Ausgabe 2 – Mai 2017

tribune

Das Magazin mit unternehmerischen Visionen

Editorial

Dr. Philip Baumann
Geschäftsfeld Basel
Notenstein La Roche
Privatbank AG
philip.baumann@
notenstein-laroche.ch

Als dieses Magazin produziert wurde, berichteten die Medien gerade über einen aufgeflogenen Schweizer Spion, der im Auftrag unseres Nachrichtendienstes die Aktivitäten deutscher Steuerfahnder in unserem Land ausspioniert haben soll. In der verworrenen Agentenstory spielten unter anderem wieder einmal illegal beschaffte CDs mit Angaben zu mutmasslichen Steuerhinterziehern eine Rolle.

Der Klau sensibler Daten ist auch das Thema der vorliegenden «tribune»-Ausgabe. Heutzutage müssen dafür aber nur noch in Ausnahmefällen Schlapphüte ausrücken und heimlich physische Speichermedien brennen und verkaufen. Kriminelle auf der Höhe der Zeit bewegen sich als «Hacker» im virtuellen World Wide Web, wo sie längst nicht nur mehr Daten klauen, sondern auch offensichtlich Wahlen manipulieren.

Unternehmen mit Visionen, an die sich diese Publikation ja richtet, entnehmen den Beiträgen dieser Themennummer nützliche Hinweise auf die Herausforderungen, vor die sie sich bei der Verteidigung ihrer wichtigsten Werte gestellt sehen. Sie werfen einen Blick hinter die Kulissen von Spezialisten, die im ausdrücklichen Auftrag von Firmen in deren eigene Netzwerke einbrechen. Und sie erfahren mehr über die komplexe juristische Situation auf dem sich ausweitenden Feld der Cyber-Kriminalität.

Ich wünsche Ihnen informative Lektüre.

Cyberrisiken

Eine Publikation der Handelskammer beider Basel, der Advokatenkammer Basel und des Basellandschaftlichen Anwaltsverbands mit grosszügiger Unterstützung der Jubiläumsstiftung La Roche & Co Banquiers.

handelskammer beider basel

NOTENSTEIN LA ROCHE PRIVATBANK

Advokatenkammer Basel
Basellandschaftlicher Anwaltsverband

Cyberrisiken – eine reale Bedrohung

Reto Häni
Partner und Leiter Cybersecurity,
PwC Digital Services
reto.haeni@ch.pwc.com

Über die Auswirkungen von digitalen Gefahren ist heute in der Tagespresse regelmässig zu lesen. Und dennoch wissen die wenigsten Firmen und Privatpersonen, was man gegen diese inzwischen zur Tagesordnung gehörenden Cyberangriffe tun kann. Aber es sind nicht nur die Risiken, die zunehmen. Auch neue Technologien lassen sich immer einfacher einsetzen und digitale Geschäftsmodelle setzen sich durch. Wer die digitale Transformation richtig nutzt und für eine angemessene Datensicherheit sorgt, kann interessante Vorteile daraus ziehen und daran wachsen.

Die Bedrohungen aus dem Cyberspace nehmen unaufhaltsam zu. Negativbeispiele sind in der Presse an der Tagesordnung und auch die Schweiz ist davon nicht ausgenommen. Gerade der neue Bericht von PwC zur «Operation Cloud Hopper» zeigt auf, wie sich ein Staat in einer grossen digitalen Spionageaktion Zugriff auf Daten von Firmen in 15 Ländern beschafft hat. Dabei waren auch mehrere Firmen in der Schweiz aus unterschiedlichen Industrien betroffen. Zum ersten Mal wurde nicht direkt eine einzelne Firma angegriffen, sondern der Angriff lief über den IT-Serviceprovider, bei dem die betroffenen Unternehmen ihre Informatikdienstleistungen ausgelagert hatten. Dieses Beispiel zeigt, dass die Schweiz keine Insel ist und die Unternehmen, die in der Schweiz angesiedelt sind, denselben Risiken unterliegen wie solche in anderen Ländern. Anders ist in der Schweiz aber, dass wir über die Gefahren aus dem Internet noch viel zu wenig sprechen. Die Problematik der Cyberangriffe wird auch in absehbarer Zukunft nicht abnehmen. Mit der zunehmenden Erschliessung von Schwellenländern durch das Internet werden auch die Angriffe zahlreicher, da die Cyberkriminalität für die dort lebenden Menschen oft die einzig mögliche Einnahmequelle ist und das Risiko gering ist.

Die wachsende Gefahr verlangt nach einer erhöhten Aufmerksamkeit für das Thema Cybersicherheit, allerdings muss es ganzheitlich betrachtet werden. Denn aufgrund der zunehmenden erfolgreichen Angriffe und der daraus resultierenden Veröffentlichungen von sensitiven Informationen steigen auch die regulatorischen Anforderungen auf nationaler und internationaler Ebene. Und dennoch geht speziell für den Dienstleistungsplatz Schweiz kein Weg mehr an der Digitalisierung vorbei. So ist die digitale Transformation heute nicht nur Überlebensstrategie, sondern auch Quelle von neuen Geschäftsmodellen. An digitalen Möglichkeiten für mehr Effizienz und weniger Kosten mangelt es an keiner Stelle der Wertschöpfungskette.

In diesem vielseitigen Spannungsfeld stehen Unternehmen aller Grössen und Industrien. Denn sie sammeln und pflegen Daten, seien es Kunden-, Vertriebs-, Produkt- oder Finanzdaten. Damit stehen sie vor zahlreichen neuen Herausforderungen.

Schutz von Daten und Prozessen

In den letzten Jahren haben die meisten Unternehmen eindeutig zu wenig in ihre Digitalisierung und in die Cybersicherheit investiert. Wenn sie dies nun nicht nachholen, sind die neuen Geschäftsmodelle, die finanziellen Einsparungen und die Erhöhung der Arbeitseffizienz, die die Digitalisierung mit sich bringt, auf Sand gebaut. Was aber genau gemacht werden sollte, ist für viele Firmen noch unklar. Die Schweizerische Finanzmarktaufsicht (FINMA) hat 2016 ein Rundschreiben publiziert, welches definiert, was Banken tun müssen, um sich gegen Cyberrisiken zu schützen. Die Grundsätze sind vollumfänglich auch auf andere Bereiche anwendbar. Die nachfolgenden Punkte enthalten eine verallgemeinerte Zusammenfassung dieser Grundsätze.

- **Identifikation und Bewertung**

Firmen müssen Abhilfemassnahmen identifizieren, bewerten und planen, um sich auf die Bewältigung von Cybervorfällen

vorzubereiten. Insbesondere sollten sie die Einführung einer Threat-Intelligence-Lösung erwägen, die ihnen hilft, ein Risikoprofil zu erstellen und stets eine vollständige Aufstellung ihrer besonders wichtigen Systeme und Daten garantiert.

- **Schutz vor Cyberattacken**
  Die Sicherheit von Firmennetzwerken und Schnittstellen mit externen Netzen sollte durch den Einsatz von Cybersicherheitsmassnahmen verbessert werden, um sowohl einen unbefugten Abfluss von sensitiven Daten zu verhindern wie auch den sicheren und korrekten Betrieb von Geschäftsprozessen zu gewährleisten.

- **Erkennung von Cyberattacken**
  Firmen müssen ihre Überwachungsansätze so verbessern, dass es ihnen möglich ist, jegliches unbefugte Eindringen in ihr internes Netzwerk zu erkennen und zu blockieren, Unregelmässigkeiten bei den Datenflüssen innerhalb des Netzwerks zu bemerken sowie effektiv mit Sicherheitswarnungen umzugehen.

- **Reaktion auf Cyberattacken**
  Prozesse, Personen und Instrumente, die für die Reaktion auf eine Cyberattacke notwendig sind, müssen definiert sein. Firmen sollten auch ihre Massnahmenpläne und die gesamte Kommunikation mit internen oder externen Interessenvertretern formalisieren und die Zusammenarbeit mit einem spezialisierten Cybersicherheitspartner, der bei der Reaktion auf Cyberattacken gesamtheitlich mit Spezialisten unterstützen kann, vertraglich regeln.

- **Wiederherstellen des Betriebs**
  Um zu garantieren, dass die Verfügbarkeit und die Integrität der Systeme sowie korrumpierte oder verloren gegangene Daten nach einer Cyberattacke wiederhergestellt werden können, müssen die erforderlichen Massnahmen definiert werden.

Unterstützung bei der Umsetzung

Nur wenige Unternehmen schaffen die digitale Transformation und das Sichern der digitalen Geschäftsprozesse vollständig aus eigenen Kräften. Das Know-how dafür ist intern meist nicht vorhanden, und selbst grössere Firmen können oft nicht genügend Cybersecurity-Spezialisten einstellen. Entsprechend werden auch in der Cybersicherheit immer häufiger sogenannte Managed Services eingesetzt. Dabei werden Sicherheitsleistungen nicht mehr nur in Form von Technologie und Beratung, sondern direkt als Service eingekauft. Dies entspricht sowohl dem Grundsatz der Reduktion von Investitionskosten wie auch der Technologieentwicklung. Denn dank des Wissens von Cyberexperten und dank durchdachter Lösungen kann ein Unternehmen die Dynamik der digitalen Transformation mitmachen und diese als Chance wahrnehmen, ohne durch die Cyberrisiken gebremst zu werden.

Zusätzlich zum Einsatz von Managed Security Services können viele Sicherheitsbedürfnisse auch mit modernen Cloudlösungen abgedeckt werden. Die Diskussion um die Sicherheit von solchen Cloudservices hält schon lange an, aber oft werden dort zwei Themen vermischt. Betrachtet man die Sicherheitsvorkehrungen eines professionellen grossen Cloudanbieters objektiv, so sind diese signifikant höher als bei firmeninternen Lösungen. Entsprechend gewinnt ein Unternehmen für die meisten Szenarien an Sicherheit, wenn es seine Daten in die Cloud verlagert. Dabei neu aufkommende Herausforderungen sind aber die Compliance und der Datenschutz, da grosse Cloudanbieter die Daten nicht in der Schweiz speichern. Diese Themen müssen gründlich überlegt, klar geregelt und die Cloudlösung entsprechend implementiert werden. Das gelingt in den meisten Fällen mit einem überschaubaren Aufwand. So wird ein Unternehmen mit der Cloud an Sicherheit gewinnen und die eigenen technischen Sicherheitsrisiken senken.

Fazit

Für Unternehmen wird es immer entscheidender, hauseigene Daten und Plattformen zu schützen, damit sie von den positiven Effekten der Digitalisierung profitieren können. Wenn sie den Übertritt in die digitale Welt mit den richtigen Sicherheitsvorkehrungen vollziehen und sich den neuen Herausforderungen stellen, gewinnen sie auch an Glaubwürdigkeit und Vertrauen ihren Kunden gegenüber.

Reto Häni
ist Partner bei PwC Schweiz sowie Mitglied des Führungsteams von PwC Digital Services. Er leitet den Bereich Cybersecurity, eine multidisziplinäre Gruppe von Spezialisten auf den Gebieten Cybersicherheit, Technologierisiko, Forensik und Datenschutz. Häni verfügt über mehr als 17 Jahre Erfahrung in der Informations- und Telekommunikationstechnik (IKT) mit den Schwerpunkten Informatikstrategie und -steuerung, Cyber- und Infrastruktursicherheit, Risikomanagement, Identity & Access Management, Cloud Services und Datenschutz. Zudem hat er Führungserfahrung im kommerziellen sowie im öffentlichen Sektor auf lokaler, regionaler und globaler Ebene. Bevor er PwC beitrat, war er unter anderem als Chief Security Officer von Microsoft verantwortlich für Westeuropa und vorher als CIO des Departements Verteidigung, Bevölkerungsschutz und Sport tätig.

Den Hackern auf der Spur – im Auftrag von Unternehmen

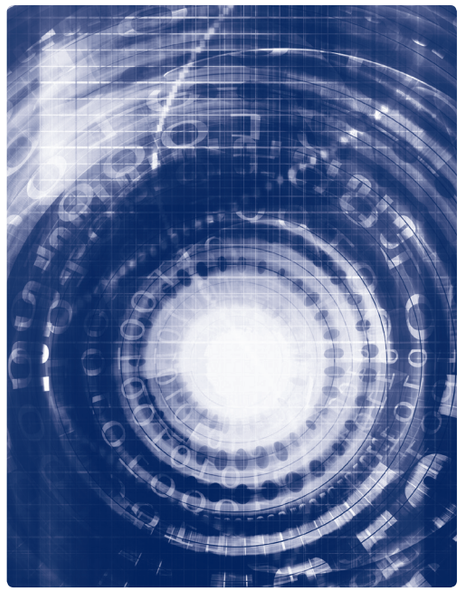
Dr. Helmut Mahler
Gesellschafter Code White
helmut.mahler@code-white.com

Computer haben heute fast jeden Bereich der Geschäftswelt, der Gesellschaft und des Privatlebens erobert. Gründe dafür sind die unglaubliche Leistungsfähigkeit, die hohe Benutzerfreundlichkeit und leichte Vernetzbarkeit sowie die enorme Vielfalt von Einsatzmöglichkeiten. Überall auf der Welt nutzen Menschen Computer – ob als Smartphone beim Surfen in den sozialen Netzwerken, als Laptop im Büro oder in einem Roboter in der Produktion. Der vorliegende Beitrag vermittelt einen kurzen Einblick in die Techniken möglicher Angreifer auf diese Welt der Computer, um das Verständnis für Risiken zu schärfen und Abwehrmassnahmen aufzuzeigen.

So genannte «Hacker» sind in der Regel hochspezialisierte Computerfachleute. Sie zeichnen sich durch exzellentes Fachwissen, hohe Kreativität und ausgeprägte analytische Fähigkeiten aus. Sie beherrschen die Funktionsweise von Computern im Detail und kennen deren Unzulänglichkeiten oder Fehlfunktionen. Hacker sind untereinander hochgradig vernetzt; ihr Ziel ist es, Schwachstellen in Computersystemen aufzuspüren und diese für die eigenen Zwecke zu missbrauchen. Als technische Voraussetzung genügen dafür in der Regel ein einfacher Computer und ein Zugang zum Internet. Das Risiko, bei einem Angriff aus dem Netz entdeckt zu werden, ist gering, da ein Hacker aus der Distanz über das Internet angreifen und seine Identität sehr einfach und wirksam verschleiern kann. Die Chancen, die sich durch den Missbrauch fremder Computer ergeben, sind dagegen beliebig hoch. Dies macht Angriffe aus dem Cyberspace derart attraktiv, dass mittlerweile eine regelrechte Industrie entstanden ist, die illegal Angriffe und Missbrauch von Computern als Dienstleistung oder durch Missbrauch erlangte Informationen auf dunklen Märkten zum Kauf anbietet.

Suche nach Eingangstoren

In der Regel erfasst der Angreifer zunächst mit Hilfe gängiger Suchmaschinen akribisch alle Websites des Zielsystems. In mühsamer Kleinarbeit wird jede einzelne Website daraufhin untersucht, ob sie sich für einen Angriff eignet. Dies ist zum Beispiel der Fall, wenn zur Authentifizierung ein Benutzername erforderlich ist und es möglich ist, die Eingabe beliebig oft zu wiederholen, selbst wenn die Eingabe nicht korrekt ist. Dann kann der Angreifer spezielle Programme einsetzen, die automatisch gängige Benutzernamen und Passwörter so lange ausprobieren, bis eine Kombination von der Website akzeptiert wird. Sind Benutzername und Passwort auf diese Weise identifiziert, hat der Angreifer Zugang erlangt. Noch einfacher kann ein erster Zugang zum Zielsystem gelingen, wenn es dieses zulässt, dass anstatt eines Namens, einer Adresse oder eines Passworts auf einer Website ein Computerbefehl eingegeben und ausgeführt werden kann. Auch auf diesem Weg verschafft sich der Angreifer Zugang auf das Zielsystem. Moderne Websites mögen unter strengen Sicherheitsrichtlinien entwickelt worden sein, die das geschilderte Vorgehen möglicherweise blockieren. Doch wer garantiert, dass all die Internetauftritte aus den zurückliegenden Jahren, die vielleicht noch ohne strikte Vorschriften entwickelt worden sind, ebenfalls ausreichend abgesichert sind? Genau diese Systeme mit solchen Unzulänglichkeiten sucht ein Angreifer.



Erweiterung der Zugriffsrechte

Hat sich der Angreifer erst einmal Zugang verschafft, versucht er seine Rechte im Zielsystem zu erweitern. Dabei verwendet er Programme, die bekannte Unzulänglichkeiten in Systemen ausnützen. Ist also auf dem Zielsystem nicht die aktuelle und bereinigte Version einer Software installiert, stehen die Chancen gut, dass sich der Angreifer unrechtmässig so lange weitergehende Rechte zuweisen kann, bis er die vollständige Kontrolle über das Zielsystem erreicht hat. Neben dem rein technischen Angriff über Unzulänglichkeiten in den Systemen erfolgen Angriffe zudem gerne über Mitarbeiter, die zu Fehlverhalten verleitet werden. So wird zum Beispiel versucht, Mitarbeiter über fingierte E-Mails zu veranlassen, Passwörter preiszugeben oder infizierte Software zu laden, die vom Hacker programmierte Schadsoftware enthält und die Kontrolle über den vom Mitarbeiter verwendeten Computer ermöglicht. Ist das Zielsystem einmal unter Kontrolle, ist der Weg frei zum Missbrauch: Daten können gezielt manipuliert oder vertrauliche Daten entwendet werden, Anwendern der Zugriff zum System verweigert werden oder über E-Mailadressen des Kaders unrechtmässig Anweisungen an Mitarbeiter erteilt werden.

Abwehrmassnahmen ...
Die dargestellten Praktiken sind hier sehr vereinfacht und nur exemplarisch dargestellt, führen in der Praxis jedoch oft zum Erfolg. Es ist davon auszugehen, dass heute schon jeder Computernutzer, ob im Unternehmen, in der Behörde oder im privaten Bereich, mit einem Angriff aus dem Cyberspace konfrontiert war. Durch die zunehmende Vernetzung im Rahmen der Industrie 4.0 ist davon auszugehen, dass die Gefahr in Zukunft eher noch zunimmt. Jeder Anwender muss sich über die eigene Angriffsoberfläche und über die Schutzwürdigkeit von Informationen im Klaren sein und wirksame Abwehrmassnahmen ergreifen. Dazu gehören zum Beispiel die verbindliche Einhaltung von Passwortrichtlinien, der Einsatz von leistungsfähigen Programmen zum Erkennen von Schadsoftware und Firewalls oder die Sicherstellung, dass immer nur die aktuellen Versionen der eingesetzten Software zum Einsatz kommen.

... intern und extern
Die Erfahrung zeigt, dass es offensichtlich nicht ausreicht, dass Anwender gegenüber den Gefahren aus dem Cyberspace immer wieder lediglich sensibilisiert werden. Vielmehr müssen sie regelmässig und intensiv geschult und auf die Einhaltung der Sicherheitsrichtlinien verpflichtet werden. All diese Massnahmen sind wichtige Voraussetzungen für einen ausreichenden Schutz. Sie decken aber nur den Blick von innen nach aussen ab (Compliance Driven Security). Offen bleibt meist die Nagelprobe – der Test also, ob qualifizierte Angreifer tatsächlich wirksam abgewehrt werden können. Hier kommen sogenannte Penetrationstests zum Einsatz. Spezialisierte Unternehmen testen unter klaren Vorgaben, was und wie getestet werden soll, die Sicherheit von Computersystemen und Netzwerken. Ein anderer umfassender und realitätsnaher Ansatz ist der, den das Beratungsunternehmen Code White unter dem Titel «Intelligence Driven Security» verfolgt. Wie bei einem echten Angriff aus dem Cyberspace ermitteln hochkarätige Experten die Verwundbarkeit von Computersystemen und Netzwerken. Ohne Informationen und Vorgaben von Seiten des Auftraggebers wird realitätsnah versucht, Eingangstore im Computersystem des Kunden zu identifizieren und über diese in das Zielsystem einzudringen und sich sukzessiv Rechte zu verschaffen mit dem Ziel, die vollständige Kontrolle über die Computer des Auftraggebers zu übernehmen. Die identifizierten Schwachstellen und die gewählte Vorgehensweise werden dabei akribisch dokumentiert, sodass der Auftraggeber danach problemlos in der Lage ist, den Angriff im Detail nachzuvollziehen und Gegenmassnahmen schnell und wirksam einleiten zu können.

Erfahrungen zeigen, dass durch die Kombination aus Compliance Driven Security und Intelligence Driven Security die Verwundbarkeit von Computern wirksam gesenkt und das Sicherheitsniveau deutlich verbessert werden kann. Eine Garantie für eine vollständige Sicherheit gegenüber Angriffen aus dem Cyberspace kann es allerdings nicht geben. Vielleicht können aber die Hürden so mühsam zu überwinden sein, dass ein Hacker den Angriff abbricht und sich dafür ein anderes, einfacheres Ziel sucht.

Dr. Helmut Mahler
ist Gründer und Mehrheitsgesellschafter der Firma Code White. Er war Wissenschaftler im Post Doctoral Fellowship Program am IBM Forschungslaboratorium Zürich in Rüschlikon und in verschiedenen Positionen im IT-Management bei Daimler beschäftigt. Zuletzt war er dort als Vice President und CIO für das internationale Nutzfahrzeuggeschäft verantwortlich, bis er vor drei Jahren die Firma Code White gründete. Code White hat den Sitz in Ulm, Deutschland, und wurde als Startup von zwei Teilhabern der damaligen Bank La Roche mitgegründet.

Prävention schützt vor Online-Kriminalität

Dr. iur. Jascha Schneider-Marfels
Advokat für Medien- und Wirtschaftsrecht
schneider@lexpartners.ch

Hacking, Phishing, Identitätsdiebstahl und andere Formen von Online-Betrug geistern als Schreckgespenst durch die Cyber-Stuben. Dessen ungeachtet nimmt die Zahl der Finanzgeschäfte zu, die online abgeschlossen werden, wie E-Banking oder Online-Handel. Die Industrie reagiert mit Sicherheitsupdates, errichtet Firewalls und suggeriert wirksamen Schutz vor digitalen Attacken. Versicherer bieten Versicherungen gegen Datenverlust und Cyber-Angriffe an. Dennoch verbleibt ein nicht unerhebliches Restrisiko. Welcher Schutz ist wirkungsvoll? Wie ist die Rechtslage? Wie sollen sich Betroffene verhalten?

Zunächst gilt es, sich einen Überblick über die Formen von Cyber-Kriminalität zu verschaffen. In erster Linie handelt es sich dabei um Angriffe auf Privatpersonen und Firmen, welche zumindest teilweise über das Internet verübt werden. Die Täter verfolgen in der Regel unterschiedliche Motive. Im Vordergrund steht die finanzielle Bereicherung, zum Beispiel durch einen Online-Betrug (exemplarisch Bundesstrafgericht, BG.2016.23). Aus der Praxis bekannt sind aber auch die blosse Schädigungsabsicht, wie der sogenannte «Identitätsdiebstahl», bei dem der Täter in so genannten Sozialen Medien im Namen des Opfers rufschädigende Einträge verbreitet. Bekannt sind auch Attacken von Geheimdiensten oder Organisationen auf Länder oder andere Organisationen, was jedoch eher als Terrorismus, Sabotage oder Spionage zu qualifizieren ist und hier nicht weiter thematisiert werden soll.

Darüber hinaus darf nicht unterschätzt werden, dass Hacking auch als Hobby betrieben wird. Das Überlisten fremder Schutzmechanismen und das damit verbundene Eindringen in fremde Systeme verschafft Nervenkitzel, Anerkennung und persönliche Befriedigung, wie das jüngst bekannt gewordene Beispiel junger russischer Hacker zeigt. Diese drangen in die Haussteuerung privater Haushalte ein, um mitten in der Nacht im Haus ein Lichtspektakel zu veranstalten oder den Whirlpool auf maximaler Stärke einzuschalten – zum Schrecken der schlafenden Bewohner.

Hacking und Datendiebstahl

Oftmals werden die Begriffe für diese Verhaltensweisen uneinheitlich verwendet oder nicht klar abgegrenzt. Beim blossen «Hacking» handelt es sich um ein unbefugtes Eindringen in ein fremdes Datenverarbeitungssystem, was durchaus auch als digitaler Hausfriedensbruch bezeichnet werden kann. Der Täter verschafft sich unbefugterweise Zugriff auf einen Computer, einen Laptop, ein Smartphone oder einen Server. Hat er dabei keine Bereicherungsabsicht, wie im Fall der erwähnten russischen Hacker, droht ihm gemäss Art. 143bis StGB eine Freiheitsstrafe bis zu drei Jahren oder eine Geldstrafe. Beschafft sich der Täter indes nicht für ihn bestimmte Daten, um sich oder einen anderen dadurch zu bereichern, spricht man von «Datendiebstahl» (Art. 143 StGB). Daneben kennt das Strafgesetzbuch mit Art. 144bis StGB die der klassischen Sachbeschädigung nachempfundene «Datenbeschädigung» als besonderes Computerdelikt. Der Täter dringt beispielsweise in die EDV eines Konkurrenzunternehmens ein und löscht dessen Kundenliste, um den Mitbewerber zu schwächen. Unter diesen Tatbestand fällt auch die Programmierung von «Viren» oder sogenannter «Malware»; darunter versteht man versteckte Programme, die von Computern verbreitet werden und Schäden und Störungen verursachen.

Phishing und Social Engeneering

Die Art und Weise, wie diese Delikte verübt werden, ist vielfältig und, oftmals findet eine Kombination verschiedener Tatbestandselemente statt, welche am Ende zusammengefasst als Internet-Betrug bezeichnet werden (exemplarisch BGE 6B_150/2016 vom 28. Juni 2016). Zwei Formen seien besonders hervorgehoben: Beim «Phishing» versucht der Täter über gefälschte Internetseiten, E-Mails oder

Kurznachrichten an vertrauliche Daten zu gelangen. Der Täter versendet zum Beispiel an potenzielle Bankkunden eine E-Mail, welche vom Absender her und der optischen Gestaltung einer offiziellen E-Mail ihrer Bank entspricht. Darin werden die Opfer aufgefordert, einen Link anzuklicken und aus technischen Gründen unter Angabe ihres Usernamens ihr Passwort zu erneuern. Dabei landen die Betroffenen nicht auf einem Server ihrer Bank, sondern einer Webseite des Täters, welcher auf diese Weise in den Besitz von Bankdaten gelangt (vgl. allgemein: Bachmann Adrian, «Phishing» nach Zugangsdaten der Kundendaten von Onlineportalen, Diss. Zürich 2015). Beim sog. «Social Engineering» zielt der Täter auf gutgläubige und hilfsbereite Mitarbeiter eines Unternehmens ab, indem er sich zum Beispiel am Telefon als Systemadministrator ausgibt und nach E-Mail-Daten, wie Benutzer-

namen und Passwörter fragt. Dabei ist es seine Intention, an einen allfälligen E-Mail-Verkehr zwischen den Opfern und ihrer Bank zu gelangen. Dies ermöglicht ihm, Einblick in die bisherige Korrespondenz mit dem Kreditinstitut zu erlangen und sich allenfalls gegenüber der Bank als Kunde auszugeben, um Überweisungen auf sein Konto veranlassen zu können (Portmann Armand, Phishing: Mitarbeiter auf dem Prüfstand, in digma 2016, S. 30 ff.).

Täter im Vorteil

Wie bereits dargelegt, stehen diese Verhaltensweisen allesamt unter Strafe, wobei neben den erwähnten Computerdelikten freilich auch die allgemeinen Strafbestimmungen wie zum Beispiel Betrug (Art. 146 StGB) und Geldwäscherei (Art. 305bis StGB) zur Anwendung gelangen (vgl. auch Bundesstrafgericht BG.2016.26 vom 27. Oktober 2016). Strafrechtlich relevante Handlungen stellen grundsätzlich eine Anspruchsgrundlage für zivilrechtliche Ansprüche nach Art. 41 OR dar. Die Hauptproblematik besteht jedoch darin, dass die Täter ihren Opfern und den Untersuchungsbehörden oftmals einen Schritt voraus sind, was ihnen das Verwischen von Spuren im Netz ermöglicht. Nicht selten erfolgen derartige Angriffe aus dem Ausland und sind nur schwer zurückzuverfolgen, weil die Täter eine weltumspannende Serverkette eingerichtet haben, welche es nahezu unmöglich macht, sie zu lokalisieren (vgl. auch: «Wir brauchen höhere Strafen» – Bundesanwalt Lauber über den Kampf gegen die Mafia, den Terrorismus – und Probleme im eigenen Haus», in: NZZ Nr. 276 vom 25. November 2016, S. 13).

Opfer im Nachteil

Darüber hinaus dauert es oftmals einige Stunden bis Tage, bis die Betroffenen realisieren, Opfer einer Cyber-Attacke geworden zu sein; Zeit, die dem Täter ausreicht, das rechtswidrig erlangte Geld von einer Bank zur anderen zu verschieben, anonym im Darknet oder in Bitcoins umzuwechseln oder von einer Tarnfirma zur anderen zu verschieben. Die Möglichkeit, über eine Geldwäschereimeldung international Konten zu sperren, verkommt unter diesen Umständen zur Farce. Hinzu kommt, dass es oftmals Monate dauert, bis hiesige Strafverfolgungsbehörden die Serverdaten von Behörden aus dem Ausland erhalten. Es muss an dieser Stelle jedoch betont werden, dass die Staatsanwaltschaften in diesem Bereich zum Teil massiv in Personal und Technik investieren und die internationale Zusammenarbeit ständig ausgebaut wird. Ferner hat der Bund eine Melde- und Analysestelle Informationssicherung eingerichtet (www.melani.admin.ch; vgl. Seite 8 dieser «tribune»). Dennoch müssen die Erfolgsergebnisse oftmals als bescheiden bezeichnet werden.

Wer haftet?

Am Ende bleiben die Täter oftmals unbestraft und der Schaden ungedeckt. Nicht selten stellen sich dann Haftungsfragen, besonders beim Phishing: Hat der Kunde seine Pflichten verletzt oder haftet die Bank? Die relevanten Rechtsfragen reichen von der Zulässigkeit profaner Vertragsbestimmungen – beispielsweise einer stillschweigenden Genehmigung eines Kontoauszugs innert definierter Frist – bis hin zu komplexen Abklärungen hinsichtlich der Sorgfaltspflicht des Kunden oder des Bankinstituts. Nur wenige Kunden nehmen unter diesen Umständen das Risiko eines teuren Prozess gegen eine Bank in Kauf. Die Rechtsprechung ist entsprechend spärlich, nicht zuletzt auch deshalb, weil Banken oder Kreditkartenaussteller von sich aus den Schaden aus Kulanz decken, damit ihre digitalen Angebote nicht in Verruf geraten oder weil eine Versicherungslösung greift. In einem konkreten Fall hatte ein Kunde seine Sorgfaltspflicht verletzt, wodurch seine E-Mail-Daten in unbefugte Hände gerieten, was zu einer betrügerischen Transaktion führte. Das Zürcher Obergericht entschied, dass ausnahmsweise die Bank für den Schaden hafte, weil sie die vertraglich vereinbarte Limite für E-Mail-Zahlungsaufträge überschritten hatte, ohne weitere Sicherheitsabklärungen vorzunehmen (vgl. Bubb Lukas, Wenn der Bankkunde zum Risiko wird: Können Phishing-Attacken versichert werden?, in: HAVE 2016, S. 190 ff.).

Prävention ist wichtig

Aus diesen Ausführungen wird deutlich: Prävention, das heisst die Wahrung und Vorkehrung von Vorsichtsmassnahmen, stellt nach wie vor den besten Schutz vor Cyber-Angriffen dar (vgl. von Ow Andreas, Konzepte gegen Cyberspace-Angriffe, in: digma 2015, S. 86). Ebenso wichtig ist eine Schulung des Personals sowie ein gesundes Mass an Skepsis gegenüber ungewöhnlichen Anfragen. Generell gilt: Banken, Kreditkartenfirmen oder Systemadministratoren fragen niemals telefonisch Benutzerdaten oder Passwörter ab. Ebenso wenig verschicken Banken unaufgefordert Links auf Internetseiten, welche die Eingabe solcher Daten verlangt. Ist dennoch ein Cyber-Angriff erfolgt, gilt es, möglichst rasch die Untersuchungsbehörden einzuschalten und die betroffenen Unternehmen zu informieren. Durchaus in Erwägung zu ziehen ist auch der Abschluss einer entsprechenden Versicherung.

Dr. iur. Jascha Schneider-Marfels
ist seit 2005 als Advokat u. a. auf dem Spezialgebiet Medienrecht tätig. Seine Dissertation war über Rundfunkrecht; 2008 bis 2012 war er Dozent für Medienrecht und Medienethik PHZ/MAZ und Dozent für Wirtschaftsstrafrecht an der Schweizerischen Treuhänder Schule (STS). Seit 2015 ist er zudem Lehrbeauftragter an der Universität Basel (Lehrstuhl Prof. Klaus Neumann-Braun).

MELANI – gegen Hacker und Betrug

Mit dem Schutz kritischer Infrastrukturen und der Sensibilisierung der Bevölkerung in der Schweiz gegenüber Angriffen aus dem Internet hat der Bundesrat die Melde- und Analysestelle Informationssicherung beauftragt.

Seit dem 1. Oktober 2014 ist die Melde- und Analysestelle Informationssicherung MELANI als Organisation der Bundesverwaltung der Schweiz operativ tätig. Der Bundesrat hat die Stelle geschaffen, um den Auftrag der Bundesverfassung bezüglich Erhaltung der Wohlfahrt des Landes auch im Internetzeitalter erfüllen zu können. Dementsprechend ist MELANI von der Landesregierung mit der Früherkennung von Gefahren und deren Bewältigung sowie der Unterstützung der Betreiber von kritischen Infrastrukturen in der Krise beauftragt worden. MELANI funktioniert als Kooperationsmodell zwischen dem Eidgenössischen Finanzdepartement (EFD), vertreten durch das Informatiksteuerungsorgan des Bundes (ISB) und dem Eidgenössischen Departement für Verteidigung, Bevölkerungsschutz und Sport (VBS), seinerseits vertreten durch den Nachrichtendienst des Bundes (NDB).

Wer sind die Kunden von MELANI?
MELANI bedient zwei Kundengruppen: Einen offenen und einen geschlossenen Kreis.

Der offene Kundenkreis umfasst private Computerbenützer sowie kleine und mittlere Unternehmen (KMU). Zu ihrem Schutz bietet MELANI:

- Informationen über Gefahren und Massnahmen im Umgang mit modernen Informations- und Kommunikationstechnologien (beispielsweise Internet, E-Banking).
- Berichte, welche die wichtigsten Tendenzen und Entwicklungen rund um Vorfälle und Geschehnisse in der Informations- und Kommunikationstechnologie erläutern (Factsheets, Halbjahresberichte).
- Ein Meldeformular, um Vorfälle zu melden.

Zum geschlossenen Kundenkreis gehören ausgewählte Betreiber von nationalen kritischen Infrastrukturen in der Schweiz (Energieversorger, Telekommunikationsunternehmen, Banken etc.). Hier besteht die Aufgabe von MELANI darin, diese kritischen Infrastrukturen zu schützen, insbesondere dort, wo diese vom Funktionieren der Informations- und Kommunikationsinfrastrukturen abhängig sind. Ziel ist, dass Netz- und Systemunterbrechungen sowie Missbräuche selten, von kurzer Dauer, beherrschbar und von geringem Schadensausmass sind. Betreiber kritischer Infrastrukturen können diesem geschlossenen Kundenkreis beitreten und verfügen so über Informationen, die für die Allgemeinheit nicht zugänglich sind.

Was tut MELANI sonst noch?
Die Stelle liefert Lageberichte, in Vergangenheit zum Beispiel anlässlich der UEFA Euro 2008, der Eishockey-Weltmeisterschaft 2009 oder des Weltwirtschaftsforums WEF in Davos. MELANI informiert zudem die Öffentlichkeit bei grösseren Vorfällen mittels eines Newsletters und stellt auf der Website eine Reihe von Tools und Anleitungen zum Schutz der privaten Computer an. Ausserdem wurde MELANI mit der Umsetzung der «Nationalen Strategie zum Schutz der Schweiz vor Cyber-Risiken» (Nationale Cyber-Strategie; NCS) beauftragt.

Wie ist MELANI organisiert?
Der strategische Teil von MELANI gehört zum Eidg. Finanzdepartement EFD und ist Teil des Informatiksteuerungsorgans Bund ISB. Bei MELANI arbeiten verschiedene Partner aus Verwaltung und Wirtschaft zusammen. Das Operation Information Center OIC, der operative Teil von MELANI, gehört zum Eidg. Departement für Verteidigung, Bevölkerungsschutz und Sport (VBS).

Quelle/weitere Informationen:
www.melani.admin.ch/melani/de/home

IMPRESSUM Nummer 2/2017, erscheint viermal jährlich.

HERAUSGEBER: Handelskammer beider Basel (info@hkbb.ch), Advokatenkammer Basel, Basellandschaftlicher Anwaltsverband (sekretariat@advokaturambahnhof.ch)
grosszügig unterstützt von der Jubiläumsstiftung La Roche & Co (jubilaeumsstiftung@larochebanquiers.ch)
REDAKTION: Dr. Philip R. Baumann, lic. iur. Roman Felix, Dr. iur. Alexander Filli, Dr. iur. Urs D. Gloor, lic. phil. I Jasmin Fürstenberger, MLaw Andrea Tarnutzer-Münch, lic. phil. I Roger Thiriet
LAYOUT: Elmar Wozilka, Handelskammer beider Basel, Druck: bc medien ag, Münchenstein
ADRESSE: «tribune», St. Jakobs-Strasse 25, Postfach, 4010 Basel, Telefon: +41 61 270 60 31, Telefax: +41 61 270 60 05, E-mail: info@hkbb.ch
«tribune» ist eine offizielle Publikation der herausgebenden Organisationen für deren Mitglieder.
Der Abonnementspreis ist im Mitgliederbeitrag inbegriffen. Für Nichtmitglieder kostet das Jahresabonnement CHF 20.–.

AZB
CH-4010 Basel
P.P. / Journal

tribune