Klaus Lenssen

IT-Angriffe: Wie **sicher** ist die Finanzbranche?

Unternehmen aller Branchen sind heute permanent mit Schadprogrammen aus dem Internet konfrontiert. Dabei ist ein klarer Trend zu erkennen: Malware will möglichst lange unerkannt bleiben, um langfristig Daten auslesen oder Schaden anrichten zu können. Gleichzeitig setzen viele Firmen weiterhin keine Techniken ein, um diese versteckten Angriffe oder ihre Auswirkungen zu entdecken. Diese Situation lässt viele Unternehmen in dem Glauben, dass sich keine Schadsoftware auf ihren Systemen befindet, obwohl diese eventuell längst ihr Unwesen treibt.

Hohe Selbstsicherheit in der Finanzindustrie

Entsprechend fühlen sich IT-Sicherheitsteams deutlich sicherer als sie es in Wirklichkeit sind. Dies zeigt der Cisco Annual Security Report 2015, der in seiner neuesten Ausgabe sowohl Cybersecurity-Trends als auch die aktuelle Situation der IT-Sicherheit in Unternehmen untersucht. Demnach sind 90 Prozent der Sicherheitsverantwortlichen in Unternehmen von ihren Vorkehrungen überzeugt, doch nur 60 Prozent aktualisieren ihre Systeme regelmäßig und lediglich 10 Prozent der Internet-Explorer-Anwender nutzen die aktuellste Version der Software. Die Verantwortlichen in Deutschland liegen damit im weltweiten Durchschnitt.

Diese hohe Selbstsicherheit gilt jedoch nicht für die Finanzbranche. So haben gemäß dem Global CEO Survey 2014 der Wirtschaftsprüfungs- und Beratungsgesellschaft PwC weltweit 70 Prozent der Bankmanager Angst, dass Sicherheitslücken im unternehmenseigenen IT-System das Geschäft gefährden könnten. Diese Furcht ist nicht unbegründet, denn die Sicherheitsexperten von Kaspersky Lab erwarten, dass Cyberkriminelle in diesem Jahr verstärkt die Banken selbst gezielt angreifen, nicht mehr nur die Online-Banking-Nutzer. Dabei stehen auch Geldautomaten, virtuelle Zahlungssysteme und mit dem Internet verbundene Geräte wie Netzwerkdrucker als mögliches Einfallstor in das Unternehmen im Fokus.

Geringe Zahl von Angriffen mit schwerwiegenden Folgen

Weltweit sollten insbesondere die pharmazeutische und chemische Industrie den größten Fokus auf ihre Schutzmaßnahmen legen, denn sie sind aktuell am stärksten von Schadsoftware aus dem Internet betroffen. Noch in der ersten Hälfte des Jahres 2014 belegten Medien und Verlagswesen Rang eins, sie rutschten aber im November auf den zweiten Platz. Danach folgen die Fertigungsindustrie, Transport und Logistik sowie die Luftfahrtbranche (siehe Abbildung). Diese Wirtschaftszweige blieben das ganze Jahr 2014 hindurch die fünf am häufigsten angegriffenen Branchen weltweit.

Gerade die Finanzbranche gilt zwar als lohnenswertes Ziel, doch viele Cyberkriminelle wissen um die bereits bestehenden hohen Schutzmaßnahmen der Institute. Entsprechend verwenden sie hier in der Regel keine breit gestreuten Methoden, um über allgemeine Schadsoftware viele mögliche Einfallstore zu prüfen. Stattdessen gehen sie ganz gezielt gegen einzelne Unternehmen oder Mitarbeiter vor. Damit ist zwar die Anzahl der Angriffe vergleichsweise niedrig, doch deren Folgen umso schlimmer.

So wurde im Februar 2015 der bislang größte Online-Raubzug aufgedeckt, bei dem über 1 Milliarde US-Dollar erbeutet wurde. Davon waren bis zu 100 Geldinstitute in mehr als 20 Ländern betroffen. Die „Carbanak"-Gang war seit 2013 tätig und setzte verschiedene Methoden ein, von gezielten Phishing-Angriffen auf die Mitarbeiter bis zur Kontrolle von Überwachungskameras und Geldtransfersystemen.

Gezielte Angriffsmethoden gegen die Branchen mit dem höchsten Risiko

Die Studie hat auch ermittelt, dass die am meisten betroffenen Branchen siebenmal häufiger mittels Hilfsprogrammen zum Herunterladen von Dateien angegriffen werden als die vier Branchen mit der niedrigsten Angriffsrate. Dies ist zu erwarten, wenn gezielte Angriffsmethoden gegen die Branchen mit dem höchsten Risiko eingesetzt werden. Die Anzahl der Angriffe durch Klickbetrug und Adware (in Werbeanzeigen versteckte Schadsoftware) ist in den am häufigsten angegriffenen Branchen ebenfalls höher.

Klaus Lenssen, Senior Business Development Security, Cisco Deutschland, Düsseldorf

Weltweit sind Unternehmen Tag für Tag den Angriffen von Cyberkriminellen ausgesetzt. Die daraus entstehenden Gefahren hat gerade die Finanzbranche durchaus erkannt. Entgegen der weitverbreiteten Überzeugung in vielen Unternehmen anderer Industriezweige, sich ausreichend gegen Angriffe aus dem Internet zu schützen, gehen 70 Prozent der Bankmanager davon aus, dass Sicherheitslücken im eigenen IT-System das Geschäft gefährden können. Dabei kommt es, auch aufgrund der bereits getroffenen Sicherheitsvorkehrungen, zu relativ wenigen Angriffen auf Banken und Versicherer, die aber im Erfolgsfall immensen Schaden anrichten. Der Autor plädiert für eine umfassende Strategie im Bereich der Cybersicherheit im Gegensatz zu einem nur „scheibchenweisen" Vorgehen. (Red.)

Die Gründe für diese höheren Raten können sowohl bei den Angreifern liegen, die sich lohnenswerte Ziele aussuchen, als auch bei den Anwendern. Zum Beispiel verwenden die Nutzer verschiedener Branchen das Internet unterschiedlich. Während etwa Mitarbeiter in Verlagshäusern und Agenturen oft ausführliche Recherchen auf potenziell unbekannten Seiten durchführen, suchen Produktionsmitarbeiter meist nur Anleitungen auf Webseiten von bekannten Herstellern. Der breit gestreute Aufruf verschiedener Internetseiten erhöht naturgemäß die Gefahr, mit schädlichen Programmen in Kontakt zu treten.

Maßnahmen für hohe Sicherheit

Um sich vor diesen Gefahren zu schützen, benötigen Unternehmen heute eine umfassende Sicherheitsstrategie, die vor, während und nach einem Angriff wirken muss. Dieser bedrohungsorientierte Sicherheitsansatz setzt sich aus verschiedenen Lösungen zusammen, die zu einem einheitlichen Schutzschild für das Unternehmen ineinandergreifen müssen. Einen Bereich bildet die Absicherung von Endgeräten, die entweder mit einem geschützten Netzwerk oder mit dem Internet verbunden sind. Dies geschieht mithilfe durchgängiger und integrierter Erkennungs- und Blockierungsfunktionen im Rahmen von Advanced Malware Protection (AMP).

Diese ist mit Netzwerksicherheit der nächsten Generation zu ergänzen. Dazu gehören Next Generation Firewalls und Intrusion Prevention, AMP für Netzwerke, Security Intelligence sowie ein Management Center. Moderne Sicherheitslösungen für das Rechenzentrum ermöglichen den Wechsel von herkömmlichen zu virtuellen Umgebungen der nächsten Generation ohne Abstriche bei den Schutzmaßnahmen. Auch die Zugriffskontrolle und das Richtlinienmanagement sind zu berücksichtigen, um die Angriffsfläche zu verkleinern – mit umfassenden Kontextinformationen und hoher Transparenz. Zudem sollten sich Unternehmen durch Content Security-Lösungen vor zunehmenden Bedrohungen aus dem Internet oder per E-Mail schützen.

Unternehmen, die ihr aktuelles Sicherheitskonzept verifizieren möchten oder Unterstützung bei der Suche nach der geeigneten Technik für die Behebung bereits identifizierter Schwachstellen benötigen, können beispielsweise auf Security Assessment Services oder Cybersecurity Readiness Services am Markt zurückgreifen. Diese bestehen in der Regel aus zwei Teilen. Das Security Posture Assessment überprüft dabei zuerst die Sicherheitsziele und -anforderungen. Darauf basierend wird die IT-Infrastruktur proaktiv mit verschiedenen Angriffsmethoden von innen und außen getestet. Die entdeckten Schwachstellen werden anschließend analysiert und mit Security Best Practices abgeglichen. Der zweite Teil besteht aus den Security Plan and Build Services. Diese dienen zur Entwicklung und Implementierung einer umfassenden Sicherheitsstrategie.

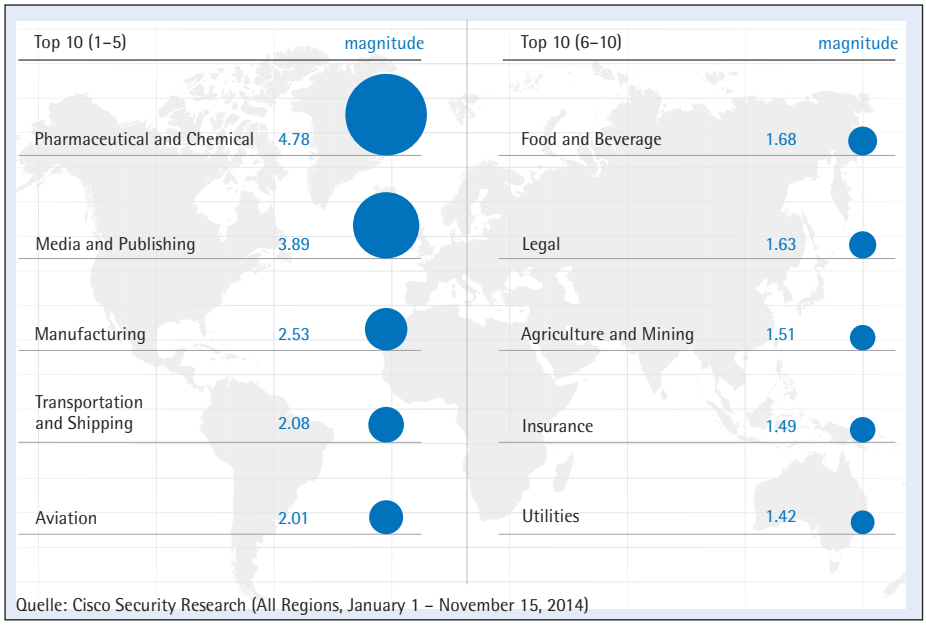
Social Engineering als Betrugsmasche

In der Finanzbranche sind die Sicherheitsstandards auch in Bezug auf die eigenen Mitarbeiter bereits sehr hoch. Trotzdem können diese unbewusst auf Betrugsversuche hereinfallen. Dies zeigt ein aktuelles Beispiel in einem Agrarmanagement-Unternehmen, das aber auf ähnliche Weise auch jederzeit in der Finanzbranche geschehen kann: Im Februar 2015 hat ein Manager des US-Unternehmens Scoular in mehreren Schritten insgesamt 17,2 Millionen US-Dollar an Betrüger auf ein chinesisches Bankkonto überwiesen. Sie hatten ihm vorgetäuscht, dass er dies im Auftrag seines Chefs für eine angebliche Firmenübernahme erledigen solle.

In der Regel funktionieren solche Angriffe über Social Engineering. Im Beispiel hatten die Betrüger dem Mitarbeiter zunächst Mails von einer neuen E-Mail-Adresse geschickt, deren angeblicher Absender sein Chef war. Da die Transaktion vertraulich wäre, solle er nur an diese Mail-Adresse schreiben und Stillschweigen bewahren. Der Mitarbeiter schöpfte keinen Verdacht, da sein Arbeitgeber tatsächlich eine Expansion nach China überlegt hatte, und überwies das Geld, ohne seinen Chef zur Sicherheit persönlich zu kontaktieren.

Über ähnliche Methoden erhalten Cyberkriminelle auch Passwörter, die ihnen Zugang zu Systemen mit Kontodaten oder persönlichen Angaben von Kunden ermöglichen, und umgehen somit die strengen Sicherheitsmaßnahmen der Banken. Einmal im System können sie meist unbemerkt auch auf weitere Anwendungen und Datenbanken zugreifen. Entsprechend müssen Banken nicht nur ihre Verbindungen nach außen schützen, sondern auch die Aktivitäten auf ihren eigenen Netzwerken. Hier müssen sie ungewöhnliche Aktivitäten erkennen und den Verlauf der schädlichen Vorgänge nachverfolgen können, um Angriffe möglichst schnell zu stoppen. Dazu ist eine vollständige Transparenz über das gesamte Netzwerk nötig – vor, während und nach einem Angriff. Nur dann lassen sich Angriffe entdecken, bevor sie größeren Schaden anrichten.

Abbildung: Die zehn weltweit am häufigsten von Web-Malware betroffenen Branchen Ende 2014



Quelle: Cisco Security Research (All Regions, January 1 – November 15, 2014)

IT-Sicherheit
Tipps und Hinweise für Schutzmaßnahmen

- Konzentration auf den Mehrwert statt auf die Kosten der Schutzmaßnahmen. Schließlich kann ein Sicherheitsvorfall zu hohen Umsatzausfällen oder teuren Rechtsstreitigkeiten mit Kunden führen.
- Eine umfassende Strategie sollte Richtlinien zur allgemeinen Nutzung der Systeme, zur Verwendung von E-Mail- und Kommunikationslösungen sowie dem Einsatz von Antivirus, Identitäten, Passwörtern, Verschlüsselungen und Remote-Zugängen besitzen.
- Angriffe können nicht nur von außen kommen. Auch die eigenen Mitarbeiter können unbewusst Sicherheitslücken erzeugen oder unzufriedene (Ex-)Kollegen absichtlich Schaden anrichten.
- Bestandsaufnahme im Unternehmen über bereits eingesetzte Firewalls, VPNs, Intrusion Prevention, Antimalware, sichere drahtlose Netzwerke, Identitäts- sowie Richtlinienmanagement.
- Umfassende Sicherheitsplanung in einem Stück: Nur eine einheitliche Strategie kann das gesamte Netzwerk schützen, sie lässt sich aber Schritt für Schritt einführen.
- Identifikation der wichtigsten digitalen Informationen: Wo diese liegen und wer nutzt sie. Dazu gehören zum Beispiel geistiges Eigentum sowie persönliche Kunden- und Mitarbeiterdaten.
- Einbindung aller Fachabteilungen, um Sicherheitsstrategien zu entwickeln und umzusetzen. Nur so lassen sich die optimalen Technologien, Trainings und Sicherheitslösungen finden.
- Betrachtung von Szenarien: Wie stark kann ein Sicherheitsvorfall die Geschäftstätigkeit beeinträchtigen? Wie hoch sind die möglichen finanziellen Verluste eines Netzwerk- oder Website-Ausfalls sowie einer Unterbrechung der Lieferkette?
- Benutzerfreundlichkeit: Wenn Sicherheitsmaßnahmen die Nutzer zu sehr einschränken, steigt die Wahrscheinlichkeit, dass sie die Sicherheitsmaßnahmen umgehen.
- Blick in die Zukunft: Wie flexibel müssen sich die Sicherheitslösungen den künftigen Geschäftsanforderungen anpassen können? Wann steht die nächste Aktualisierung von Hardware oder Software an? Werden Mitarbeiter zunehmend über Mobilgeräte oder aus dem Home Office auf die Systeme zugreifen?

Diese umfassenden Maßnahmen sind nötig, da die heutigen Angriffe meist nicht mehr reiner Vandalismus sind, sondern Attacken finanziell gut ausgestatteter, hochmotivierter krimineller Banden. Diese Profis nutzen alle Möglichkeiten des Internets, um an möglichst viel Geld zu kommen, entweder unbemerkt über einen langen Zeitraum oder durch einen zwar spektakulären, aber lohnenswerten Coup.

IT-Team stets auf dem aktuellen Stand halten

So reichen technische Lösungen alleine heute nicht mehr aus. Genauso wichtig ist eine fortwährende Weiterbildung der Mitarbeiter auf allen Ebenen. So müssen die Nutzer lernen, wie sie mögliche Schadprogramme und Social Engineering-Techniken der neuesten Generation erkennen können. Dabei helfen teilweise einfache Tipps wie das Fahren mit der Maus über einen Link, um die Adresse zu prüfen, oder keine Anhänge von unbekannten Absendern zu öffnen. Sie sollten auch wissen, wann und wie sie die Sicherheitsorganisation ihres Arbeitgebers über verdächtige Vorgänge informieren sollten.

Unternehmen müssen auch dafür sorgen, dass ihr IT-Sicherheitsteam bei Lösungen und Gefahrenlage immer auf dem aktuellen Stand bleibt. Damit steigt nicht nur die Effektivität der eingesetzten Maßnahmen, sondern auch die Motivation der Fachkräfte. Sie erwarten und benötigen eine kontinuierliche Weiterbildung und Zertifizierung mit speziellem Fokus auf die Identifizierung und Klassifizierung von Vorfällen sowie der Blockierung und Entfernung von Malware. Auch in diesem Segment gibt es externe Unterstützung, beispielsweise durch Security Incident Services oder Cyber Attack Response Services.

Bei der Durchführung der Maßnahmen müssen Sicherheits- und Geschäftsverantwortliche eng zusammenarbeiten. Denn die Ursache für viele Sicherheitsprobleme sind schwache oder fehlende Kontrollen. Entsprechend umfasst ein praxisfähiger Sicherheitsansatz die ständige Optimierung der Prozesse, basierend auf den jeweiligen Risiken. Dabei ist zu berücksichtigen, dass IT-Sicherheit zunehmend ein strategisches Business-Ziel wird. So sollten Unternehmen hoch standardisierte Geschäftsprozesse einsetzen und regelmäßig kontrollieren, ob die strategischen Ziele erreicht werden.