Liebe Leser,

das Zeitalter der Digitalisierung hat neue Möglichkeiten des Austauschs und der Vernetzung mit sich gebracht. Gleichzeitig sind durch die erweiterte Vernetzung und den Austausch von Daten aber auch neue Risiken aufgetaucht. Neben der Nutzung des Internets tauschen Privatnutzer heute auch über Smartphones sensible Daten aus. Unternehmen vernetzen sich über das Internet und mancher Betrieb sorgt mit Cloud-Computing für flexiblere Arbeitsmöglichkeiten. Für Kriminelle und Betrüger haben sich damit weitere Türen für aufgetan. Viele Verbraucher und Unternehmer wissen nicht genau, welche Gefährdungen sich durch Internet Kriminalität ergeben können.

Mit der Lektüre des vorliegenden Buches erhalten Sie einen Überblick über Gefahren des Internets, der bewusst in einfacher und Sprache geschrieben wurde. Es kann für einen ersten Einstieg in das Thema wie auch zur gezielten inhaltlichen Vertiefung genutzt werden. Auch Nutzer ohne Vorkenntnisse wird damit ein Einblick in eines der bedeutenden Themen unserer Zeit gegeben. Tatsächlich braucht heute niemand ein eigenes Informatikstudium, um sich sicherer im Internet zu bewegen.

Viele Gefahren lassen sich mit einfachen Tipps bereits umgehen. Jeder Abschnitt des Buches beinhaltet zum einen Tipps dieser Art, die von jedermann genutzt werden können. Zum anderen gibt das Buch gerade Unternehmern eine gezielte Hilfe an die Hand. Es hat auch die Firmenkultur im Blick.

Wer seine Mitarbeiter für das Thema sensibilisiert und schult, schützt sich auch damit erfolgreich gegen verschiedene Formen der Internetkriminalität. Am Ende des Textes gibt es Literaturhinweise auf Fachliteratur, die zur Erstellung des Buches beigetragen hat.

Ich wünsche Ihnen viel Erfolg mit diesem Wissen auf Ihren Wegen,

Sanjay Sauldie

CEO iroi Global OÜ

Ausbildungen und Zertifikate:

- Master of Sciences in Marketing (University of Salford, Manchester, UK)
- MIT Design Thinking (EMERITUS, in collaboration with MIT Sloan, USA)
- Mathematik & Informatik (Universität Köln, Deutschland)
- Surviving Disruptive Technologies (University of Maryland, USA)
- Organizational Leadership (Northwestern University, Illinois, USA)
- Digital Business Strategy (MIT Sloan School of Management, Massachusetts, USA)

Inhaltsangabe:

Das Phänomen der Internetkriminalität im digitalen Zeitalter

Als das deutsche Bundesamt für Sicherheit in der Informationstechnik (BSI) Anfang Mai 2019 die Ergebnisse seiner jährlichen Umfrage zum Thema Cybersicherheit vorstellte, sprachen die Zahlen eine deutliche Sprache. Gut ein Drittel aller vom Bundesamt befragten Unternehmen gab an, dass es im Jahr 2018 von Sicherheitsvorfällen im Cyberbereich betroffen war. Etwa 50% dieser Vorfälle konnten nicht einfach abgewehrt werden. Ein nicht unerheblicher Anteil der Täter kam demnach ungeschoren und mit Erfolg davon.

Aus den Ergebnissen der aufschlussreichen Umfrage, die auf der Homepage des BSI eingesehen werden können, gehen noch weitere Erkenntnisse hervor. Offenbar sind größere Unternehmen noch stärker von Cyberkriminalität betroffen. Während von mittelständischen Betrieben 26% betroffen waren, gaben 43% der großen Unternehmen an, dass sie 2018 entsprechende Vorfälle zu verzeichnen hatten. Die häufigste Angriffsart der Kriminellen war dabei übrigens die sogenannte Malware. Dabei handelt es sich um fremde Programme, die sich unerlaubt Zugang zum eigenen Computersystem verschaffen und anschließend sensible Daten abrufen oder Schäden herbeiführen. 90% dieser Malware wurde als Link in einer E-Mail oder als Anhang einer E-Mail verschickt und so an den Mann oder die Frau gebracht. In den meisten dieser Fälle blieb es offenbar nicht "nur" beim Ausspionieren von Informationen und sensiblen Daten. 87% der betroffenen Unternehmen meldeten Betriebsausfälle oder Störungen des laufenden Betriebs aufgrund der Vorfälle in 2018.

Für die Wiederherstellung von Datensicherheit oder die Reparatur von Betriebssystemen fielen mitunter erhebliche Kosten an. Wenn Unternehmen erst dann reagieren, wenn es bereits zu spät ist, können hohe Kosten auf sie zukommen.

Doch nicht nur Unternehmen, auch Privatpersonen können heute Opfer von Internetkriminalität werden. Die Bandbreite ist in diesem Fall relativ groß. Vom Ausspähen geheimer Passwörter über Abofallen bis hin zum Stehlen digitaler Identitäten können Kriminelle viel Unheil anrichten. Sie können Menschen psychisch terrorisieren, erpressen oder ausrauben. Um dies zu tun, müssen die Täter nicht einmal selbst vor Ort sein. Sie können Straftaten von einem völlig anderen Ort begehen. Nicht wenige Täter agieren von anderen Ländern aus und werden nicht gefasst.

Gegenüber einem direkten Raub ist die Internetkriminalität damit unnahbarer und kann deshalb noch gefährlicher sein. Oft sitzen die Täter und auch die Anbieter von Internetdienstleistungen in anderen Ländern, in denen eine andere Gesetzeslage gilt. Das macht es für Betroffene nicht unbedingt leichter. Nur wer

sich richtig schützt, kann kriminelle Eingriffe verhindern. Doch vielen Verbrauchern und Unternehmen fehlen die dafür nötigen Kenntnissen. Dies mag auch ein Grund dafür sein, dass die Internetkriminalität in den letzten Jahren massiv zugenommen hat.

Mitte 2019 veröffentlichte das Bundesministerium für Inneres Österreich eine Statistik über die angezeigten Fälle von Cybercrime, die in den Jahren 2004 bis 2018 in Österreich gemeldet wurden. Die entsprechenden Zahlen weisen einen Anstieg von 753 Fällen in 2004 auf 19627 Fälle in 2018 auf. Einen derart massiven Anstieg von Kriminalität dürfte kaum ein anderer Bereich aufweisen. Verbraucher und Unternehmen sollten angesichts derartiger Statistiken gewarnt sein.

Aber welche Methoden nutzen Kriminelle bei ihrem Vorgehen und worauf sollten Verbraucher und Unternehmen achten? Tatsächlich ergeben sich nicht alle Vorfälle aus völlig neuen Techniken. Viele der Sicherheitsvorfälle resultieren aus altbekannten Sicherheitslücken. Sie müssen nicht immer mit einer schlechten technischen Ausstattung zusammenhängen. Oft hängen sie auch ganz einfach mit dem Verhalten der Nutzer zusammen.

Auch ein gut ausgebautes Sicherheitssystem ist letztlich nur so sicher, wie seine Nutzer es verwenden. Wer sich für Internetkriminalität schützen möchte, sollte deshalb zunächst ein Bewusstsein für mögliche Gefahren schaffen. Die folgenden Abschnitte helfen genau dabei. Sie bieten einen Überblick über unterschiedlichste Gefahren, die sich im digitalen Zeitalter ergeben können. Die Palette der Informationen ist dabei bewusst breit angelegt. Auch klassische und sehr einfache Tipps werden erläutert.

In manchen Fällen mag ihre ausführliche Darstellung dem Leser weitere Hinweise an die Hand geben, die über seinen bisherigen Kenntnisstand hinausgehen. Den Leserinnen und Lesern soll mit dem vorliegenden Text ein möglichst umfangreicher Überblick über das Fachgebiet gegeben werden. Wer über einfachere Tipps bereits im Bilde ist, kann die jeweiligen Abschnitte gegebenenfalls überspringen und sich dem jeweils nächste widmen.

Exkurs: Welche Akteure sind im Bereich der Internetkriminalität relevant?

Im Vergleich mit einem direkten Überfall fällt die Internetkriminalität auf Seiten der Täter wesentlich bequemer aus. Anders als bei dies beispielsweise bei einem Raubüberfall der Fall ist, müssen sie in diesem Fall ja nicht direkt vor Ort sein. Es ist daher nicht verwunderlich, dass mancher Kleinkriminelle heute gerade das Internet als Tatort für sich entdeckt. Doch es gibt noch einen anderen Faktor, der zum Anstieg der Vorfälle beitragen mag. Tatsächlich gibt es neben kleinen

Kriminellen und großen Betrügern nämlich noch diverse andere Akteure, die sich als Risiko der Cyber Security hervortun. In seinem Buch "Cyber Security" listet Sebastian Klipper (2015) die folgenden Gruppen auf: Während Kriminelle (1) vor allem auf schnellem Weg zu Geld kommen wollen, bedrohen auch Geheimdienste (2) die Cyber Security. Sie haben nicht selten nahezu ungeahnte technische Möglichkeiten und ein starkes Interesse daran, unbemerkt an Informationen zu gelangen. Zudem gibt es Hacker (3), die Klipper zufolge heute statt der Schließung von Sicherheitslücken immer mehr kommerzielle Interessen verfolgen. Damit werden Teile dieser Gruppen zu möglichen Ansprechpartnern sowohl für Kriminelle wie auch für Geheimdienste. Daneben führt der Autor auch unzufriedene Mitarbeiter (4) als Risikofaktor an. Sie können sich Zugang zu sensiblen Informationen verschaffen und damit Schaden anrichten oder Kapital aus diesen Daten schlagen. Auch Whistleblower (5) können für Organisationen zum Risikofaktor werden. Schließlich verschafft sich auch mancher reguläre Marktteilnehmer (6) - wenn entsprechende Lücken dies zulassen - auf digitalem Weg gerne Informationen über den Konkurrenten.

Viren im Visier - was man über die schädlichen Programme wissen sollte

Eine gängige Malware sind Computerviren. Dabei handelt es sich um schädliche Programme, die auf verschiedenen Wegen auf den Computer gelangen können. In manchen Fällen erreichen sie diesen über das Internet. In anderen übertragen sich Viren von einem Datenträger wie einem USB-Stick. Sind sie auf den Computer gelangt, so kann dies zu verschiedenen Effekten führen. Manche Viren beschädigen die Software oder können ganze Computer außer Gefecht setzen.

Sogenannte Trojaner dringen in das System ein, rufen sensible Daten ab und senden diese nach Außen an Dritte. Wie ein trojanisches Pferd gelangt das Programm ungesehen auf den Computer und dringt in den internen Bereich ein. Anschließend hat der Angreifer freie Hand. Überdies gibt es Malware, die dem Angreifer erlauben kann, den Computer extern zu steuern. Möglichkeiten wie diese öffnen Tür und Tor für Kriminelle, welche geheime Daten abrufen wollen oder es darauf abgesehen haben, die Nutzer zu erpressen. Hier kann also nicht nur der Computer in Gefahr gebracht werden. Es können noch ganz andere Gefahren lauern. Es ist daher wichtig, dass sich Unternehmen und private Nutzer genau mit den Gefahren von Viren auseinandersetzen.

Das bedeutet nicht, dass man etwas über das technische Funktionieren verschiedene Viren wissen muss. Es bedeutet jedoch, dass man über die Handlungsmöglichkeiten zur Bekämpfung von Viren im Bilde sein muss. Viren dürften die Art von Gefahr sein, von der sich die meisten Nutzer bereits darüber bewusst sind, dass es sie geben kann. Doch in manchen Fällen herrscht ein gefährliches Halbwissen darüber, wie man sich gegen Viren zur Wehr setzen

kann. Ein wichtiges Instrument gegen die schädlichen Programme ist ein Antivirenprogramm. Wer Kriminellen aus dem Internet keine Chance geben will, sollte einige Tipps beherzigen. Erstens sollte das Anti-Viren-Programm bereits installiert werden, bevor sich das Gerät das erste mal mit dem Internet verbindet. Ansonsten haben Viren hier die Möglichkeit, auf den Rechner zu gelangen. Zweitens sollte im Idealfall bei der Nutzung des Internets auch eine professionelle Firewall aufgebaut werden. Gerade für Unternehmen lohnt sich dieser Schritt. Bei dieser handelt es sich um eine virtuelles Schutzschild. Es soll dafür sorgen, dass potentielle Angreifer außen vor bleiben.

Ein dritter Tipp ist die regelmäßige Aktualisierung des Anti-Viren-Programms. Da sich auch die Viren stets weiter entwickeln, muss die Software mit deren Entwicklung Schritt halten. Nur wer sie regelmäßig aktualisiert, gewährleistet die Sicherheit seiner Systeme. Neben dem Anti-Viren-Programm sollten auch andere Aktualisierungen der Software, die auf den einzelnen Geräten genutzt wird, regelmäßig vollzogen werden. Nur wer Betriebssysteme und Browser immer wieder aktualisiert, sorgt dafür, dass Angreifer keine Lücken finden, die sie nutzen können. Viertens sollten externe Datenträger wie beispielsweise USB-Sticks, CDs oder externe Festplatten vor der Nutzung auf Viren geprüft werden.

Mails und Malware - das größte Einfallstor für Internetkriminalität

Die bereits zitierten Zahlen des Bundesamtes für Sicherheit in der Informationstechnik verweisen auf einen entscheidenden Risikofaktor. Sie machen deutlich, dass der größte Anteil an Sicherheitsvorfällen durch Malware ausgelöst wird, die sich über E-Mails unerlaubt Zugang zum System verschafft hat. Damit kann sie Unheil stiften oder das Einfallstor für weitere kriminelle Aktivitäten öffnen. Von dieser Art von Internetkriminalität sind sowohl private Nutzer wie auch Unternehmen betroffen.

Die sichere Nutzung von E-Mails ist deshalb ganz klar ein Schlüsselfaktor im Kampf gegen Internetkriminalität. Zunächst einmal ist es wichtig zu wissen, dass die Malware nicht bereits dadurch auf den Computer gelangt, weil sich eine entsprechende Mail im Posteingang befindet. Dieser Weg öffnet sich erst dann, wenn die Anhänge dieser Mails geöffnet werden oder unbemerkt auf den PC gelangen.

Auch über das Klicken von Links, die sich in den Mails finden, kann es zu einem Sicherheitsrisiko kommen. Links können auf Seiten führen, die entsprechende Malware bereithält, die sich dann Zugang zum Computer verschafft. In den seltensten Fällen eröffnen Nutzer der Malware in böser Absicht Zugang zum System. Oft passiert dies durch Unwissen. Der Nutzer öffnet einfach naiv den gefährlichen Anhang, ohne zu erwarten, dass der Absender Böses im Schilde

führen könnte. Noch mehr Fälle gibt es, in denen die entsprechende Mail schlichtweg aus Unachtsamkeit geöffnet wurde oder der Anhang versehentlich heruntergeladen wurde. Gerade bei einem vollen Arbeitsalltag können solche Unachtsamkeiten jedem Menschen einmal passieren. Hier gilt ein Grundsatz, der auf unzählige Fälle im Bereich der Internetkriminalität zutrifft: Die größte Sicherheitslücke bildet oftmals nicht die Technik, sondern das Nutzerverhalten des Menschen.

Obwohl es ein Bewusstsein für die Gefahr der Internetkriminalität gibt, ist die Mail bis heute das große Einfallstor in vielen Fällen von Cyber Crime. Eine Ursache liegt im Vorgehen der Täter. Geschickt formulieren sie E-Mails mit Betreffzeilen, welche die Empfänger gezielt dazu verlocken sollen, die E-Mail samt Anhang zu öffnen. Von einem großen Geldgewinn oder einem guten Geschäft kann da die Rede sein.

Manchmal weist der Betreff auch auf wichtige Hinweise zur Sicherheit des eigenen Systems hin. Auch unmoralische Angebote oder erotische Avancen können manche Verbraucher dazu verleiten, eine Mail von einem unbekannten Absender zu prüfen. In anderen Fällen hat sich eine Malware Zugang zum E-Mailkonto eines Bekannten verschafft und verschickt seltsame Nachrichten an diverse Personen, die in dessen Adressbuch aufgelistet sind.

Auf diese Weise kann sich die Malware wie bei einem Schneeballprinzip schnell immer weiter ausbreiten. Auch die Anhänge von Nachrichten, die in sozialen Netzwerken verschickt werden, können entsprechende Malware enthalten. Wer sie öffnet, ist sich im nächsten Moment damit konfrontiert, dass sich die schädlichen Programme direkt auf dem eigenen Computer installieren. Nicht in allen Fällen bekommt der Nutzer etwas davon mit. Bei Untersuchungen von Computern kommt immer wieder heraus, dass PCs, die über eine lange Zeit genutzt wurden, entsprechende Malware beherbergen.

Exkurs: Was machen Kriminelle mit den erschlichenen Informationen?

In vielen Fällen bekommen die Unternehmen oder die Nutzer selbst zunächst gar nichts davon mit. Währenddessen greift die Malware sensible Daten ab und leitet sie an Dritte weiter. Manche der Betrüger erpressen Unternehmen dann damit, dass sie diese Daten haben. Sie drohen mit der Veröffentlichung der Daten. In vielen Fällen erklären die Täter, dass sie die Daten nur löschen, wenn eine bestimmte Summe an Geld auf elektronischem Weg transferiert wird.

Doch es kommt auch immer wieder vor, dass die Kriminellen einen ganz anderen Weg gehen. Sie bieten die Daten, die auf dem System abgerufen wurden, anderen Unternehmen an. Im Internet floriert der Handel mit entsprechenden Daten

geradezu. Diese Art der Wirtschaftskriminalität kann nicht nur dafür sorgen, dass Unternehmen ihre Konkurrenten ausstechen. Wer die richtigen Daten zum richtigen Zeitpunkt erhält, kann sich einen handfesten Vorteil am Markt verschaffen. Auch deshalb interessieren sich viele Akteure auf der ganzen Welt für Daten. Es geht dabei längst nicht nur darum, andere Menschen unmittelbar finanziell zu schädigen und Dinge zu tun, die nur von Kriminellen gemacht werden. Mit den richtigen Informationen verschaffen sich auch "ganz normale" Unternehmen einen Vorteil am Markt. Das Interesse an Daten ist also sehr breit gestreut.

Diese Tipps sollten im Umgang mit E-Mails beachtet werden

Um die erwähnten Risiken zu vermeiden, gibt es einige wichtige Tipps. Die meisten davon erfordern weder eine aufwändige Technik noch umfangreiches Wissen über die Datenverarbeitung. Sie lauten wie folgt: Erstens sollten nur E-Mails geöffnet werden, die von Absendern stammen, die vertrauenswürdig sind. Im besten Fall kennt man den Absender persönlich. Aber auch wenn dies nicht der Fall ist, deuten bestimmte Kriterien auf Seriosität hin. Dazu zählt etwa eine normale E-Mailadresse eines bekannten Anbieters. Je kurioser die E-Mailadresse des Absenders ist, umso weniger sollte man der E-Mail vertrauen.

E-Mails von gänzlich unbekannten Mailanbietern mit auffälligen Zahlenkombinationen deuten auf mögliche Sicherheitsrisiken hin. Falls eine Mail also von einem Absender stammt, der nicht bekannt ist und anhand der Absenderadresse einen solchen unseriösen Eindruck erweckt, sollte sie am besten direkt gelöscht werden.

Wie gesagt sollten entsprechende Mails am besten gar nicht erst geöffnet werden. In manchen Fällen könnten sich hinter Grafiken, die zur Ansicht geladen werden, bereits schädliche Programme verstecken. Zweitens sollten auf keinen Fall Anhänge solcher E-Mails geöffnet werden. Sie bilden das Einfallstor für die Malware. Drittens dürfen Nutzer nicht auf Links klicken, die wenig Vertrauen erwecken. Sie können sich ebenfalls in solchen E-Mails verstecken. Über die Links können Viren auf den Rechner gelangen. Auch in Mails von Bekannten, die über Malware verschickt wurden, können sich solche Links finden. Wer diese aufruft, verschickt in manchen Fällen damit bereits eine entsprechende Mail an Vertraute aus dem eigenen Adressbuch weiter.

In einem Haushalt sollten alle Nutzer auf entsprechende Tipps aufmerksam gemacht werden. Das ist in diesem Fall nicht besonders schwierig. In den meisten Fällen gestaltet sich die Zahl der Menschen, die in einem Haushalt ein Gerät nutzen, überschaubar. Auch Jugendliche kann man über die Risiken gut informieren. In vielen Fällen werden sich diese selbst sogar bereits besser mit dem

Thema Datensicherheit und sicherem Verhalten auskennen, als dies bei älteren Generationen der Fall ist. Zum einen wachsen die Jugendlichen heute mit dem Internet und Smartphones auf. Zum anderen informieren viele Schulen auch über das Thema Sicherheit im Internet.

Aber längst nicht jede Lehrkraft ist mit der notwendigen Expertise in Sachen Datensicherheit und digitaler Kompetenz ausgestattet. Wer sich ausführlich über das Thema informieren möchte, sollte sich deshalb nicht allein auf den Schulunterricht oder offizielle Mitteilungen verlassen. Im besten Fall sollte man sich aktiv selbst mit der Thematik vertraut machen. Durch diese Art des Lernens wird auch ein Wissen erworben, das nachhaltiger wirkt. Das Gedächtnis prägt sich Dinge bei Lernprozessen, die aus eigener Motivation stattfinden, wesentlich besser ein.

Wenn das erlernte Wissen dann auch noch angewendet wird, bleibt es besonders gut in Erinnerung. Wer also beispielsweise nicht nur über sicheres Surfen liest, sondern dieses auch praktiziert, wird seine eigenen digitalen Kompetenzen erfolgreich stärken.

In einem Unternehmen kann sich die Informationsarbeit noch sehr viel komplexer als in der Schule oder im Familienverbund gestalten. Hier werden die Geräte von einer Vielzahl von Mitarbeitern genutzt. Wenn lediglich ein einzelner eine entsprechende Mail anklickt, kann sich die Malware Zugang zum System verschaffen. Bleibt sie länger unbemerkt, so breitet sie sich aus und wird zum ernsthaften Sicherheitsrisiko.

Es ist deshalb wichtig, dass man ein Bewusstsein unter den eigenen Mitarbeitern schafft. Wer entsprechende Schulungen anbietet, sorgt damit für eine verbesserte Sicherheit des Systems. Übrigens nehmen viele Mitarbeiter Angebote dieser Art gerne an. Sie erwerben damit Kenntnisse, die ihnen auch als private Nutzer helfen können. Entsprechende Schulungen können als Arbeitszeit verbucht werden und so organisiert werden, dass sie die Beschäftigten gezielt dort abholen, wo sie stehen. In jedem Fall empfiehlt sich deshalb eine sehr allgemeine Einführung, die vor allem auf praktische Tipps abzielt. In anderen Fällen können auch externe Anbieter für sehr gezielte Schulungen auf einem hohen technischen Niveau engagiert werden. Was im einzelnen Fall sinnvoll ist, hängt jeweils von den konkreten Vorkenntnissen und Bedürfnissen der Gruppe ab.

E-Mailverschlüsselung sorgt für sicheren Datenverkehr

Neben dem Passwort gibt es weitere Lücken im Bereich des Mailverkehrs. Viele Nutzer wissen nicht, dass beim Austausch einer Mail zwischen Absender und Empfänger die Möglichkeit besteht, dass die Daten gleichsam unterwegs

abgefangen werden. Wenn die E-Mail nicht verschlüsselt wurde, können Dritte dann unter Umständen sensible Daten in Erfahrung bringen.

Deshalb sollte man E-Mails grundsätzlich verschlüsseln. Manche Anbieter sehen eine solche Verschlüsselung in den Grundeinstellungen vor. Bei anderen muss diese Technik erst eingestellt werden. Es gibt spezielle Schlüssel, die genutzt werden können, um Mailverkehr zu verschlüsseln.

Für den Empfänger wird das Lesen der Mail damit nicht schwieriger. Niemand muss also Angst haben, dass er seinen Empfängern damit einen großen Aufwand aufzwingt. Prinzipiell ist die Verschlüsselung von E-Mails deshalb sehr sinnvoll. Sie führt dazu, dass technische versierte Dritte nicht automatisch auf dem Weg die E-Mail abfangen und auslesen können. Angesichts der gestiegenen Internetkriminalität müssen Unternehmen und Verbraucher heute damit rechnen, dass Dinge wie diese passieren können. In manchen Fällen mag dies nicht so viel Schaden herbeiführen. Falls aber doch einmal vertrauliche Daten in Mails enthalten sind, kann dies gefährlich werden.

Unternehmen sollten eine solche Gefahr schon deshalb nicht riskieren, weil sie die eigenen Kunden und Wirtschaftspartner treffen kann und damit den eigenen Ruf schädigt. Wer seine E-Mails prinzipiell verschlüsselt, erweckt dagegen einen guten Eindruck bei Empfängern. Falls wiederum sehr vertrauliche Daten verschickt werden, wie beispielsweise PINs oder Passwörter sollte dies über eine gesicherte Verbindung oder noch besser per Postverkehr geschehen. Nach wie vor gewährt der Postverkehr die bestmögliche Sicherheit von verschickten Daten.

Empfehlung: Mailadressen mit dem Identity Leak Checker überprüfen

Der wichtigste Tipp gegen den Datendiebstahl kommt an erster Stelle: Es gibt Möglichkeiten, mit denen Verbraucher und Unternehmen gezielt herausfinden können, ob die eigenen Accounts vom großen Datendiebstahl betroffen sind.

Ein wichtiges Instrument in diesem Zusammenhang ist der Identity Leak Checker des Hasso-Plattner-Instituts. Das an der Universität Potsdam beheimatete Institut bildet ein Exzellenz-Zentrum für IT-Systeme. Mit dem Identity Leak Checker dieses Instituts können Verbraucher und Unternehmen kostenfrei überprüfen, ob die eigenen Accounts vom großen Datenklau betroffen sind. Auf dem entsprechenden Online-Auftritt geben die Nutzer die jeweilige E-Mailadresse ein.

Der Identity Leak Checker greift dann auf eine Datenbank mit fast 6 Milliarden Datensätzen zu. Das Ergebnis erhält man anschließend per E-Mail an die angegebene Adresse. Durch die Überprüfung lässt sich also herausfinden, ob Daten in Bezug auf das eigene Konto erschlichen und veröffentlicht oder verkauft

wurden. Der Aufwand dafür ist minimal. Weder kostet die Dienstleistung des Instituts etwas noch vergeht viel Zeit. Auf entsprechende Anfrage können Nutzer unmittelbar eine Auskunft erhalten. Falls man dabei herausfindet, dass man betroffen ist, sollte man unmittelbar reagieren. Der wichtigste Schritt besteht hier darin, das Passwort unmittelbar zu ändern. Veröffentlichte Daten erlauben dann keinen Zugriff auf das persönliche Konto mehr.

Passwörter und der große Datendiebstahl

Ein weiteres Einfallstor für Cyber Crime ist das Passwort. Durch Passwörter erhalten wir Zugang zu unseren E-Mails, gelangen zum persönlichen Auftritt in sozialen Netzwerken, nutzen Apps und andere technische Anwendungen oder greifen mit unserem festen Account auf ein System zu. Sowohl beim Zugang zu den persönlichen E-Mails wie auch in allen anderen genannten Bereichen spielt ein sicheres Passwort deshalb eine wichtige Rolle. Doch immer wieder kommt es vor, dass Passwörter geknackt werden.

Betrüger können dann Dienste unter dem eigenen Namen nutzen. Sie können mit E-Mails Bestellungen unter der eigenen Identität aufgeben, sich Zugriff auf Konten verschaffen und viel Schaden anrichten. Es kann unterschiedliche Gründe dafür geben, dass dies passiert. Zum einen können sich Kriminelle und Hacker Zugang zum System des Anbieters verschaffen.

Es ist noch nicht lange her, dass ein besonders großer Fall dieser Art von Internetkriminalität vorkam. Unbekannte verschafften sich Zugang zu den Servern von Universitäten und E-Mailanbietern. In manchen Fällen wurden die Zugangsdaten von Tausenden von Nutzern online im Klartext veröffentlicht. Über die entsprechenden Daten können sich dann Dritte einfach Zugang zum eigenen Mailaccount verschaffen. In manchen Fällen verkaufen Kriminelle solche Daten auch. In diesem Fall gelangen sie wohl noch gezielter in die Hände von Menschen, die kriminelle Vorhaben damit planen können. Unzählige Identitäten sind von dem Datendiebstahl betroffen. Und viele Verbraucher wissen bis heute nicht einmal, dass ihre Daten ausspioniert wurden.

Sichere Passwörter machen Betrügern das Leben schwer

Ein zweiter wichtiger Tipp zielt auf die Formulierung des Passwortes ab. Viele Hacker verschaffen sich Zugang zu Konten, weil die Nutzer ein zu einfaches Passwort verwendet haben. Ein Passwort mit dem eigenen Namen und Geburtsdatum lässt sich beispielsweise bereits ohne Kenntnisse der Informatik knacken. Aber auch andere Passwörter können mit entsprechenden Techniken leicht geknackt werden. Wer ein sicheres Passwort haben möchte, sollte deshalb die folgenden Ziele im Blick behalten.

Das Wort sollte wenigstens acht Zeichen enthalten. Je länger ein Passwort ist, umso schwerer können sich Dritte Zugriff verschaffen. Überdies sollte das Passwort sowohl Großbuchstaben wie auch Kleinbuchstaben enthalten. Anders als in sauberer Schriftsprache sollte es dabei nicht die typische Reihenfolge eines Großbuchstabens am Anfang und darauffolgende Kleinbuchstaben haben. Stattdessen sollte die Reihenfolge von Groß- und Kleinbuchstaben zufällig gewählt werden. Daneben sollte das Passwort auch Zahlen und Sonderzeichen enthalten. Sichere Passwörter machen deshalb oft gar keinen Sinn. Nun stellt sich natürlich die Frage, wie man sich ein solches sinnfreies Passwort merken soll. Damit es gut benutzt werden kann, müssen die Nutzer das geheime Passwort schließlich gut in Erinnerung behalten können. Dazu gibt es eine einfache aber nützliche Vorgehensweise, die im nächsten Abschnitt erläutert wird.

Professionelle Passwörter durch einprägsame Eselsbrücken entwickeln

Man kann Passwörter zufällig zusammenstellen. Eine gängige Variante besteht darin, die jeweiligen Buchstaben aus den Anfangsbuchstaben eines Satzes zusammenzustellen, der gut im Gedächtnis haften bleibt. Auch Satzteichen sollten in das Passwort eingefügt werden, zudem nach Möglichkeit eine Zahl. Die einfachste Vorgehensweise dafür geht wie folgt: Man wählt entweder einen Satz aus einem Film, den man gut kennt oder einem persönlichen Lieblingsbuch. Die Anfangsbuchstaben werden in das Passwort übersetzt. Am Anfang oder Ende kann auch die Jahreszahl des Films hinzugefügt werden. Im Falle eines Buches bildet die Seite, auf der sich der Satz im Buch findet, oder das Erscheinungsjahr die Zahl, die in das Passwort eingefügt wird. Bei Lieblingsbüchern lässt sich der Satz in der eigenen Ausgabe schnell wiederfinden.

Wenn das Passwort genutzt wurde, haftete es ohnehin im Gedächtnis. Auch bekannte Filmzitate bilden eine ideale Eselsbrücke für sichere Passwörter. Man muss sich nur zusätzlich merken, in welchem Jahr der Film erschienen ist. Die gleiche Technik funktioniert ebenso gut mit Zeilen aus einem Lied. Aus den ersten Zeilen des 1827 erschienenen Goethe-Gedichts "Der Zauberlehrling" ("Hat der alte Hexenmeister/ sich doch einmal wegbegeben!") kann mit der beschriebenen Technik etwa das Passwort "HdaHsdew!1827" entstehen.

Weitere Tipps für eine sichere Passwortnutzung im Alltag

Drittens sollten die Nutzer bei der Verwendung von Passwörtern Vorsicht walten lassen. Hier gibt es zwei wichtige Tipps. Zum einen sollte man nicht das immergleiche Passwort für viele verschiedene Dienste nutzen. Im besten Fall sollten für unterschiedliche Dienste verschiedene Passwörter verwendet werden, vor allem wenn sensible berufliche Informationen bewahrt werden sollen und im

anderen Fall soziale Netzwerke genutzt oder private Anwendungen verwendet werden. Zum anderen sollten Passwörter immer wieder gewechselt werden.

Wenn sich Diebe zwischenzeitlich Zugang zum Passwort verschafft haben, schiebt das neue Passwort dem fremden Zugriff erfolgreich einen Riegel vor. Wer diese beiden Tipps beherzigt, kann es den Betrügern schon sehr viel schwerer machen. In Unternehmen sollte man diese Hinweise auch an Mitarbeiter weitergeben. Zudem sollte die Technik es den Nutzern einfach machen, die persönlichen Passwörter immer wieder zu ändern.

Falls dafür ein großer Aufwand notwendig ist, werden viele Mitarbeiter diesen schon aus Bequemlichkeit scheuen. Manche Menschen wissen auch nichts von der beschriebenen Technik, mit der sie sich Eselsbrücken bauen und auch komplexere Passwörter merken können. Sie sollte einmal vorgestellt werden.

Phishing - so dreist ergaunern Kriminelle persönliche Zugangsdaten

Eine weitere verbreitete Form der Internetkriminalität ist unter dem Begriff Phishing bekannt. Der Begriff ist in Analogie zum englischen Wort fishing für Angeln gebildet worden. Er benennt die Versuche von Kriminellen, mit gefälschten Webseiten oder einer direkten Kontaktaufnahme nach persönlichen Zugangsdaten zu angeln. Meist wollen sich die Diebe mit solchen Versuchen Zugriff zu einem Bankkonto verschaffen oder anderen Konten verschaffen.

In nicht wenigen Fällen können sie auch große Summen der Betroffenen ergaunern. Während diese Technik in früheren Zeiten vor allem zum Klau von Bankdaten genutzt wurde, kommt sie heute bei unterschiedlichen Delikten zum Einsatz. Viele Betrüger ergaunern Passwörter aller Art, greifen anschließend im Rahmen krimineller Aktivitäten auf die Konten zu oder verkaufen die Daten an Dritte. In diesem Zusammenhang ist es wichtig, zu wissen, dass sich der Betrüger in jedem Fall strafbar macht.

Er muss die Daten nicht selbst zur Tat nutzen, indem er beispielsweise aktiv das Konto des Geschädigten leerräumt. Bereits das unbefugte Abrufen der Daten ist strafbar. Falls der Täter die dadurch erlangten Daten an Dritte verkauft, macht er sich wiederum der "Datenhehlerei" strafbar. Wie man anhand der Formulierung der Gesetze nachvollziehen kann, halten diese also sehr wohl mit dem digitalen Zeitalter Schritt. Längst haben diverse Tatbestände der Internetkriminalität in die Strafgesetzbücher Eingang gefunden.

Gängige Techniken bestehen darin, dass die Nutzer auf Webseiten gelockt werden, welche denen bekannter Unternehmen oder Banken fast gleichen. Die

Nutzer denken, dass sie sich auf der Homepage ihrer Bank befinden oder gerade in ihrem Ebay-Konto einloggen. Hier werden die Nutzer nun dazu aufgefordert, ihre Daten einzugeben. Dazu können Zugangsdaten, PIN-Nummern und vieles andere mehr gehören. Die Daten werden dann von Dritten abgegriffen. Beim Nutzen des Internets ist es also sehr wichtig, solche Daten nicht unbedacht einzugeben.

Wer sich im Internet bewegt, sollte im Zweifelsfall stets die Adresszeile seines Browsers im Blick behalten. Hier lässt sich meist schnell erkennen, ob man auf der Startseite der bekannten Homepage ist oder sich auf eine zwielichtige Seite verirrt hat. Wenn der Name der Bank oder der Plattform hier nicht erscheint und eine denkbar seltsame Adresse auch dann vorliegt, wenn man auf die Start-Seite klickt, so ist in jedem Fall Vorsicht angebracht. Wer sich an diesen Tipp hält, kann Phishing-Versuchen oft erfolgreich aus dem Weg gehen.

Mit der Zeit sind die Diebe dreister geworden. Heute kontaktieren sie Nutzer auch direkt, um entsprechende Daten in Erfahrung zu bringen. Wenn man von einem Unbekannten angerufen und nach entsprechenden Daten gefragt wird, sollte man diese nicht einfach herausgeben.

Banken weisen ihre Kunden heute auch explizit darauf hin, dass sie niemals in einfachen Mails nach geheimen Passwörtern fragen. PIN-Nummern werden von seriösen Banken zumeist per Post übermittelt oder mit Hilfe technischer Eingabegeräte speziell verschlüsselt. Wann immer Sie Anfragen erreichen, die von einem solchen Verfahren abweichen, sollten Sie hellhörig werden. Es gibt sogar Diebe, die sich telefonisch melden und direkt nach Bankdaten fragen. Auch in diesem Fall dürfen Zugangsdaten nicht unbedacht herausgegeben werden. Ansonsten haben Betrüger schnell freie Hand bei der Plünderung von Bankkonten.

Online-Banking sicher gestalten

Wo Kriminelle Geld im Internet ergaunern wollen, ist Onlinebanking eine wichtige Größe. Wenn hier ein Zugriff von Dritten gelingt, können Kriminelle unter Umständen direkt das Konto des Unternehmens oder der Privatperson leeren. Unzählige Privatnutzer wurden so bereits um Geld erleichtert.

Aber auch manches Großunternehmen ist geschickten Tricks von Betrügern aufgesessen. Es ist deshalb wichtig, einen sicheren Umgang beim Onlinebanking zu pflegen. Aber worauf sollte man speziell in dieser Hinsicht achten? Die folgenden Hinweisen geben wichtige Tipps für ein sicheres Onlinebanking. Mit ihrer Hilfe kann man die Fallen von Internetbetrügern umgehen.

Erstens ist es wichtig, auf der richtigen Seite zu landen. Deshalb sollte man die offizielle Homepageadresse der persönlichen Bank direkt in die entsprechende Zeile des Browsers eingeben. Auch ein Abruf über feste Lesezeichen erfüllt die gleiche Funktion. Die angesteuerte Zieladresse sollte dabei genau dem entsprechen, was die Bank in den eigenen Unterlagen ihren Kunden angibt.

Zweitens ist es notwendig, dass die Verbindung beim Abschließen von Geldgeschäften verschlüsselt wird. Ob dies der Fall ist, kann man an zwei Dingen erkennen. Zum einen taucht bei einer verschlüsselten Verbindung als "https" am Beginn der Adresszeile im Browser auf. Zum anderen weisen manche Browser die Nutzer zusätzlich durch ein symbolisches kleines Bild von einem Schloss auf eine verschlüsselte Verbindung hin.

Drittens sollte bei der Transaktion ein professionelles Sicherungsverfahren genutzt werden. Dieses gewährleistet, dass auch dann keine Überweisungen möglich sind, wenn Dritte den Vorgang im Netz beobachten können. Dazu verwenden die Banken heute spezielle Transaktionsnummern. Dabei ist jeweils nur eine solche Nummer notwendig. Falls beim Besuchen der Homepage gleich mehrere dieser Transaktionsnummern erfragt werden oder zusätzliche Daten wie die persönliche Adresse oder Informationen zur Kreditkarte eingegeben werden sollen, ist Vorsicht angesagt. In diesem Fall kann man damit rechnen, dass Betrüger einen in eine Falle locken möchten. Die Bank sollte unter diesen Umständen umgehend informiert werden.

Software kann Sicherheitslücken verursachen

Auch bekannte Programme können ungeahnte Sicherheitslücken eröffnen. Unternehmen und Nutzer sollten deshalb darauf achten, was für zusätzliche technische Tools und Zusatzprogramme auf den Geräten installiert werden.

Manches Plug-In kann ansonsten schnell dafür sorgen, dass der Computer angegriffen werden kann. Tatsächlich versuchen sich Betrüger auch diesen Weg zu Nutze zu machen. So kursieren heute unzählige Gratis-Möglichkeiten, welche Versprechen, dass bekannte Software kostenfrei heruntergeladen werden kann.

Fragwürdige Anbieter stellen Raubkopien von Software zur Verfügung. In vielen Fällen lädt sich der Nutzer mit dem Programm auch entsprechende Malware auf das eigene Gerät. Anschließend haben die Betrüger leichtes Spiel. Manchmal kann die Malware auch "nur" Schäden auf dem Computer anrichten. Es ist deshalb wichtig, solche leichtsinnigen Downloads möglichst zu umgehen. Software und Erweiterungen zur Software sollten nur von offiziellen Anbietern und seriösen Quellen erworben und heruntergeladen werden. Wann immer die Seriösität der Anbieter fraglich ist, sollte man auf einen Download verzichten. Auch die

Nutzung von Tauschbörsen, auf denen proprietäre Software kostenfrei angeboten wird, sollte man aus den genannten Gründen verzichten. Ansonsten können sich allzu schnell Gefahren ergeben. Gerade unbedarfte Nutzer wissen oftmals nicht, welche Probleme sie sich mit der Nutzung unseriöser Downloads und der Installation solcher Programme einhandeln können.

Vor dem Herunterladen aus unseriösen Quellen raten die Profis daher mit Recht eindringlich ab. Falls die bekannte Software zu teuer sein sollte, gibt es zwei Tipps. Zum einen gibt es oftmals eine freie Software, die ähnliche Funktionen erfüllt. Wenn private Nutzer sich etwas informieren, können sie meist erfolgreich auf diese ausweichen und Geld sparen.

Bei Unternehmen gibt es diese Möglichkeit nicht immer. Sie benötigen professionelle Programme, die ihnen ein breites Spektrum an Nutzungsmöglichkeiten zur Verfügung stellen und souverän bedient werden können. Allerdings haben Unternehmen oder Beschäftigte oftmals Möglichkeiten, mit denen sich eine professionelle Software von der Steuer absetzen lässt. Sie sollten dann eher diese Möglichkeit nutzen, als Risiken einzugehen, die zu erheblichen Sicherheitslücken führen können.

Der Identitätsdiebstahl als Cyber Crime-Delikt

Im heutigen Zeitalter zählt Identitätsdiebstahl ebenfalls zu den Delikten im Bereich des Cyber Crime. Diese Art von Betrug kann unterschiedliche Formen annehmen. Wenn Dritte Zugang zu verschiedenen privaten Informationen erlangen, können sie diese miteinander kombinieren. Je nachdem, was alles weitergegeben wurde, ermöglicht dies den Betrügern, sich im Internet als eine andere Person auszugeben. Sie können dann beispielsweise Bestellungen im Namen dieser Person aufgeben.

Manche Kriminelle haben es auch nur darauf abgesehen, einem Unternehmen oder einer Person zu schaden. Sie richten Profile in sozialen Netzwerken ein, mit denen sie sich als diese Person ausgeben. Anschließend können Bilder hochgeladen werden, welche die betroffene Person in ein schlechtes Licht rücken sollen. In diesem Fall bewegen wir uns nahe am Cyber Mobbing. Manche Betrüger erpressen ihre Opfer auch mit solchen Methoden.

Sie fordern Geld ein, wenn der Identitätsdiebstahl unterlassen werden soll. Es ist wichtig, in solchen Fällen die Polizei zu kontaktieren. Es handelt sich hier keineswegs um ein einfaches Delikt, sondern um eine strafbare Handlung. Die Polizei ist heute darauf vorbereitet, dass Menschen mit solchen Anzeigen vorstellig werden. Dennoch kann man die Betrüger nicht immer dingfest machen. Allzu oft verschleiern sie ihre eigene Identität und ihre Bewegungen im Internet.

Ein sicherer Umgang mit privaten Daten ist daher von großer Bedeutung. Je vorsichtiger Menschen hierbei vorgehen, umso mehr sinken die Chancen, selbst Opfer eines solchen Identitätsdiebstahl zu werden. Verhindern lässt sich dies allerdings nicht. Zu viele technische Anwendungen und Institutionen verfügen heute über unsere Daten und speisen diese ins Netz ein. Wenn an einer Stelle eine Sicherheitslücke auftaucht, können Dritte sich bereits Zugriff verschaffen. Selbst Banken wurden bereits gehackt. Nutzerdaten können dann ausgespäht werden.

Exkurs: Der Gesetzgeber auf EU-Ebene

Nicht ohne Grund wurde auf EU-Ebene zuletzt eigens eine neue Datenschutzverordnung verabschiedet, die mittlerweile auch in den Ländern greift. Sie soll verhindern, dass zu viele Daten gebündelt erfasst werden. Dritte können diese dann abgreifen und für ihre kriminellen Machenschaften nutzen. Das Gesetz hat deshalb Vorgaben gemacht, die dies möglichst einschränken sollen.

Diese Vorgaben fordern wiederum auch von den Unternehmen ein, dass sie selbst auf die Sicherheit der Daten achten, die sie von ihren Kunden erfassen. Selbst die Daten von Besuchern der Homepage eines Unternehmens dürfen nicht ohne Weiteres abgespeichert werden. Die Verordnung hat komplizierte Vorgaben gemacht, welche festlegen, dass die Besucher darüber informiert werden müssen, was für Daten von ihnen gespeichert wurden. Auch wer Datenbündel von Kunden in Formularen erfasst und abspeichert, muss nach der neuen Gesetzeslage eine Erlaubnis dafür einfordern.

Verbraucher sollen stets im Bilde darüber sein, welche Daten von ihnen erfasst wurden. Die Gesetzesänderungen in Verbindung mit der Datenschutzverordnung wurde von vielen Unternehmen als aufwändige Vorgabe wenig geschätzt. In Anbetracht der gestiegenen Internetkriminalität erscheinen entsprechende rechtliche Regelungen jedoch als sinnvoller Schritt.

Sie können möglicherweise noch besser umgesetzt werden, als dies im konkreten Fall geschehen ist. Dass der Gesetzgeber jedoch auf die neuen Herausforderungen des digitalen Zeitalters reagieren muss, steht außer Frage. Es dürften vermutlich noch weitere juristische Regelungen in den nächsten Jahren folgen.

Im Idealfall machen diese Internetbetrügern das Geschäft schwerer oder legen ihnen das Handwerk, ohne dass dabei die praktische Nutzbarkeit des Internets schwieriger wird.

Das sollten Nutzer und Unternehmen in Bezug auf private Daten beachten

Mit verschiedenen Vorsichtsmaßnahmen kann man es den Betrügern immerhin etwas schwerer machen. Dazu zählen auch wieder einfache Tipps, die sich in der Praxis ohne großen technischen Aufwand umsetzen lassen. Erstens sollten nur enge Vertraute in sozialen Netzwerken Zugriff auf ausführliche private Kontaktdaten und persönliche Fotos erhalten. Wer wenig von der eigenen Privatsphäre öffentlich online stellt, bietet den Betrügern eine geringere Angriffsfläche.

Das gilt insbesondere auch für den Gebrauch sozialer Netzwerke. Diese haben die Betrüger nämlich unlängst als Handlungsort für ihr schmutziges Spiel erkannt. Wer dafür sorgt, dass nur die eigenen Freunde alle Fotos sehen können, schränkt den Zugriff ein. In manchen Fällen lassen die Betrüger dann schon vom eigenen Profi ab, weil das Ausspähen in diesem Fall mit zu viel Arbeit verbunden ist.

Sicherheit und Social Media

Für viele Menschen gehören soziale Netzwerke heute zu den wichtigsten Anlaufstellen im Internet. Mit ihrer Hilfe vernetzen wir uns mit Freunden, die mittlerweile weit weg von unserem eigenen Wohnort wohnen und halten kontinuierliche Kontakte auf der ganzen Welt. Zudem werden die Plattformen auch genutzt, um berufliche Netzwerke zu knüpfen. In diesem Zusammenhang können sie auch die Karrierechancen fördern. Nicht wenige Nutzer geben deshalb auch ihre berufliche Laufbahn in den Netzwerken an.

Wenn diese öffentlich angezeigt wird, können Dritte diese Information unmittelbar abrufen und für ihre Zwecke einbinden. Ein weiterer Faktor trägt ebenfalls noch zur Beliebtheit der Plattformen bei. In der Regel teilen die Nutzer dort Bilder aus ihrem Leben. Sie dokumentieren damit ihr gutes Leben und zeigen etwas von ihrem Status. Daraus lassen sich wiederum Rückschlüsse darüber ziehen, wie vermögend ein Nutzer ist. Über viele der Bilder teilen die Nutzer zudem etwas über ihren Gefühlszustand oder persönliche Befindlichkeiten mit.

Auch darauf greifen Kriminelle heute zu und richten Schaden damit an. In manchen Fällen werden Bildmaterialien gestohlen und von anderen Accounts aus hochgeladen. Bei Menschen, die psychische Labilität signalisieren, können Betrüger erst Kontakt aufnehmen und dann Druck auf diese Menschen ausüben. Wenn solchen Betrügern sensible Informationen mitgeteilt oder private Bilder geschickt wurden, kommt es nicht selten auch zu Erpressungsversuchen. Als Nutzer sozialer Netzwerke sollte man die Möglichkeit auf dem Schirm haben, dass man selbst mit derartigen Gefahren konfrontiert wird. Einige Tipps können dazu beitragen, dass sich der Schaden in Grenzen hält.

Erstens sollte sich jeder Nutzer in den Einstellungen der jeweiligen Plattform über Datennutzung und Datenschutz informieren. Mit Hilfe dieser Einstellungen kann gezielt dafür gesorgt werden, dass nur Freunde private Bilder und Informationen angezeigt bekommen. Wenn man private Daten oder Bilder online stellt, sollten zweitens nur Freundschaftsanfragen von Menschen angenommen werden, die man auch persönlich kennt oder deren Identität einem zumindest bekannt ist. Je nachdem, was ein Nutzer oder eine Nutzerin alles online stellt, sollte er oder sie die Anfragen unbekannter Dritter besser ablehnen.

In manchen Fällen können diese Nutzer auch einen Status erhalten, der ihnen nur einen beschränkten Zugriff auf das eigene Profil gestattet. Drittens sollten über das Netzwerk nicht direkt private Adressen öffentlich ausgetauscht werden. Auch sensible Firmendaten sollten keineswegs über Foren oder Gruppen in sozialen Netzwerken ausgetauscht werden. Selbst wenn es sich um eine "geschlossene Gruppe" handelt, zu der auf der Plattform nur eingeladene Mitglieder Zugang haben, ist ein Verzicht auf einen solchen Austausch ratsam.

Wie vor einiger Zeit bekannt wurde, durchforsten manche Anbieter sowohl die Beiträge wie auch private Nachrichten der Nutzer nach bestimmten Informationen. Es gab sogar Fälle, in denen solche Daten dann an Unternehmen verkauft wurden, die Marketing-Analysen oder politische Beratung auf dieser Basis anbieten. In der Diskussion um "Big Data" wurde deutlich, dass manches Unternehmen hier Schindluder mit den Daten der Nutzer betreibt. Meist ist es schwierig, dies zu unterbinden. In aller Regel räumen die Nutzungsbedingungen der "kostenlosen" Plattformen den Betreibern nämlich die Rechte dafür ein.

Manche Nutzer sind deshalb unter einem Pseudonym in sozialen Netzwerken unterwegs. Manch einer verzichtet sogar bewusst auf die Nutzung. Für Unternehmen ist dies jedoch nicht so einfach. Zum einen muss es unter seinem echten Namen auftreten, um auch erkannt zu werden. Zum anderen sind soziale Netzwerke heute eine wichtige Anlaufstelle, um Marketing für eigene Produkte und Dienstleistungen zu betreiben und mit potentiellen Kunden in Kontakt zu treten.

Ein Verzicht auf die Nutzung sozialer Netzwerke ist für erfolgreiche Unternehmer deshalb heute kaum mehr möglich. Der Auftritt des Unternehmens darf jedoch auf keinen Fall mit dem internen Austausch verwechselt werden. Auch die Nutzung von manchen bekannten Kurznachrichtendiensten verbietet sich für den Austausch sensibler Daten. Der Austausch des Unternehmens sollte keineswegs über Chats und Gruppen der sozialen Netzwerke stattfinden. Er muss in einem gesicherten Rahmen ablaufen. Ansonsten läuft man Gefahr, das interne Informationen aus dem Unternehmen vom Anbieter abgerufen und sogar

ausgewertet werden, ohne dass man selbst dagegen aktiv werden kann. Diese Situation sollte tunlichst vermieden werden. Ein wichtiger Bestandteil der Firmenkultur besteht deshalb darin, die Mitarbeiter auch hier für das Thema zu sensibilisieren.

Sie sollten darüber informiert werden, dass soziale Netzwerke Sicherheitslücken enthalten. Für den internen Austausch gibt es professionelle Tools. Sie sorgen dafür, dass keine Daten abgegriffen oder ausgewertet werden.

Smart Home und intelligente Technik sorgen für neue Herausforderungen

Intelligente Technik macht vielen Menschen heute das Leben einfacher und erlaubt Unternehmen eine neue und effiziente Art der Produktion. Längst rufen Smartphones Updates selbstständig ab. Immer mehr technische Geräte tauchen auf, die in einem gewissen Rahmen selbstständig agieren, um ihren Nutzern den Alltag zu erleichtern.

Der Drucker, der ganz von selbst zum richtigen Zeitpunkt eine neue Patrone bestellt, ist ein Beispiel dafür. Aber auch Geräte wie der von Amazon vertriebene mit Spracherkennung ausgestattete Lautsprecher "Alexa" zeugen davon. In manchem Smart Home stellt sich die Technik individuell auf die Bedürfnisse der Nutzer ein. Um dies zu tun, müssen die technischen Geräte natürlich Daten erheben. Geräte wie Alexa vernetzen sich zudem mit dem Internet und anderen technischen Geräten. Aus den erhobenen Daten erstellen sie Nutzerprofile und schließen auf die Bedürfnisse ihrer Nutzer.

Bei der Bestellung weiterer Geräte können diese als Grundlage für eine individuelle und passgenaue Anfertigung dienen. Damit der Nutzer sich darum nicht kümmern muss, übernimmt die Technik dies für ihn. Die Dinge vernetzen sich. Es bildet sich ein "Internet of Things".

In dieses „Internet of Things“ können sich auch Unternehmen einklinken, welche die technischen Produkte verkaufen. Eine individuellere und schnellere Produktion ist möglich. Diese spart dem Kunden Zeit und verschafft ihm Bequemlichkeit. Den Unternehmen erlaubt sie eine kostengünstigere Just-in-time-Produktion, die zugleich optimal auf die Ansprüche der Kunden abgestimmt ist. Zugleich ergeben sich hier neue Herausforderungen auf der digitalen Ebene.
Durch das Internet of Things wird es nicht gerade leichter, die sensiblen Daten der Kunden sicher vor fremden Zugriffen zu bewahren. Das gilt sowohl auf Seiten der Verbraucher wie auch auf Seiten der Unternehmer. Schließlich müssen die Produzenten oder Anbieter von Dienstleistungen Sorge dafür tragen, dass die

intelligente Technik und die Wege, über welche diese Informationen sendet, sicher sind.

In der Informationstechnologie zählt die Erarbeitung sicherer Rahmenbedingungen für diesen Bereich wohl zu den großen Herausforderungen unserer Zeit. Zwei Ziele hat die Forschung dabei im Blick. Erstens sollten die Dinge, die sich mit dem Internet verbinden, ein sicheres Internet of Things gewährleisten. Ein zweites Ziel wäre freilich noch besser: Wenn die intelligente Technik die Unternehmen wie auch den Verbraucher gezielt auf Sicherheitslücken aufmerksam machen könnte. Bis wir dieses Ziel erreichen, dürfte es aber noch ein weiter Weg sein.

Die Abofalle - was sie ist und was man dagegen tun kann

Eine weitere Form der Abzocke im Internet ist die sogenannte Abofalle. In diesem Fall bieten Webseiten scheinbar kostenlose Internetdienstleistungen an. Wer die Nutzungsbedingungen genau durchliest, entdeckt, dass diese gar nicht kostenlos sind. Nutzer stellen schnell fest, dass ihnen monatliche Entgelte in Rechnung gestellt werden. Manchmal gehen die Betrüger so vor, dass Verbraucher auf eine SMS antworten sollen oder einen Code an eine bestimmte Nummer schicken sollen, um sich für den Dienst zu registrieren.

Indem die Nutzer dies tun, akzeptieren sie die Nutzungsbedingungen des Angebots. Dieses läuft dann auf den Abschluss eines monatlich fälligen Abos hinaus. Jeden Monat ergeben sich dann neue Kosten. Selbst wenn es sich um einen kleinen Betrag handelt, kann sich das Geld über die Zeit hinweg summieren. Die meisten Verbraucher wissen nicht, wie sie das angeblich abgeschlossene Abo kündigen sollen. Und die Anbieter stellen den Nutzern in aller Regel auch keine wirklich hilfreichen Informationen dafür zur Verfügung. Sie haben ein Interesse daran, weiter das Geld der unbedarften Verbraucher einzuziehen, die ihnen in die Falle gegangen sind.

Ein wichtiger Tipp zum Umgehen solcher Fallen lautet deshalb klipp und klar: Vor einer Registrierung bei einem Dienst oder dem Herunterladen von Programmen sollte man sich die Allgemeinen Geschäftsbedingungen durchlesen. Bei bekannten Anbietern kann auch ein Testbericht im Internet einen guten Einblick bieten. Wer gar eine SMS von einem unbekannten Absender erhält, die auf ein besonderes Angebot oder einen Gewinn hinweist, sollte ebenfalls hellhörig werden.

Betrüger haben diesen Weg perfektioniert, um unbescholtene Bürger in die Abofalle zu locken. Manchmal trifft es sogar Unternehmen. Allerdings hat der Gesetzgeber in einzelnen Ländern auf diese Entwicklung bereits reagiert.

Deutschland ist ein Beispiel dafür. Hier gab es entsprechende gesetzliche Änderungen. Diese zielen darauf ab, den Anbietern von Abofallen das Handwerk zu legen.

Die Regelung schreibt deutschen Anbietern vor, dass sie kostenpflichtige Inhalte durch einen Button auf der Seite deutlich machen müssen. Dieser muss für den Verbraucher klar erkennbar sein. Im Falle eines Abonnement-Angebots müssen die Anbieter auf ihrer Homepage sowohl den Preis wie auch die Mindestlaufzeit des Angebots explizit benennen. Alle Angebote, die über deutsche Server laufen, müssen ihr genaues Angebot also klar kennzeichnen. Doch es gibt genügend Seiten, die im Ausland betrieben werden und die deshalb nicht an diese Regelungen gebunden sind. In diesem Fall kann der generelle Verzicht der Dienstleistungen von ausländischen Anbietern, die noch keinen guten Namen haben, von Vorteil sein.

Auch wenn man in eine Abofalle hineingetappt ist, gibt es noch Handlungsmöglichkeiten. Gegen unberechtigte Forderungen können Nutzer nämlich Widerspruch einlegen. Wenn die Anbieter die Geschäftsbedingungen nicht deutlich machen, konnte der Betroffene auch nicht wissen, worauf er sich einlässt.

Falls sogar kostenfreie Nutzung versprochen wurde, liegt sogar eine Täuschung vor. Es ist nun wichtig, dass man einen solchen Widerspruch auf richtige Weise einlegt. Dies ist jedoch kein großer Aufwand. Es gibt Musterschreiben, die genau dafür entwickelt wurden und verwendet werden können. Diese Schreiben können von Verbrauchern selbst verwendet werden, ohne dass dafür eine Kanzlei oder ein Anwalt beauftragt werden muss.

Musterschreiben dieser Art erhält man auf den Internetseiten der Verbraucherzentralen. Überhaupt haben die Verbraucherzentralen eigene Informationsangebote, die über Abofallen informieren. Wer sein Wissen in diesem Bereich vertiefen möchte, kann sich über diese Seiten weiterführende Informationen über Abofallen und die rechtliche Handhabe dagegen verschaffen. Diese machen schnell deutlich, dass man nicht jeder Drohung sofort auf den Leim gehen muss.

Die Datenverarbeitung im Unternehmen

In Unternehmen werden viele verschiedene Daten verarbeitet. Manche dieser Daten müssen von vielen oder allen Mitarbeitern eingesehen werden können. Ein einfaches Beispiel dafür wäre etwa ein Dienstplan, über den man sich austauscht,

wer wann arbeitet. In manchen Plänen werden dabei auch Aufgaben vermerkt, die in bestimmen Bereichen erledigt werden.

In diesem Fall landen wir schnell bei sensibleren Informationen. Schließlich können aus solchen Daten bereits Arbeitsstände zu wichtigen Projekten erahnt werden. Auch sensible Informationen über Kunden des Unternehmens können daraus hervorgehen. Schnell ergeben sich also Graubereiche. Zudem gibt es in Unternehmen auch solche Informationen, die besonders sensibel sind.

Haushaltszahlen können dazu zählen. Aber auch Informationen über Beschäftigte, wie sie beispielsweise in Personalakten erfasst werden. Hier haben die Beschäftigten sogar ein Recht darauf, dass diese Informationen sicher verwahrt werden, so dass Dritte keinen Zugriff auf sie erhalten.

Damit wird schnell deutlich, dass bei der Arbeit mit Daten unterschiedlich hohe Sicherheitsvorkehrungen zu treffen sind. Einerseits sollen diese Sicherheits-vorkehrungen nun gewahrt werden. Andererseits sollte ein möglichst flexibler Umgang mit Daten möglich sein, der es den Mitarbeitern leicht macht, an genau die Informationen zu kommen, die sie für ihre Arbeit benötigen. Welche Schlüsse ergeben sich daraus für die Sicherheit und Vorkehrungen gegen Internet-kriminalität?

Ein Unternehmen sollte seinen Mitarbeitern einen unterschiedlichen Status zuordnen. Professionelle EDV erlaubt die gezielte Einteilung in verschiedene Statusgruppen. Wenn sich der Mitarbeiter oder die Mitarbeiter mit seinem Account im System anmeldet oder in der Cloud einloggt, wird er oder sie entsprechend eingeordnet.

Das bedeutet, dass die einzelnen Personen nur zu genau den Informationen Zugang erhalten, die sie auch brauchen. Eine solche Maßnahme ist nicht nur für den internen Datenschutz wichtig. Sie ist von enormer Bedeutung, wenn es um den Schutz vor Internetkriminalität geht. Wenn nur ein kleiner Kreis an Führungskräften Zugriff auf besonders sensible Daten hat, gestaltet sich naturgemäß auch die Angriffsfläche für Eingriffe wesentlich geringer. Aus genau diesem Grund zählt die Zuteilung von eingeschränkten Nutzerkonten zu den wichtigsten praktischen Maßnahmen gegen Internetkriminalität. Sie bringt gleich noch einen zweiten Vorteil: In der Regel dürfen bei solchen Zuteilungen nur Administratoren des Systems Programme und technische Anwendungen installieren. Falls ein einfacher Nutzer sich versehentlich eine Malware einfängt, kann diese sich in der Regel nicht unmittelbar installieren. Der genutzte Account hat nicht die Rechte, frei Hand Programme zu installieren. Auf diese Weise wird eine weitere Brücke gegen manche Malware geschaffen. Ein dritter Vorteil

unterschiedlicher Statusgruppen ist ein erweiterter Schutz gegen die Vorhaben frustrierter Mitarbeiter.

In manchen Fällen kann es passieren, dass ein Mitarbeiter aus Enttäuschung oder Frustration Schaden im Unternehmen anrichtet. Die Möglichkeiten des digitalen Netzwerks können hier Türen öffnen. Wenn Mitarbeiter jedoch nur auf eigene Daten Zugriff haben und sensible Informationen nur von der Führungsebene aus aufgerufen werden können, sinkt auch die Wahrscheinlichkeit solcher Risiken.

Fester Bestandteil der Datensicherheit: die regelmäßige Datensicherung

Malware kann ganze Systeme lahmlegen. Manche Erpresser legen es auch darauf an, den Zugang zum Computer zu sperren. Erst nach Transfer von Geld, wollen sie den Zugang wieder freigeben. In beiden Fällen wird dem Unternehmen der Zugriff auf die Festplatten versagt. Sie haben Informationen nicht, die sie für den Betriebsablauf dringend brauchen. Malware kann aber auch dafür sorgen, dass die Festplatte beschädigt, Daten verschwinden oder nicht mehr genutzt werden können. Für private Nutzer ist dies ebenso ärgerlich wie für Unternehmen. Mit einer wichtigen Vorbeugemaßnahme lässt sich der Schaden einer solchen Situation begrenzen. Es ist wichtig, dass die Daten regelmäßig gesichert werden. Bei der Datensicherung sollten verschiedene Tipps beachtet werden.

Alle Dateien, die von Bedeutung sind, sollten gesichert werden. Das bedeutet konkret, dass auf einem externen Speichermedium eine Kopie dieser Datei angefertigt wird. Es gibt für diese Zwecke eigene Anwendungen. In der Regel verwendet man in Unternehmen eine entsprechende Backup-Software, die sich automatisch und genau nach Vorgaben um das regelmäßige Abspeichern kümmert.

Manche Unternehmen speichern Backups auch in einem zweiten und separaten Rechenzentrum. Falls es beispielsweise zu einem Brand kommt, kann dies betroffene Daten retten. Zudem gibt es die Möglichkeit, Daten in einer Cloud zu spiegeln. In diesem Fall müssen die Daten jedoch gut gegen äußere Maßnahmen abgeschirmt werden. Entsprechende Handhabungen können schnell sehr teuer werden. Beim regelmäßigen Abspeichern ist die Bedeutung der Daten für das unternehmerische Handeln ein wichtiger Faktor. Je sensibler oder wichtiger die Daten sind, ums häufiger sollten sie auch gesichert werden. Je nach Sensibilität können sich verschieden viele Sicherungskopien empfehlen.

Empfehlung: Daten beim Sichern verschlüsseln!

Sensible Daten sollten nicht einfach so abgespeichert werden, so dass sie anschließend auf der Sicherungskopie oder der internen Festplatte frei geöffnet

werden können. Eine wichtige Technik gegen Cyber Crime besteht hier in der Verschlüsselung. Es gibt verschiedene Techniken, mit denen dies bewerkstelligt werden kann.

Eine Möglichkeit ist die Software GPG (GNU Privacy Guard). Hinter dem Kürzel verbirgt sich ein freies Kryptographie System. Eine andere Variante besteht in der Verschlüsselung der Festplatte. Übrigens sind nicht nur Daten von diesem Problem betroffen, die sich fest in den Händen des Unternehmens befinden. Auch und gerade dann, wenn es zum Transfer von Daten im Internet kommen soll, ist eine professionelle Verschlüsselung unabdingbar.

Wenn also beim Onlineshopping auf der Seite des Unternehmens Bankdaten übertragen werden, ist auf die Sicherheit zu achten. Die Übertragung kann in diesem Fall durch Hypertext Transfer Protocol Secure (HTTPS) gesichert werden. Diese erlaubt nur solchen Parteien Zugriff auf die verschickten Daten, die den passenden Schlüssel bereithalten. Auch bei der Nutzung von offenen WLANs ohne Passwort kann es zu Risiken kommen. Wenn hier keine Verschlüsselung zustande kommt, können im Ernstfall Dritte unbemerkt die verschickten Daten auslesen.

Nicht nur für Unternehmen spielt die Datensicherheit in dieser Hinsicht heute eine Rolle. Auch staatliche Institutionen und Behörden sind mit den Problemen konfrontiert, die sich aus Cyber Crime und Internetkriminalität ergeben. Wenn es um den Transport von Daten geht, sind gute Kenntnisse der Datensicherheit gefragt. Zugleich erfordert das alltägliche Geschäft eine permanente Verfügbarkeit von Kundendaten. Wenn die Institutionen und Behörden hier nicht höchste Sicherheit im Austausch walten lassen, können die Daten von Unternehmen und Verbrauchern ebenfalls unbefugt in die Hände Dritter geraten.

Die meisten Institutionen haben genau deshalb sehr strikte Vorgaben für die Abläufe, mit denen Daten übermittelt, abgespeichert oder transportiert werden. In nicht wenigen Fällen kann sich nach wie vor der Schriftverkehr für den Austausch empfehlen.

Er ist sicherer als der digitale Austausch. Anders als bei E-Mails und digitalen Datenübertragungen kann bei einem verschlossenen Brief kein Internetbetrüger die Daten während der Verschickung ungesehen kopieren.

Professionelle Datenvernichtung im Blick behalten!

Ein weiterer Tipp zum Schutz gegen unerlaubten Datendiebstahl besteht in einer sicheren Vernichtung alter Daten. Wenn Informationen nicht mehr benötigt werden oder gelöscht werden müssen, muss dies auf professionelle Weise

geschehen. Auf einer Festplatte können sie direkt gelöscht werden. Alte Festplatten sollten zudem vernichtet werden, so dass Dritte sich keinen Zugang zu den darauf abgespeicherten Informationen mehr verschaffen können. Auch externe Sicherungskopien müssen auf diese Weise vernichtet werden. Wenn also Backups auf einer DVD oder CD gespeichert wurden, so darf diese niemals in einem einfachen Mülleimer landen.

Unbefugte könnten sie aus diesem herausholen und Informationen auslesen. Es reicht auch nicht, die CD zu verkratzen oder zu brechen. Mit der richtigen Technik können Betrüger auch von beschädigten Speichermedien unter Umständen noch Daten auslesen. Wie es Firmen gibt, die Akten vernichten, so gibt es auch für digitale Speicher die richtigen Dienste. Staatliche Behörden nutzen deren Angebote nach Vorschrift. Auch Unternehmen sollten im Fall von sensiblen Daten auf Nummer sicher gehen. Wer einen solchen Dienst zur Vernichtung des Speichermediums in Anspruch nimmt, kann sich sicher sein, dass die vorhandenen Daten auch sicher vernichtet wurden und nicht mehr von Dritten ausgelesen werden.

Empowerment der Mitarbeiter stärkt souveränen Umgang

Ein wichtiger Faktor für Sicherheit gegen Cyber Crime besteht nicht nur in der Technik alleine. Vor allem die Mitarbeiter selbst spielen hierbei eine Rolle. Je besser sie für das Thema sensibilisiert wurden, umso weniger Angriffsfläche bietet das Unternehmen Betrügern und Angreifern aus dem Internet. Für das Unternehmen selbst bedeutet dies, dass es seine Mitarbeiter schulen muss. Das heißt in diesem Fall, dass nicht nur die Führungskräfte sich mit der Thematik der Datensicherheit und des souveränen Umgangs mit digitalen Systemen und technischen Anwendungen auskennen sollten. Alle Mitarbeiter sollten ein Bewusstsein hierfür entwickeln.

Das Unternehmen selbst muss sich dabei auch immer wieder weiter entwickeln. Es sollte mit der technischen Entwicklung und der Zeit Schritt halten. Das Unternehmen wird so zur lernenden Organisation, die sich der Digitalisierung bewusst stellt. Aber was sollten Unternehmen beachten, wenn sie einen Schritt in diese Richtung tun und die digitale Kompetenz zum Bestandteil der eigenen Unternehmenskultur machen wollen? In der Organisationswissenschaft gab es dazu eine Debatte, die in mehreren Etappen verlaufen ist.
Als die Diskussion um Internetkriminalität erstmals aufkam, ergab sich schnell die Frage, wie Unternehmen ihre Mitarbeiter zu dieser Thematik schulen sollen. Dabei definierte die Organisationswissenschaft und Unternehmensberatung zunächst vor allem ein Ziel: Die Mitarbeiter sollten auf mögliche Gefahren aufmerksam gemacht werden.

Unternehmen sollten Mitarbeitern sensibilisieren - oder auf Englisch formuliert: Sie sollten im Kreis der Mitarbeiter für eine digitale "Awareness" sorgen. Als Ergebnis einer solchen Arbeit sollten ihnen Risiken gegenwärtig sein. Sie sollten mögliche Gefahren des digitalen Datenverkehrs und Cyber Crime bewusst auf dem Schirm haben. Gegenüber einem allzu naiven Gebrauch digitaler Techniken ist mit solchen Schulungen ein wichtiger Schritt getan. Allerdings wurden schnell auch die Grenzen einer solchen Arbeit deutlich.

In manchen Fällen ergaben sich nachweislich oft Ängste bei den Beschäftigten. Sie wussten nun um alle möglichen Gefahren und wussten nicht so richtig, wie sie damit umgehen sollen. War es nicht besser, zumal sicherer, dann auf die Nutzung digitaler Technik zu verzichten? In der heutigen Zeit ist dies jedoch nicht mehr möglich und auch nicht sinnvoll.

In der zweiten Etappe der wissenschaftlichen Diskussion hat sich die Zielrichtung deshalb etwas verschoben. Es geht nicht mehr nur um Sensibilisierung, sondern um gezielte Befähigung der Mitarbeiter. Sie sollten also ermutigt werden, die Technik auf die richtige Art zu nutzen und sich von selbst sicher im Internet zu bewegen. Die Ergebnisse einer solchen Arbeit können mehr Erfolge in den Unternehmen vorweisen.

Dabei hat sich gezeigt, dass die Führungskräfte oft Vorbildfunktion haben. Wenn sie gerne und souverän mit digitaler Technik umgehen, eifern die anderen Mitarbeiter ihnen schnell nach. Überdies sollte das Unternehmen in regelmäßigen Abständen Qualifikationsangebote für die Mitarbeiter anbieten und dafür einen angenehmen Rahmen schaffen. Auf diese Weise schafft man Akzeptanz für die notwendigen Lernprozesse.

Aktuelle Trends im Kampf gegen Internetkriminalität

Die Nachfrage nach professioneller Software zur Absicherung von Unternehmen ist ebenso groß wie auch der Bedarf an Qualifikationsmaßnahmen und externer Beratung. Große Unternehmen und auch mittelständische Betriebe geben heute viel Geld aus, um Software auf dem aktuellen Stand zu halten und Malware mit aktuellen Anti-Viren-Programmen zu identifizieren und unter Quarantäne zu stellen. Sie wissen genau, dass sie mit diesen Kosten Risiken abwenden, die ansonsten noch teurere Ausgaben ergeben könnten. Auch was die Qualifikation von Mitarbeitern betrifft, gibt es eine steigende Tendenz. Nicht wenige Betriebe nehmen dafür externe Expertise in Anspruch. Sie laden Experten zu Schulungen ein, bei denen die Mitarbeiter einen professionellen Umgang mit den verwendeten Anwendungen und Geräten erlernen.

Private Nutzer informieren sich ebenfalls über die Tücken des Internets. Schulen haben das Thema Datensicherheit und Gefahren des Internets auf ihre Lehrpläne genommen. Ratgeber bereiten Eltern darauf vor, wie sie ihre Kinder bei der Nutzung der ersten Smartphones pädagogisch sinnvoll begleiten können. Senioren besuchen Volkshochschulkurse, um im Gebrauch des Computers oder bei der Nutzung des neuen Smartphones mit ihren Enkeln Schritt halten zu können. Alle diese Maßnahmen können mehr Sicherheit ermöglichen. Sie sorgen dafür, dass sich Nutzer im Netz nicht allzu naiv verhalten. Wie aus den erschreckenden Zahlen über Internetkriminalität aber deutlich hervorgeht, lässt sich eine absolute Sicherheit auf diesem Weg jedoch nicht erreichen. Was bedeutet dieser Tatbestand nun für die Unternehmen?

Ohne Resilienz werden Unternehmen Opfer

Bei der Bekämpfung von Cyber Crime lässt sich gegenwärtig eine kleine Akzentverschiebung beobachten. Ging es früher oftmals nur um die Prävention, so haben viele Unternehmen heute eine erweiterte Ausrichtung ihrer Maßnahmen im Blick. Diese lässt sich mit dem Begriff der Resilienz fassen. Resilienz ist ein Begriff, das ursprünglich in der psychologischen Debatte Fuß gefasst hat. Es bezeichnet die psychische Widerstandsfähigkeit, mit der ein Mensch auf Krisen oder bestimmte Situationen reagiert.

Während diese Situationen für die einen Menschen zur sprichwörtlichen Zerreißprobe werden, halten resiliente Menschen auch unter der kritischen Situation stand. Sie sind sozusagen auf die Möglichkeit der Krisensituation vorbereitet und wenn sie eintritt, lassen sie sich nicht von dieser verängstigen, sondern bleiben weiter handlungsfähig. Auch unter Situationen der Unsicherheit lassen sich resiliente Menschen nicht verunsichern. Das ist genau der Ansatz, mit dem der aus der psychologischen Forschung stammende Begriff heute in den Debatten über die Digitalisierung aufgegriffen wird. Christian Schuldt verweist etwa auf die Komplexität und Unsicherheit, die das digitale Zeitalter mit sich bringt. Er hält es für elementar, dass Unternehmen und Nutzer sich mit dieser Unsicherheit auseinandersetzen.

Unsicherheiten und auch Bedrohungen können nicht vollständig vermieden werden. Deshalb ist es wichtig, den einzelnen Menschen darauf vorzubereiten, dass sie eintreten. Er oder sie soll in seinem Handeln auch im Ernstfall sicher und souverän bleiben. Für die Unternehmen bedeutet dies, dass sie ihren Fokus darauf legen, Sicherheitsverstöße nicht nur zu unterbinden. Sie sollten ein System entwickeln, mit dem diese möglichst schnell erkannt werden und durch das im Ernstfall eine schnelle Behebung der Problemsituation möglich wird.

Das richtige Personal

Ein wichtiger Faktor im Kampf gegen Internetkriminalität ist auch gut ausgebildetes Personal. Wer einen Administrator oder eine Fachkraft hat, die genau weiß, was im Ernstfall zu tun ist, kann schnell Schadensbegrenzung betreiben. Auch dieser Faktor zählt bei der Frage der Resilienz von Unternehmen im digitalen Zeitalter. Allerdings können Unternehmen hier auch vor manchen Herausforderungen stehen. Tatsächlich macht sich in diesem Bereich nämlich ein gewisser Fachkräftemangel bemerkbar. Experten, die eine informatische Expertise mitbringen und als Profis gegen Internetkriminalität aktiv werden können, gibt es nicht wie Sand am Meer.

Im besten Fall sollten diese Menschen auch noch eine ruhige Hand mitbringen und in Krisensituationen Führungsqualitäten beweisen. Noch besser wäre es, wenn sich die Qualitäten dieser Menschen auch auf andere Beschäftigte im Betrieb übertragen könnten. Dazu müssten sie entsprechende Qualitäten in der Vermittlungsarbeit mitbringen. Nur wenige Fachkräfte vereinen alle diese Vorteile auf sich.

Wenn ein Unternehmen die Chance bekommt, einen Fachmann einzustellen, der mehrere dieser Qualitäten vereint, sollte es ohne Zweifel zugreifen. Sicherheitsexperten dieser Art sind ein entscheidender Schlüsselfaktor im digitalen Zeitalter. Es gibt ansonsten auch die Möglichkeit, sich externe Unterstützung ins Boot zu holen. Allerdings hat dies den Nachteil, dass die externen Experten im Ernstfall nicht bereits direkt vor Ort sind. Zudem haben eigene Mitarbeiter in manchen Fällen einen besseren Überblick über die Architektur des Betriebssystems und die genaue Gestaltung der digitalen Sicherheitsvorkehrungen, die ein Unternehmen getroffen hat.

Anlaufstellen und Tipps für den Ernstfall

Falls man bereits Opfer von Cyber Crime geworden ist, kann ein solches System einem bei schnellem Handeln helfen. Neben dem richtigen Plan für ein geplantes Vorgehen kann auch die Kenntnis wichtiger Anlaufstellen für Betroffene die entscheidende Hilfe bieten. Für private Nutzer geben die Seiten der Verbraucherzentrale dazu weiterführende Hinweise. Bei unrechtmäßigen Kostenforderungen oder Abmahnungen kann sich die Kontaktaufnahme mit einem Anwalt empfehlen. Es gibt Kanzleien und Anwälte, die sich auf Auseinandersetzungen um das Internet und Internetkriminalität spezialisiert haben. Im Fall von Erpressung oder Diebstahl ist die Polizei die richtige Anlaufstelle. Hierzu ist es wichtig zu wissen, dass die Polizeien der Länder eigene Stellen eingerichtet haben, die sich um das Thema Internetkriminalität kümmern.

Das Bundeskriminalamt (BKA) der Bundesrepublik Deutschland hat zudem eine offizielle Handreichung herausgegeben. Die Broschüre "Cybercrime - Handlungsempfehlungen für die Wirtschaft" kann online abgerufen werden. Sie enthält wichtige Tipps für den Ernstfall. Zudem finden sich in der Broschüre die zuständigen Anlaufstellen der Bundesländer mit den jeweiligen Kontaktdaten.

Aus der Broschüre geht auch hervor, dass es eine große Dunkelziffer im Bereich der Internetkriminalität gibt. Viele Vorkommnisse werden nicht angezeigt. Für den Verzicht auf eine Anzeige kann es die unterschiedlichsten Gründe geben. Manchmal haben Firmen beispielsweise Angst, dass im Zuge von Ermittlungen deutlich werden könnte, dass sie Software nutzen, ohne eine offizielle Lizenz für diese zu haben.

In anderen Fällen gehen die Probleme nicht von externer Seite aus, sondern wurden von einem Mitarbeiter verursacht. Dies kann dazu führen, dass man das Geschehen intern unter den Teppich kehren will. Bei einfachen Fehlern ist dies auch kein Problem. Es muss nicht in allen Fällen sofort Anzeige erstattet werden. Wer jedoch schwerwiegende Straftaten wie Erpressung nicht zur Anzeige bringt, schränkt laut BKA eine effektive Bekämpfung von Cyber Crime ein.

Die Broschüre bietet zudem einen schnellen Überblick über die unterschiedlichen Straftatbestände im Bereich der Internetkriminalität. Dies ist für alle Nutzer von Vorteil, die sich nicht erst ausführlich in komplizierte Gesetzestexte einlesen möchten. Bei einem Teil der aufgelisteten Tatbestände ist es vielen Verbrauchern gar nicht bewusst, dass diese explizit gesetzlich untersagt sind. Sie wissen deshalb gar nicht, dass sie in Deutschland eigentlich eine klare rechtliche Handhabe haben. Auch in anderen deutschsprachigen Ländern wie Österreich oder der Schweiz gibt es klare rechtliche Regelungen Das Wissen um das Recht im Zusammenhang mit dem Internet ist noch nicht in allen Köpfen angekommen.

Welche Straftatbestände definiert das Strafgesetzbuch?

Das Strafgesetzbuch der Bundesrepublik Deutschland - um ein prominentes Beispiel zu wählen - definiert eine ganze Reihe von Straftatbeständen, die in Bezug auf Internetkriminalität von Bedeutung sind. Dazu zählt etwa das "Ausspähen von Daten" Dritter. Dieses ist nach §202a StGB strafbar. Gleiches gilt auch für das "Abfangen von Daten" (§202b StGB). Ferner wird im § 202c StGB bereits das "Vorbereiten des Ausspähens und Abfangens von Daten" untersagt. Auch wer also fremden die Möglichkeit verschafft, auf diesem Wege an sensible Daten zu kommen, macht sich strafbar. § 202d StGB untersagt die "Datenhehlerei". Neben diesen Tatbeständen wird aber nicht nur das Abrufen von Daten untersagt. Auch deren Manipulation kann strafbar sein. Deshalb untersagt

§ 303a StGB die "Datenveränderung" durch Löschung oder Unterdrückung bestimmter Informationen, während § 269 StGB die "Fälschung beweiserheblicher Daten" verbietet.

Eine weitere wichtige Regelung ist in § 303b StGB festgehalten. Hier wird erläutert, wann genau der Tatbestand der "Computer-sabotage" vorliegt. In Österreich und der Schweiz gibt es ebenfalls Gesetze, die sich gegen Internetkriminalität wenden. Wer von entsprechenden Vorfällen betroffen ist, kann sich hier auch selbst darüber schlau machen, welche Straftatbestände im Einzelnen vorliegen könnten. Im Zweifelsfall kann dann Anzeige erstattet werden. Die konkrete Prüfung muss zuletzt ein Gericht vornehmen.

Literatur

- Bartsch, Michael/ Frey, Stefanie (2018): Cybersecurity Best Practices: Lösungen zur Erhöhung der Cyberresilienz für Unternehmen und Behörden
- Bullinger, Hans-Jörg/ Hompel, Michael ten (2007): Internet der Dinge
- Bundeskriminalamt: Cybercrime - Handlungsempfehlungen für die Wirtschaft, abrufbar über: https://www.polizei.de/Polizei/DE/Einrichtungen/ZAC/zac_node.html
- Gattiker, Urs E. (2004): The Information Security Dictionary
- Graham, James/ Olson, Ryan/ Howard, Rick (2018): Cyber Security Essentials
- Klipper, Sebastian (2015): Cyber Security: Ein Einblick für Wirtschaftswissenschaftler
- Nehls, Marin (2018): Cybercrime und Kriminalität im Internet - Methoden zur Minimierung des Dunkelfeldes
- Rudder, Christian (2016): Inside Big Data. Unsere Daten zeigen, wer wir wirklich sind
- Schneier, Bruce (2015): Data und Goliath. Die Schlacht um die Kontrolle unserer Welt: Wie wir uns gegen Überwachung, Zensur und Datenklau wehren müssen
- Weiser, Mark: The Computer for the 21st Century, in: Scientific American (September 1991), abrufbar über: https://www.lri.fr/~mbl/Stanford/CS477/papers/Weiser-SciAm.pdf
- Europäisches Verbraucherzentrum Deutschland: Informationen zum Thema Abofallen: https://www.verivox.de/ratgeber/schutz-vor-internet-kriminalitaet-59218/
- Identity Leak Checker des Hasso-Plattner-Instituts, Universität Potsdam: https://sec.hpi.de/ilc/search
- Schuldt, Christian: Ein neuer Blick auf Digitalisierung, abrufbar über: https://www.zukunftsinstitut.de/artikel/digitalisierung/ein-neuer-blick-auf-digitalisierung/
- Statistik zu angezeigten Fällen von Cybercrime in Österreich: https://de.statista.com/statistik/daten/studie/294141/umfrage/cybercrime-in-oesterreich/
- Umfrage des Bundesamtes für Sicherheit in der Informationstechnik: https://www.allianz-fuer-cybersicherheit.de/ACS/DE/Informationspool/Cyber-Sicherheits-Umfrage/CyberSicherheitsUmfrage_2018/cs_umfrage_2018_node.html;jsessionid=076D7980DA9189C8062443C415BB715A.1_cid341