur an berechtigte Personen weitergeben, sich nicht manipulieren oder aushorchen lassen.
Foto: lolloj - shutterstock.com

Vorsicht beim Surfen im Internet
Nicht jeder Link führt zum gewünschten Ergebnis.
Foto: karen roach - shutterstock.com

Nur aktuelle Software einsetzen
Eine nicht aktualisierte Software lässt mehr Sicherheitslücken offen.
Foto: Rawpixel.com - shutterstock.com

Verwendung eigener Software
Unternehmensvorgaben beachten und niemals Software fragwürdiger Herkunft installieren.
Foto: Pressmaster - shutterstock.com

Unternehmensvorgaben
Nur erlaubte Daten, Software (Apps) und Anwendungen einsetzen.
Foto: jesadaphorn - shutterstock.com



Backups
Betriebliche Daten regelmäßig auf einem Netzlaufwerk speichern und Daten auf externen Datenträgern sichern.
Foto: Andrea Danti - shutterstock.com

Diebstahlschutz
Mobile Geräte und Datenträger vor Verlust schützen.
Foto: Studio10Artur - shutterstock.com

Gerätezugriff
Keine Weitergabe von Geräten an Dritte, mobile Geräte nicht unbeaufsichtigt lassen und Arbeitsplatz-PCs beim Verlassen sperren.
Foto: turlakova - shutterstock.com

Sicherheitsrichtlinien
Die organisatorischen Strukturen im Hintergrund bilden den erforderlichen Rahmen der IT-Sicherheit. Hier gilt es, klare Regelungen zu formulieren und einzuhalten:

Definition und Kommunikation von Sicherheitsrichtlinien
Foto: Vasin Lee - shutterstock.com

Zugriffsrechte
Regelung der Zugriffsrechte auf sensible Daten
Foto: nasirkhan - shutterstock.com

Adminrechte
Keine Vergabe von Administratorenrechten an Mitarbeiter
Foto: Potapova - shutterstock.com

Softwareupdates
Automatische und regelmäßige Verteilung von Softwareupdates
Foto: Rawpixel.com - shutterstock.com

Logfiles
Kontrolle der Logfiles
Foto: turgaygundogdu - shutterstock.com

Dokumentation
Vollständige und regelmäßige Dokumentation der IT
Foto: Freer - shutterstock.com

Datensicherung
Auslagerung der Datensicherung
Foto: www.BillionPhotos.com - shutterstock.com

Sicherheitsanalyse
Regelmäßige Überprüfung der Sicherheitsmaßnahmen durch interne und externe Sicherheitsanalysen
Foto: Kopytin Georgy - shutterstock.com

Notfallplan
Erstellung eines Notfallplans für die Reaktion auf Systemausfälle und Angriffe
Foto: Maria Maarbes - shutterstock.com

WLAN-Nutzung
Auf technischer Ebene muss ein Mindeststandard gewährleistet sein. Dieser lässt sich größtenteils ohne großen Kostenaufwand realisieren:

Dokumentation der WLAN-Nutzung, auch durch Gäste
Foto: Thomas Reichhart - shutterstock.com

Firewalls
Absicherung der Internetverbindung durch Firewalls
Foto: Goritza - shutterstock.com

Biometrische Faktoren
Einsatz von Zugangsschutz/Kennwörter/Biometrie
Foto: Patrick Foto - shutterstock.com

Zugangskontrolle
Physische Sicherung/Zugangskontrolle und -dokumentation
Foto: Dmitry Kalinovsky - shutterstock.com

Schutz vor Malware
Schutz vor Schadsoftware sowohl am Endgerät als auch am Internetgateway, idealerweise durch zwei verschiedene Antivirenprogramme
Foto: Blue Island - shutterstock.com

Webzugriffe
Definition einer strukturierten Regelung der Webzugriffe
Foto: Anteromite - shutterstock.com

Verschlüsselung
Verschlüsselung zum Schutz von Dateien und Nachrichten mit sensiblen Inhalten
Foto: Piotr Zajda - shutterstock.com

Löschen
Sicheres Löschen der Daten bei Außerbetriebnahme
Foto: Lightspring - shutterstock.com

Update der Sicherheitssysteme
Sicherstellung regelmäßiger Updates der Sicherheitssysteme
Foto: voyager624 - shutterstock.com

Monitoring
Permanente Überwachung des Netzwerkverkehrs auf Auffälligkeiten
zusammengetragen von Giegerich & Partner (https://www.giepa.de/)
Foto: Andrey Popov - shutterstock.com

31.03.2017

IDG Business Media GmbH