Götz Schartner

IT-Sicherheit ist **Chefsache**

Die Bedrohungslage durch Cyberrisiken in Deutschland hat sich in den vergangenen Jahren kaum verbessert. Laut Erhebungen des Branchenverbandes Bitkom sind in Deutschland rund 79 Prozent aller Unternehmen von Cyberattacken betroffen oder zumindest vermutlich betroffen. Die offiziellen Schäden belaufen sich auf etwa 51 Milliarden Euro im vergangenen Jahr, wobei die Dunkelziffer sogar noch deutlich höher liegen dürfte. Zu den am meisten gefährdeten Branchen zählt laut der Studie neben dem Automobilbau mit 68 Prozent und der Chemie- und Pharmabranche mit 66 Prozent auch die Finanz- und Versicherungswirtschaft.

Banken und Finanzdienstleister sind für Kriminelle besonders lukrative Ziele. Nicht nur das Geld, auch die Kundendaten lassen sich gewinnbringend verwerten. Das wissen auch die Sicherheitsbeauftragten und Aufsichtsbehörden wie BaFin und Bundesbank, die die technischen Mindestanforderungen entsprechend hoch angesetzt haben. In der Konsequenz sind Banken in puncto IT-Sicherheit eigentlich gut aufgestellt. Das gilt aber leider nur für die technische Seite, denn eines der größten Probleme in der Finanzbranche ist immer noch menschliches Versagen.

IT-Sicherheit hinkt der Entwicklung hinterher

Die Industrieländer befinden sich derzeit in einer Umbruchphase, in der sie ihre Geschäftsmodelle weiterentwickeln oder neue Geschäftsfelder erschließen. Auch in der Bankenbranche schreitet die Digitalisierung voran, wie die wachsende Zahl von Fintech-Unternehmen belegt. Innovation und Wettbewerbsfähigkeit sind die Schlagworte, die bei vielen Unternehmen im Vordergrund stehen. Aspekte der IT-Sicherheit stehen hinter diesen beiden Prämissen zurück und hinken den technischen Entwicklungen hinterher.

Doch dieses Spannungsfeld ist nur einer der Faktoren, die die Informationssicherheit erschweren. Software-definierte Strukturen ersetzen langsam, aber sicher die herkömmlichen Hardware-bestimmten Systeme. Dadurch lassen sich Ressourcen schnell und kostengünstig verteilen und Informationen und Daten stehen dezentral zur Verfügung. Im Gegensatz dazu steht das Bedürfnis der IT-Sicherheit, wichtige Prozesse und Systeme separat auszuführen. Auch der zunehmende Einsatz mobiler Geräte erschwert das Sicherheitsmanagement für Unternehmen. Nicht nur verlassen diese Geräte den Einflussbereich des Unternehmens, oft sind es auch private Geräte, die zum Zugriff auf Firmendaten genutzt werden. Die Abwägung zwischen der Erleichterung der Arbeitsabläufe durch mobile Geräte und dem Schutz sensibler Daten ist also eine der vorrangigen Aufgaben des IT-Sicherheitsmanagements. Zu guter Letzt stehen neuen und modernen Lösungen in vielen Fällen auch bestehende und etablierte Strukturen im Weg, denn oft sind diese neuen Systeme nicht mit den alten kompatibel.

Götz Schartner, Geschäftsführer, 8com GmbH & Co. KG, Neustadt an der Weinstraße

Das beste technische System nutzt wenig, wenn bestehende Sicherheitsstandards umgangen werden. Das kann dann passieren, wenn Kriminelle gezielt Mitarbeiter eines Unternehmens dazu verleiten, Schutzmechanismen zu umgehen oder unbewusst Schadprogramme zu installieren. Dafür werden oftmals Neugier, Respekt, Hilfsbereitschaft und Naivität der Menschen ausgenutzt. Um mehr Bewusstsein und Aufmerksamkeit für dieses Problem zu schaffen, schlägt der Autor Schulungsmaßnahmen vor, bei denen Mitarbeitern drastisch vor Augen geführt wird, wohin unvorsichtiges Verhalten im Netz führen kann. (Red.)

Welche Risiken bestehen?

Laut Angaben der von Bitkom befragten Unternehmen ist das häufigste Problem der Diebstahl von IT- und Telekommunikationsgeräten. Natürlich sind Taschendiebe, die Handys oder Tablets entwenden, nicht unbedingt hinter sensiblen Firmendaten her, trotzdem ist jeder dieser Fälle ein potenzielles Sicherheitsrisiko. Wesentlich kritischer ist das zweithäufigste Delikt zu sehen: Social Engineering. Dabei nutzen Kriminelle ganz gezielt die größte Schwachstelle der meisten Sicherheitskonzepte aus, nämlich die Mitarbeiter. Sie werden dazu verleitet, Schutzmechanismen zu umgehen oder unbewusst Schadprogramme zu installieren. Die menschliche Natur spielt ihnen dabei in die Hände. Vertrauen, Neugier, Respekt, Hilfsbereitschaft und Naivität sind Eigenschaften, die Kriminelle für ihre eigenen Zwecke ausnutzen. Über soziale Netzwerke lassen sich in den meisten Fällen Informationen finden, die dann als Köder genutzt werden können. Solche gezielten Attacken sind meist nur die erste Phase einer größeren Offensive. Man unterscheidet dabei zwischen verschiedenen Angriffsarten.

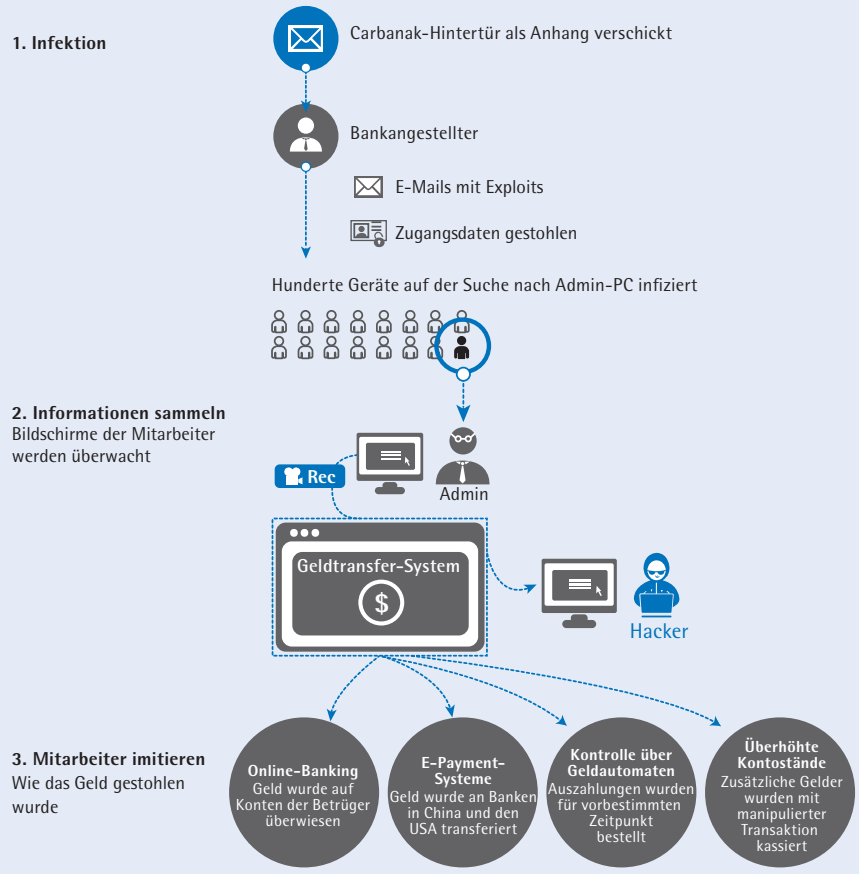
Bei Brute-Force-Angriffen werden anhand der Profildaten schlecht gewählte Passwörter erraten. Beim Social-Hacking baut der Angreifer anhand der gefundenen Profildaten ein Vertrauensverhältnis zum Opfer auf und beim Spear-Phishing-Angriff verleitet eine personalisierte E-Mail zum Öffnen eines infizierten Anhangs. Im geschäftlichen Bereich kommt außerdem immer wieder der sogenannte Fake-President-Angriff vor. Dabei wird ei-

nem Mitarbeiter vorgegaukelt, dass die Geschäftsleitung ihm ein streng vertrauliches Projekt anvertrauen möchte. Natürlich soll er mit niemandem darüber sprechen. Druck wird über eine extrem knappe Deadline für die Überweisung eines hohen Geldbetrags aufgebaut. Die Anweisungen in diesen Fällen erfolgen meist telefonisch und werden über E-Mails, vermeintlich von der Geschäftsführung, authentifiziert.

Das Bundesamt für Sicherheit in der Informationstechnik (BSI) konstatiert zum Social Engineering in seinem Bericht „Die Lage der IT-Sicherheit in Deutschland 2015": „In Anbetracht des Risikos, das durch Social Engineering entsteht, sind die Schutzmaßnahmen eher mäßig: Der Cyber-Sicherheitsumfrage 2015 des BSI zufolge führen nur 50 Prozent der befragten Unternehmen regelmäßig Sensibilisierungsmaßnahmen durch. Es mangelt in weiten Teilen an Awareness auf allen Hierarchieebenen." Diese Einschätzung können wir in der täglichen Arbeit mit Unternehmen bestätigen, sowohl was die Durchführung von Awareness-Maßnahmen als auch was den Umgang mit bereits erfolgten Angriffen betrifft.

Carbanak-Cybergang: immense Schäden

Wie die Carbanak-Cybergang 1 Milliarde Dollar gestohlen hat
Ein gezielter Angriff auf eine Bank



Quelle: 8com GmbH & Co. KG, erstellt mit Informationen von Kaspersky

Beispiel: Osteuropäische Banken im Visier

2014 richtete ein Schadprogramm unter dem Namen Carbanak weltweit immense Schäden an. Schätzungen gehen von 500 Millionen bis zu einer Milliarde US-Dollar aus. Das Besondere an dieser Attacke: Sie richtete sich gegen die bankeninternen Systeme, wodurch die Manipulation von den bestehenden Sicherheitssystemen nicht erkannt wurde, denn sie sind darauf ausgerichtet, Betrug am Endanwender aufzudecken. Die Kosten und der Aufwand hinter Carbanak waren immens, dürften sich aber angesichts der Schäden gelohnt haben.

Social Engineering als Einstieg

Social Engineering wird auch als Einstieg für gezielte Angriffe genutzt. Diese sogenannten Advanced Persistent Threat (APT)-Angriffe erfordern Zeit und finanzielle Mittel. Sie ermöglichen dem Hacker dauerhaft Zugriffsmöglichkeiten auf zentrale Bereiche des Netzwerks. Meist ist die Zeitspanne zwischen der Infektion und der Entdeckung des Schadprogramms relativ groß, im schlimmsten Fall sogar mehrere Monate. In dieser Zeit kann der Kriminelle sich ungehindert vertrauliche Daten ansehen und beträchtlichen Schaden anrichten. Wer den Verdacht hegt, dass er Opfer eines APT-Angriffs geworden ist, sollte sich schnellstmöglich einen Fachmann für IT-Forensik ins Boot holen. Er kann feststellen, wie hoch der Schaden ist, welche Bereiche infiziert sind und bei der Täterermittlung und der Bereinigung des Netzwerks helfen.

Neben diesen Angriffsarten gibt es von Spam-E-Mails über Botnetze und Distributed-Denial-of-Service-(DDoS)-Angriffe bis hin zu Drive-by-Exploits und Identitätsdiebstahl unzählige Möglichkeiten, mit denen kriminelle Hacker sich Zugriff auf Daten verschaffen – und ständig kommen neue Varianten hinzu. Mangelnde Kreativität kann man den Hackern jedenfalls nicht vorwerfen!

Mitarbeiter sind größte Gefahrenquelle

Um ein sinnvolles Sicherheitskonzept zu erarbeiten, ist die Kenntnis der Schwachstellen eines Systems und der größten Gefahrenquellen essenziell. Auch hier offenbart die Bitkom-Studie eine interessante, aber auch erschreckende Tatsache: Mit 52 Prozent sind aktuelle und ehemalige Mitarbeiter der Haupttäterkreis. Hierbei handelt es sich jedoch nur in den seltensten Fällen um eine bewusste Entscheidung, dem Arbeitgeber zu schaden. Vielmehr nutzen Kriminelle die Naivität und das Unwissen vieler Mitarbeiter, um sich Zugang zu verschaffen. Organisierte Kriminalität und Geheimdienste machen mit elf und

drei Prozent hingegen nur einen deutlich geringeren Anteil der Angriffe aus.

Wie das Beispiel Carbanak zeigt, ist das Haupteinfallstor für Hacker immer noch der Mensch. Während gerade die sogenannten Kritis-Branchen, zu denen auch der Finanz- und Versicherungssektor zählt, bereits viel für die technische Sicherung ihrer Strukturen und Daten getan haben, wird der Faktor Mensch vielfach sträflich vernachlässigt. Doch was helfen die besten Sicherheitsmaßnahmen, wenn sie nur unzureichend umgesetzt werden? Unternehmen sollten daher ihren Fokus auch auf Awareness-Maßnahmen richten. Das Ziel sollte dabei sein, Informationssicherheit nicht nur zu predigen, sondern sie zu einem festen Bestandteil der Unternehmenskultur zu machen. Ein kleines Schockerlebnis kann dabei nur hilfreich sein.

Integration der Mitarbeiter in das Sicherheitskonzept

Bevor die Mitarbeiter also überhaupt wissen, dass eine Awareness-Kampagne geplant ist, wird das aktuelle Sensibilisierungsniveau gemessen. Dazu bietet sich ein sogenanntes Social-E-Mail-Audit, eine Form von Social Engineering, an. Im Rahmen dieses Audits werden E-Mails mit manipulierten Links oder Anhängen an die Mitarbeiter eines Unternehmens verschickt und die Öffnungsraten beziehungsweise Klickzahlen anonymisiert erfasst und gemessen. Auch sogenannte Penetrationstests können Aufschluss über bestehende Sicherheitslücken geben. Dabei startet eine IT-Sicherheitsfirma eine reale Hacker-Attacke auf das Unternehmen und versucht, in die gesicherten IT-Strukturen des Auftraggebers einzudringen. So wird das System unter realen Bedingungen getestet und Schwachstellen werden aufgedeckt.

Nachdem diese erste Stufe weitgehend unbemerkt abgelaufen ist, folgt nun der Paukenschlag: Die Mitarbeiter bekommen die Auswertung des Social-E-Mail-Audits in einem Vortrag präsentiert. So sehen sie hautnah, wie angreifbar ihr Unternehmen ist. Eine weitere Möglichkeit lautet „Live-Hacking". Innerhalb von Sekunden werden vor den Augen der Mitarbeiter E-Mail-Konten oder Mobiltelefone gehackt. Es wird vorgeführt, wie Kennwörter dekodiert oder wie Informationen über Mitarbeiter aus sozialen Netzwerken zusammengeführt und für Manipulationen missbraucht werden können. Dadurch wird die Gefahr für alle Anwesenden greifbar und real. Das Schockerlebnis des Vortrags setzt die nötige Energie frei, um Informationssicherheit als gelebte Unternehmenskultur umzusetzen.

So werden die Voraussetzungen geschaffen, um eine Informationssicherheitsstrategie erfolgreich umzusetzen. Nun kommt es darauf an, diesen Schwung zu nutzen, um die nötigen Maßnahmen umzusetzen, bis sie den Mitarbeitern in Fleisch und Blut übergegangen sind.

Notfallplan vorab erstellen und implementieren

Sobald der Verdacht besteht, dass ein Unternehmen gehackt wurde oder ausgespäht wird, sollte ein Notfallplan in Kraft treten. Dafür ist es unerlässlich, dass dieser Plan bereits im Vorfeld erstellt und implementiert wird. Auch klare Verantwortlichkeiten und Zuständigkeiten sind Pflicht. Nur wenn jeder Mitarbeiter genau weiß, an wen er sich im Ernstfall wenden muss und wie er sich zu verhalten hat, kann ein Sicherheitskonzept schnell und reibungslos funktionieren.

Dazu kann es auch sinnvoll sein, die Stellung der internen IT-Sicherheitsexperten zu verbessern und direkt dem Vorstand zu unterstellen. Das BSI schlägt beispielsweise ein Managementsystem für Informationssicherheit vor, das die Zuständigkeiten und einzelnen Schritte genau vorgibt. Auch die stetige Verbesserung, Planung und Implementierung sollten Teil eines solchen Systems sein, ebenso wie eine zentrale Regelung der Installation von Updates und neuen Programmen.

Ohne Fleiß kein Preis

Es ist nicht einfach, ein Unternehmen auf ein vorbildliches Sicherheitsniveau zu heben und erfordert den Einsatz von Zeit und Herzblut. Ohne ein hohes Maß an Engagement, die richtigen Strategien und konkrete, durchführbare Handlungsvorgaben im Falle eines Sicherheitslecks kann es nicht funktionieren. Unternehmen müssen das Thema zur Chefsache erklären und es in die Unternehmenskultur integrieren – und dadurch für alle, vom kleinen Sachbearbeiter bis zur Vorstand, verbindlich machen.

Zeitschrift
für das gesamte
Kreditwesen

Verlag und Redaktion:

Verlag Fritz Knapp GmbH
Aschaffenburger Str. 19, 60599 Frankfurt,
Postfach 70 03 62, 60553 Frankfurt.

Telefon: (0 69) 97 08 33 - 0, Telefax: (0 69) 7 07 84 00
E-Mail: red.zfgk@kreditwesen.de
Internet: www.kreditwesen.de

Herausgeber: Klaus-Friedrich Otto

Chefredaktion: Dr. Berthold Morschhäuser, Philipp Otto

Redaktion: Horst Bertram (CvD), Swantje Benkelberg, Barbara Hummel, Frankfurt am Main

Redaktionssekretariat und Layout: Anja Oehrl

Die mit Namen versehenen Beiträge geben nicht immer die Meinung der Redaktion wieder. Bei unverlangt eingesandten Manuskripten ist anzugeben, ob dieser oder ein ähnlicher Beitrag bereits einer anderen Zeitschrift angeboten worden ist. Beiträge werden nur zur Alleinveröffentlichung angenommen.

Die Zeitschrift und alle in ihr enthaltenen einzelnen Beiträge und Abbildungen sind urheberrechtlich geschützt. Jede Verwertung außerhalb der engen Grenzen des Urheberrechtsgesetzes ist ohne Zustimmung des Verlags unzulässig.

Manuskripte: Mit der Annahme eines Manuskripts zur Veröffentlichung erwirbt der Verlag vom Autor das ausschließliche Verlagsrecht sowie das Recht zur Einspeicherung in eine Datenbank und zur weiteren Vervielfältigung zu gewerblichen Zwecken in jedem technisch möglichen Verfahren. Die vollständige Fassung der Redaktionsrichtlinien finden Sie unter www.kreditwesen.de.

Verlags- und Anzeigenleitung: Uwe Cappel

Anzeigenverkauf: Hans-Peter Schmitt, Tel. (0 69) 97 08 33-43

Anzeigendisposition:
Alexander Schumacher, Tel. (0 69) 97 08 33-26, sämtl. Frankfurt am Main, Aschaffenburger Str. 19.

Zurzeit ist die Anzeigenpreisliste Nr. 58 vom 1.1.2016 gültig.

Zitierweise: KREDITWESEN

Erscheinungsweise: am 1. und 15. jeden Monats.

Bezugsbedingungen: Abonnementspreise inkl. MwSt. und Versandkosten: jährlich € 582,80, bei Abonnements-Teilzahlung: 1/2-jährlich € 299,44, 1/4-jährlich € 152,64. Ausland: jährlich € 605,12. Preis des Einzelheftes € 24,00 (zuzügl. Versandkosten).

Verbundabonnement mit der Zeitschrift »bank und markt«: € 884,72, bei Abonnements-Teilzahlung: 1/2-jährlich € 465,02, 1/4-jährlich € 243,59. Ausland: jährlich € 912,08.

Studenten: 50% Ermäßigung (auf Grundpreis).

Der Bezugszeitraum gilt jeweils für ein Jahr. Er verlängert sich automatisch um ein weiteres Jahr, wenn nicht einen Monat vor Ablauf dieses Zeitraumes eine schriftliche Abbestellung vorliegt. Bestellungen direkt an den Verlag oder an den Buchhandel.

Probeheftanforderungen bitte unter Tel.: (069) 97 08 33-25.

Bei Nichterscheinen ohne Verschulden des Verlags oder infolge höherer Gewalt entfallen alle Ansprüche.

Bankverbindung: Landesbank Hessen-Thüringen Girozentrale, Frankfurt am Main, IBAN: DE73 5005 0000 0010 5550 01, BIC: HELADEFF.

Druck: Druck- und Verlagshaus Zarbock GmbH & Co. KG, Sontraer Straße 6, 60386 Frankfurt am Main.

ISSN 0341-4019