Der SolarWinds MSP Cyber Threat Guide

Neun Gefahren aus dem Internet und was Sie dagegen tun können

solarwinds msp


www.solarwindsmsp.com

Inhalt

Einleitung

Zu den anspruchsvollen Aufgaben der IT gehört es, Computernetzwerke vor Unbefugten zu schützen. Angriffsmethoden gibt es viele und unterschiedlich gefährliche. Mit Überreaktionen oder dem falschen technischen Ansatz verursacht man unter Umständen enorme Unkosten und erleichtert den Cyberschurken am Ende sogar noch ihr Treiben.

In diesem E-Book schildern wir neun Internetbedrohungen, denen ein Netzwerk heutzutage ausgesetzt ist, und beschreiben probate Strategien dagegen.

Der Leitfaden versteht sich als Einstiegslektüre für den Aufbau eines grundlegenden Schutz- und Abwehrkonzepts. Als IT-Experte müssen Sie sich zwei Dinge bewusst machen: Erstens, Internetkriminalität erzeugt ein beträchtliches Geschäftsrisiko. Zweitens, bisher ist leider kein Kraut dagegen gewachsen. Auch wenn mancher Anbieter das gerne behauptet: Die Technik, mit der Sie sich alles vom Leib halten können, gibt es nicht.

Immer wieder werden Cybergefahren, Malware oder Sicherheitslücken auf höchst dramatische Art in den Medien dargestellt – ohne Rücksicht auf die tatsächliche Faktenlage. Dabei sind die probaten Mittel gegen unbekannte und bekannte Gefahren im Großen und Ganzen unverändert die folgenden: Betriebssystem und Anwendungen aktuell halten und regelmäßig patchen, Administratorrechte nicht zu lax handhaben und Malware systematisch abwehren. Grundlage für diese Empfehlungen sind die Datenanalysen, die Regierungs- und Sicherheitsorganisationen weltweit seit Jahren betreiben.

Letztlich gilt: „Offense informs defense" – jeder Angriff liefert aufschlussreiche Daten für seine künftige Abwehr. Was heißt das? IT-Verantwortliche müssen die unter ihrer Obhut stehenden Netzwerke durch die Brille der Angreifer sehen lernen. Das meinen wir nicht als Aufforderung zur Entfaltung eigener krimineller Energien. Aber man kann sich zum Beispiel ein Cyberabwehrlabor einrichten und mit ein paar kostenlosen Tools Schwachstellen sondieren. So wird man peu à peu geschickter darin, den Eindringlingen das Handwerk zu legen.

Denken Sie daran: Als Fachmann oder Fachfrau für IT sind Sie für den Datenschutz, die Integrität und die Verfügbarkeit der Systeme zuständig, die man Ihnen anvertraut hat. Machen Sie den Schurken da draußen also das Leben schwer: An einem eisernen Schutzkonzept aus Erkennung, Prävention und Forensik werden sie sich die Zähne ausbeißen.

Ausspähung/Portscans

> “Zahllose böswillige Hacker schnüffeln sich auf der Suche nach Schwachstellen durch Netzwerke – mit Malware.”

Was ist das?

Zahllose böswillige Hacker schnüffeln sich auf der Suche nach Schwachstellen durch Netzwerke – mit Malware. Ein gutes Beispiel für diese Angriffsmasche ist der Wurm „The Moon“. Dieser Schädling hatte sich auf ganz bestimmten Routern von Linksys eingenistet, die eine Authentifizierungslücke aufwiesen. Von dort verbreitete er sich immer weiter. Router ohne die Lücke ließ der Wurm einfach links liegen und zog weiter zum nächsten Gerät mit besagter Schwachstelle. Gegenüber dem Internet unzureichend abgesicherte Services lassen sich mit kommerzieller Software wie Metasploit, Nessus oder aber dem kostenlosen Tool NMAP aufspüren.

Varianten:
Würmer und andere sich selbst verbreitende Schadprogramme gibt es in vielen Varianten. Einige zielen mit ganz bestimmten Exploits auf spezifische Sicherheitslücken in Software ab, etwa die erste Generation der Würmer NIMDA und Code Red. Andere versuchen, im Brute-Force-Verfahren an Kennwörter oder geschützte Systeme heranzukommen.

Ausspähung/Portscans

Was Sie unternehmen müssen

Wenn Sie es mit der Internetsicherheit ernst meinen, sollten Sie möglichst viele Services gehostet betreiben. Zum Internet hin sollten Sie außerdem möglichst wenige Ports öffnen, denn dies senkt erheblich die Gefahr, dass Spähprogramme oder Portscanner ein Schlupfloch entdecken.

Schwachstellenscans und eine kontinuierliche Überwachung der Sicherheitsumgebung per Logging werden im Rahmen bestimmter Sicherheitsstandards, etwa PCI-DSS, immer stärker gefordert. Unternehmen, die per Internet zugängliche Services oder Webanwendungen betreiben, sollten unbedingt eine Firewall mit Anwendungserkennung installieren – eine so genannte Firewall der nächsten Generation.

Sinnvoll sind auch Kennwort-Audits, die Einrichtung sicherer Standardkonfigurationen und ein Umzug der gesamten Architektur zu einem externen Hoster. Für IT-Serviceprovider bergen all diese Maßnahmen attraktive Projektchancen und können zu langfristigen Wartungsaufträgen führen.

“Einige Schädlinge zielen mit ganz bestimmten Exploits auf Sicherheitslücken in Software ab. Andere versuchen, im Brute-Force-Verfahren an Kennwörter oder geschützte Systeme heranzukommen.”

Welche Technik wirkt

Mit günstigen Standardfirewalls für den Privatgebrauch oder Geräten mit integrierten Firewall-Funktionen (wie sie ISPs in der Regel bereitstellen) lässt sich ein Unternehmen keinesfalls ausreichend schützen. Hier sind schon eher Lösungen renommierter Hersteller empfehlenswert: Watchguard, Cisco und Cisco Small Business, Sonicwall und Checkpoint sind beispielsweise gute Optionen. Beschränken Sie die Konfiguration nach Möglichkeit auf eine oder zwei Firewalls und programmieren Sie diese mit wirksamen Regeln.

Einige Schädlinge, etwa die erste Generation von NIMDA und Code Red, zielen mit ganz bestimmten Exploits auf spezifische Sicherheitslücken in Software ab.

Andere versuchen, im Brute-Force-Verfahren an Kennwörter oder geschützte Systeme heranzukommen.

Was in Ihr Sicherheits-Toolkit gehört

Externer Schwachstellenscan	MSP Risk Intelligence
SNMP-Monitoring	MSP RMM
Prüfung gescheiterter Anmeldeversuche	MSP RMM
Benutzerdefinierte Ereignisprotokollprüfung	MSP RMM
Scripting-Funktionen	MSP RMM
Hosted Services Provider	Google, Azure, Amazon
Firewall der nächsten Generation	Sophos, SonicWall, Cisco

DDoS-Angriff

> **“Mit massiven Datenströmen lassen sich Server und Netzwerke eines Unternehmens derart fluten, dass die komplette Internetkommunikation zum Erliegen kommt.”**

Was ist das?

Ende 2014 brachen die Spielenetzwerke PlayStation Network und Xbox Live unter dem Angriff des Hackerkollektivs Lizard Squad zusammen. Die Hacker hatten mit dem DDoS-Tool Lizard Stresser angegriffen. Die Software übernahm Router, die durch simple Standardkennwörter nur mangelhaft geschützt waren, und verwandelte sie in Abschussrampen für Spam auf die zentralen Internetserver der beiden Spielenetzwerke.

Mit Methoden wie NTP Amplification, DNS Reflection und SYN-Flooding lassen sich Infrastrukturen derart mit Daten fluten, dass Server und andere Ressourcen darin regelrecht in die Knie gehen. Besonders niederträchtig wird es, wenn die Angreifer unter Androhung eines DDoS-Angriffs Schutzgeldzahlungen erpressen.

Varianten:
Denial-of-Service-Angriffe gibt es schon geraume Zeit. Von der neueren Amplification-Variante abgesehen ist prinzipiell zwischen Angriffen auf Verbindungen und Angriffen auf Ressourcen zu unterscheiden. Im ersten Fall wird versucht, möglichst viele Verbindungen zum Zielserver gleichzeitig zu öffnen und diesen dadurch zu überlasten. Im zweiten Fall wird der Server einfach mit einem Request-Bombardement lahmgelegt. Noch schneller geht das, wenn die Hacker die Antwortrate herabsetzen oder durch den Versand schwer lesbarer oder nicht RFC-konformer Pakete die TCP/IP-Verbindung offen halten. Dann nämlich nimmt der Server an, dass in Kürze weitere Daten eintreffen und verhält sich so, wie wir Menschen es bei einer schlechten Telefonverbindung tun: Wir lauschen angestrengt in den Hörer und fragen immer wieder: „Hallo? Hallo, bist du noch da? Kannst du mich hören?“

Welche Technik wirkt

Gegen DDoS-Erpressung oder DDoS-Angriffe haben Sie verschiedene Optionen. Die wichtigste: Sämtliche Systeme, die unbedingt mit dem Internet verbunden sein müssen, sollten nicht im eigenen Haus, sondern in einem redundant ausgelegten Rechenzentrum mit mehreren Internetprovidern betrieben werden. Exzellente Internetverbindungen, DDoS-Schutzkonzepte und eine redundante Infrastruktur bieten beispielsweise Rackspace, Amazon, Google und Microsoft Azure. Für Unternehmen, deren Betrieb komplett vom Internet abhängig ist, bieten sich Lastausgleich über mindestens zwei ISPs und die Nutzung von DDoS-Schutzservices wie CloudFlare an.

DDoS-Angriff

Was Sie unternehmen müssen

Das A und O zur Minderung des Angriffsrisikos ist die Überwachung der Netzwerkleistung. Wie viel die Firewall gerade zu tun hat, können Sie relativ einfach schon mit SNMP-Funktionen ermitteln; auch Berichte Ihres ISP über das aktuelle Ausmaß des Datenverkehrs geben Aufschluss. Schließlich liefern Traps, das Spiegeln von Switch-Ports auf die Außenseite der Firewall und Tools wie Whiteshark, die eingehende Datenströme analysieren, weitere Hinweise darüber, was im Netzwerk gerade vor sich geht.

Der einfachste und pfiffigste Ansatz aber lautet: Fragen Sie die User! „Ist das Internet bei euch gerade langsam?" „Dauert das Sichern von Dateien in Netzwerkordnern auffällig lange?" Solche Fragen sind ein Lackmustest für die aktuelle Netzwerkleistung.

Schnell und simpel funktionieren auch das Pingen des äußeren Gateways oder eine TCP-Serviceprüfung auf exponierten Ports wie VPN. Stellen Sie hier Leistungsabfälle fest, so wissen Sie, dass bei der externen Netzwerkverbindung etwas im Busch ist. Wenn Sie dann noch steigende CPU-Lasten oder Paketraten an Ihrer Firewall registrieren, ist der Fall klar: DDoS-Alarm. Die meisten ISPs halten über Filterfunktionen aktiv nach derlei Angriffen Ausschau. Ein Anruf bei Ihrem Provider bringt im Zweifelsfall also weitere Klarheit. Abwehrstrategien bei DDoS sind komplex und erfordern dezidierte Planung, zumal die Hacker ihre Angriffe zusehends mit Lösegeldforderungen verknüpfen. Zu Ihrem ISP-Supportvertrag, den möglichen Auswirkungen von DDoS und den Abwehrmaßnahmen sollten Sie sich also schon Gedanken machen, bevor das Kind in den Brunnen gefallen ist. Auch hier gilt: Hängt Ihr Geschäftsbetrieb komplett vom Internet ab, ist eine Firewall mit DDoS-Abwehrfunktion gekoppelt mit einer DDoS-Schutzlösung über die Cloud Pflicht.

> **„Abwehrstrategien bei DDoS sind komplex und erfordern dezidierte Planung."**

Flankierende Maßnahmen sind eine gründliche und fachlich kompetente Prüfung Ihrer Netzwerkarchitektur und die Simulation von Angriffen, um das Systemverhalten zu testen. Mit einem sauberen, praxisbewährten Sicherheitsansatz für Server (insbesondere DNS-Server – nicht als offene Resolver betrieben) lässt sich Missbrauch und Manipulation im Rahmen eines Proxy- oder Amplification-Angriffs vorbeugen. Firewalls, Router, Edge Switches und Server sollten stets ordentlich gepatcht sein. Das kleinste Versehen macht hier Ihr Netzwerk angreifbar. Im schlimmsten Fall wird es zum Kombattanten wider Willen in einem DDoS-Angriff gegen andere Netzwerke.

Was inIhr Sicherheits-Toolkit gehört

Patch-Management für Server, auf denen Dienste gehostet sind	MSP RMM
SNMP-Monitoring der Router-, Firewall- und Switch-Infrastruktur	MSP RMM
Redundante Internetverbindungen, gehostete DDoS-Services	CloudFlare
Lösung für die Paketanalyse/-inspektion	WireShark, NetFlow, Observium
Firewall der nächsten Generation mit DDoS-Schutz	Sophos, SonicWall, Cisco
E-Mail-Schutz	MSP RMM / MSP Mail

Brute-Force-Angriff

> **“Mit Gewalt werden alle theoretisch möglichen Kennwörter solange durchprobiert, bis das richtige gefunden ist.”**

Was ist das?

*Brut*e-Force-Angriffe zielen auf einzelne gegenüber dem Internet exponierte Geräte ab: Remote-Desktops, Fernwartungstools wie VNC, die Outlook Web App, SMTP-Services und Ähnliches. Entweder werden dabei Schädlinge eingeschleust, die sich weiter verbreiten, oder aktiv Skripte ausgeführt. Mit roher Gewalt – denn genau das bedeutet „Brute Force" – werden alle theoretisch möglichen Kennwörter solange durchprobiert, bis das richtige gefunden ist. Mit diesem gelangen die Hacker dann ins Netzwerk – häufig sogar mit Administratorrechten ausstaffiert. Für die Angriffsopfer heißt das dann: „Game over."

Ohne zuverlässiges Logging kommt man Brute-Force-Angriffen nicht immer gleich auf die Schliche. Von der Warte des Opfers aus ähnelt Brute Force einem DDoS-Angriff, mit dem Unterschied, dass im Regelfall von nur einer oder zwei IP-Adressen aus angegriffen wird. Von Brute Force und seiner Verwandten, der SQL Injection, ist alles im Netzwerk bedroht, was direkten Internetanschluss hat. Ein beliebtes Angriffsziel ist Wordpress. Der voreingestellte Standardname des Wordpress-Admin-Nutzers lautet ganz profan „admin", und viele Wordpress-User begehen den Fehler, diesen Namen nicht zu ändern. Ein Leichtes, dieses Admin-Konto zu knacken, die gesamte Website zu übernehmen und darüber ins Firmennetzwerk zu spazieren – vorausgesetzt, das betroffene Unternehmen hostet seine Website selbst.

Varianten:
SQL Injection: Hier setzen Hacker in Feldern, in denen ein SQL-Server Datenwerte erwartet, SQL-Code ein und verschaffen sich per Datenbankverbindung Zutritt. So können sie die gesamte Datenbanksteuerung übernehmen – mit unter Umständen immensen Folgeschäden. SQL Injection ist eine stärker ausgeklügelte Brute-Force-Variante: Der „injizierte" Code wird immer wieder durchkombiniert, bis die (leider allzu oft schlecht oder gar nicht verschlüsselte) Tabelle mit den Datenbankzugangsdaten geknackt ist.

Welche Technik wirkt

Oberste Priorität haben die Einrichtung starker Kennwörter für alle mit dem Internet verbundenen Services und ein solides Kennwortmanagement. Bei kommerziell genutzten Domains sollten Sie die Kennwörter in einer so genannten demilitarisierten Zone (DMZ) platzieren. Diese Pufferzone liegt zwischen dem unternehmenseigenen und dem öffentlichen Netzwerk und verhindert, dass Unbefugte von außerhalb direkt an Unternehmensserver gelangen. Eine Alternative wäre der Betrieb der Website bei einem Cloud-Hosting-Anbieter, der mit mehreren ISPs arbeitet und DDoS-Abwehrfunktionen bietet. Und natürlich schließt eine wirksame SQL-Injection-Prävention auch Firewalls mit Anwendungserkennung ein.

Hilfreiche Technik gibt es zur Genüge – je komplexer die Lösungen, desto teurer. Das Wichtigste ist und bleibt aber Folgendes: Je ernster Sie das Risiko eines Angriffs über stark exponierte Ressourcen wie Webanwendungen mit SQL-Datenbankverbindung nehmen, desto weniger wahrscheinlich werden Sie zum Opfer. Angreifer erfolgreich abzuwehren, ist eine Sache. Eine gute Risikokompetenz ist jedoch nicht minder wichtig.

Brute-Force-Angriff

Was Sie unternehmen müssen

Beim Schutz vor Brute Force und SQL Injection sind die Netzwerkarchitektur und das Hosting von Anwendungen entscheidend sowie die Kenntnis davon, wie der SQL-Server konfiguriert ist, um mit der Webanwendung zu kommunizieren. Bei SQL Server beispielsweise gibt es zwei Authentifizierungsmodi: die Windows-Authentifizierung und den gemischten Modus, der sowohl die Windows- als auch die SQL-Server-Authentifizierung zulässt.

Die Windows-Authentifizierung ist weniger Brute-Force-gefährdet, da hier regulär nach einer bestimmten Anzahl von Zugriffsversuchen der Login verweigert wird. Genau deshalb sollten Produktivumgebungen mit Windows-Authentifizierung und Sperrrichtlinie ausgestattet sein: Beides zusammen macht Brute-Force-Angriffe zeitaufwändig.

Verwenden Sie außerdem für den Zugriff auf die SQL-Datenbank niemals ein Konto für die Domain-Administration. Warum nicht?

Aus den folgenden beiden Gründen:

- Ist das Admin-Kennwort schon geknackt, so ist damit auch Ihre SQL-Datenbank gefährdet.
- Wenn dann der Admin-Login aus Sicherheitsgründen gesperrt wird, geraten Sie in eine selbst erzeugte Denial-of-Service-Situation.

Bei der SQL-Server-Authentifizierung sind Brute-Force-Angriffe schon problematischer. Bei alten SQL-Versionen mit diesem Authentifizierungsmodus lässt sich nicht ermitteln, ob das betreffende System unter Brute-Force-Beschuss steht. Für Hacker ist die SQL-Server-Authentifizierung also ein gefundenes Fressen.

Prüfen Sie deshalb unbedingt, wie Ihre Datenbank verschlüsselt ist, über welchen Authentifizierungsmodus sie sich mit der Anwendung verbindet und welche Sicherheitsvorkehrungen Sie bereits vor Einrichtung von Anwendung und Datenbank treffen können. Wenn eine Anwendung auf einer alten SQL-Version beruht, Domain-Zugriffsrechte erfordert und keinerlei Logging- oder Alert-Funktionen hat, ist es inzwischen ein Ding der Unmöglichkeit, sie wasserdicht zu machen. Idealerweise werden sämtliche Dienste mit direkter Internetverbindung durch VPN und/oder Zugriffssteuerungslisten abgesichert.

Was in Ihr Sicherheits-Toolkit gehört

Schwachstellenmanagement für Anwendungen	MSP RMM
SNMP-Monitoring der Router-, Firewall- und Switch-Infrastruktur	MSP RMM
Web Application Firewall der nächsten Generation mit SQL-Injection-Schutzfunktionen	Sophos, Checkxxx, Cisco
E-Mail-Schutz	MSP RMM / MSP Mail
Prüfung gescheiterter Anmeldeversuche	MSP RMM
Benutzerdefinierte Ereignisprotokollprüfung, besonders bei neueren SQL-Versionen	MSP RMM
Schwachstellenscanner (Webanwendung)	ZED von OWASP, Nessus
Starkes Kennwortmanagement insbesondere für Services mit direkter Internetverbindung und Datenbankverbindungen	

Phishing

> **“Monat für Monat werden tausende E-Mail-Anhänge arglos geöffnet und Unternehmensnetzwerke großen Gefahren ausgesetzt.”**

Was ist das?

Im November 2013 warnte die britische National Crime Agency vor einer Spam-Mailkampagne, die es vor allem auf kleine und mittlere Unternehmen abgesehen hatte. Die E-Mails hatten einen zum jeweiligen Inhalt scheinbar passenden Anhang – eine Voicemail, ein Fax oder Informationen zu einer angeblich verdächtigen Transaktion oder Rechnung.

Tatsächlich aber war der Dateianhang eine Software namens CryptoLocker, die auf den angegriffenen Systemen Daten verschlüsselte. Der Schaden dadurch war insofern enorm, als die Opfer für die Entsperrung dieser Daten ein Lösegeld zahlen mussten. Zugegeben, CryptoLocker ist ein besonders perfides Beispiel für Phishing-Malware. Allerdings werden Monat für Monat in Unternehmen immer noch tausende E-Mail-Anhänge arglos geöffnet und dadurch Netzwerke gefährdet.

Varianten:
Zum Einschleusen von Malware sind Phishing-Mails nach wie vor der relevanteste Kanal. Sie treten in zwei etwa gleich häufigen Varianten auf: als E-Mail mit schädlichem Anhang (39,9 %) und als E-Mail mit verseuchtem Link darin (37,4 %). Das einzig Gute an Phishing: Es ist ausschließlich per E-Mail möglich – ein Umstand, der Ihnen wirksame Schutzmöglichkeiten eröffnet.

Phishing

Was Sie unternehmen müssen

Machen Sie sich vor allem eines klar: Es sind die Benutzer – Menschen also –, die irgendwann beschließen, einen Link anzuklicken oder einen Anhang zu öffnen. Eine Erkenntnis, die zur Entwicklung einer sinnvollen Strategie wichtig ist.

Eine Studie des Microsoft Security Bulletin aus dem Jahr 2013 zeigt: Zu den wirkungsvollsten Maßnahmen im Kampf gegen Phishing gehört der Entzug von Administratorrechten.

Durch den Entzug dieser Rechte ließen sich laut der Studie satte 92 % der 147 Sicherheitslücken schließen, die Microsoft im selben Jahr offiziell als „kritisch" eingestuft hatte. Verizon wiederum fand heraus, dass 99,9 % der 2014 genutzten Schwachstellen bereits ein Jahr vor Auslieferung des entsprechenden Patchs eine CVE-Nummer (Common Vulnerabilities and Exposures) erhalten hatten. Fast 97 % aller registrierten Angriffe erfolgten über gerade einmal 10 CVEs.

Was sagen Ihnen diese Zahlen? Dass es schon die halbe Miete ist, Betriebssystem und Anwendungen immer aktuell zu halten, denn damit alleine machen Sie Hackern das Leben schon deutlich schwerer.

„Phishing-Angriffe lassen sich erfolgreich über ein System aus mehreren Verteidigungslinien aushebeln."

Welche Technik wirkt

Sicherheitsbewusste IT-Profis setzen in erster Linie auf die Abwehr von Angriffen per E-Mail, denn 77 % aller Sicherheitsvorfälle resultieren aus E-Mail-Interaktionen von Benutzern. Natürlich wäre es grober Leichtsinn, es dabei zu belassen; nur eine umfassende Strategie, die auf mehreren Erkennungs- und Präventionspfeilern ruht, wappnet Sie gegen sämtliche Gefahren.

Vor Phishing-Angriffen schützen Sie sich erfolgreich über ein System aus mehreren Verteidigungslinien, mit dem Sie Netzwerkbenutzer davon abhalten, Schadanhänge zu öffnen oder verseuchte Websites aufzurufen. Diese Strategie funktioniert bei den zuvor genannten drei Angriffsmaschen so nicht.

Was in Ihr Sicherheits-Toolkit gehört

Patch-Management für das Betriebssystem und für Anwendungen	MSP RMM
Managed Antivirus	MSP RMM
Webschutz	MSP RMM
E-Mail-Schutz	MSP RMM / MSP Mail
Managed Online Backup	MSP RMM / MSP Backup
Mobilgerätemanagement	MSP RMM

Drive-by-Download

> **Mit Exploit-Kits greifen Kriminelle gezielt veraltete Software an.**

Was ist das?

Im Mai 2015 wurde die US-amerikanische Werbeplattform MadAdsMedia gehackt. Die Angreifer konnten dort Links platzieren, die Besucher der Plattform zu bösartigen Adobe-Flash-Exploits führten. Tag für Tag wurden etwa 12.500 Benutzer auf diese Weise angegriffen.

In diesem Fall war es das Exploit-Kit Nuclear, mit dem die Hacker Erfolg hatten. Exploit-Kits zielen auf Internetsurfer ab; diese sollen die Malware weiter verbreiten. Die Kits werden auf manipulierten Websites platziert und machen sich Sicherheitslücken in Software zunutze. Sie suchen alle möglichen Systeme, Browser oder Plug-ins wie Flash Player, Adobe Reader, Java oder Microsoft Silverlight auf Patching-Lücken hin ab, setzen also bei mehr oder minder veralteten Softwareversionen an.

Welche Technik wirkt

Dass Sie Ihr Sicherheitskonzept breit aufstellen sollten, anstelle sich auf einzelne Bedrohungen zu kaprizieren, geht aus dem bereits Gesagten schon hervor. Umfassender Webschutz ist keine rein technische Angelegenheit. Sie müssen sich vielmehr gründlich damit auseinandersetzen, welche Gefahren in der Nutzung des Web lauern und wie Sie sich schützen können.

Webschutz ist umfassender als ein herkömmlicher Virenschutz. Er hält Internetbenutzer davon ab, berüchtigte Problemseiten zu besuchen, und mindert so aktiv das Infektionsrisiko. Im Zuge dessen schärft Webschutz das Sicherheitsbewusstsein von Benutzern und kann bestimmte Verhaltensweisen bahnen. Hinzu kommen die damit erstellbaren Berichte, die Aufschluss geben über die Ursachen einer schlechten Internet-Performance und eine forensische Analyse verdächtiger Datenströme ermöglichen.

Drive-by-Download

Was Sie unternehmen müssen

Wie beim Phishing lässt sich auch hier mit einer Mehrlinienverteidigung viel erreichen. Vorfallanalysen zeigen: Alleine durch E-Mails mit bösartigen Links (37,4 %) und Drive-by-Downloads von Websites (16,6 %) werden schon 54 % aller Sicherheitsvorfälle verursacht. Eine gute Schutzstrategie unterbindet das Aufsuchen schädlicher Websites von vornherein. Auch die Konzentration auf Hackversuche über das Web ausgeführte schlägt schon viele Fliegen mit einer Klappe. Sie baut auf dieselben Techniken, die auch gegen das Phishing zum Einsatz kommen.

Bei Gefahren aus dem Web lohnt ein genauer Blick auf die jeweils verwendeten Infektionsmechanismen. Meist wird ein bösartiges Exploit-Kit eingesetzt, das sich auf einer manipulierten Website befindet. Die erste Kardinalmaßnahme wäre also das Löschen von Mails mit verseuchten Links. Links werden Computerbenutzern allerdings auf viele Weisen präsentiert: in Anzeigen, in sozialen Netzen, per Instant Messaging und so weiter. All diese Verbreitungskanäle sind sehr viel schwieriger zu beherrschen als E-Mails.

> **“Alleine durch E-Mails mit bösartigen Links und Drive-by-Downloads von Websites werden schon 54 % aller Sicherheitsvorfälle verursacht.”**

Selbstverständlich sollten Browser und Plug-ins immer auf dem neuesten Stand sein. Ein weiteres probates Mittel besteht darin, auf Computern oder Workstations mehrere Browser zu installieren. Sollte ein bestimmter Browser Ziel eines Zero-Day-Angriffs werden (was nur selten vorkommt), kann solange auf andere Browser ausgewichen werden, bis es ein Patch für den angegriffenen Browser gibt.

Als Fachmann oder Fachfrau für IT kennen Sie die Rolle von DNS im Zusammenhang mit dem Surfen im Web und der Nutzung von E-Mail sowie anderer Internetverbindungen, die eine Namensauflösung erfordern. Bestimmt wissen Sie dann auch, dass DNS keine sichere Technik ist; der bisherigen Datenlage zufolge stellen schlecht abgesicherte DNS-Server von ISPs vielmehr ein großes Risiko dar. Ein gehackter DNS-Server kann Anfragen an legitime Websites auf manipulierte Sites umleiten.

DNS ist ein Fundament der Webkommunikation. Sie ziehen eine weitere Sicherheitsebene ein, wenn Sie sich auf einen Anbieter von DNS-Services konzentrieren, etwa Google oder Webroot. Zusätzlicher Bonus: Entsprechende Firewall-Regeln oder DNS-Server-Logging vorausgesetzt, können Sie dann Unregelmäßigkeiten aufdecken, etwa wenn eine Workstation in Ihrem Netzwerk versucht, einen DNS-Server beispielsweise in Russland zu erreichen. Per se ist das keinesfalls beunruhigend, es sei denn, Sie haben mit Russland so gar nichts zu tun ...

Was in Ihr Sicherheits-Toolkit gehört

Patch-Management für das Betriebssystem und für Anwendungen	MSP RMM
Managed Antivirus	MSP RMM
Webschutz	MSP RMM
Sichere oder gut etablierte öffentliche DNS-Server	Sicherer DNS-Service von Webroot, Google, Microsoft
Schwachstellen-Scanner	MSP Risk Intelligence

Spear Phishing

> **“Spear Phishing setzt auf den Faktor Mensch: Es erschleicht sich Vertrauen. Dem ist mit technischen Mitteln nicht richtig beizukommen, was einen wirksamen Schutz erschwert.”**

Was ist das?

2014 geriet das US-Unternehmen Scoular ins Visier krimineller Hacker. Der Finanzcontroller der Firma überwies insgesamt gut 17 Millionen Dollar an eine Bank in China. Dazu hatten ihn verflixt echt wirkende E-Mails gebracht, die ihn anwiesen, Instruktionen zur Überweisung von einem Mitarbeiter von KPMG einzuholen, dem Unternehmen also, das für Scoular die Bücher führte.

Der genannte Mitarbeiter existierte tatsächlich bei KPMG, auch erweckte die E-Mail den Anschein, von KPMG zu kommen. In Wirklichkeit steckte dahinter jedoch ein Server in Russland, und die angegebene Telefonnummer führte zu einem israelischen Skype-Account. Der Coup glückte und zog eine ganze Reihe weiterer spektakulärer Spear-Phishing-Affären im Bereich elektronische Zahlungsabwicklung nach sich.

Spear Phishing setzt auf den Faktor Mensch: Es erschleicht sich das Vertrauen des Adressaten. Dem ist mit technischen Mitteln nicht richtig beizukommen, was einen wirksamen Schutz erschwert. Plumpe und schlecht gemachte Betrugsversuche wie die Nigeria-Connection oder „heiße Girls aus Russland" gibt es zuhauf, und die Grenze zwischen Phishing und Spam verwischt immer mehr. Spear Phisher spielen aber leider in einer ganz anderen Liga.

Varianten:
Spear Phishing zielt immer auf Unternehmen ab. Ein Verwandter davon ist das Whale Phishing: Hier werden gezielt „große Tiere", Mitglieder der Unternehmensführung, angesprochen.

Was Sie unternehmen müssen

Natürlich ist auch beim Spear Phishing das technische Rüstzeug wichtig. Die beste Verteidigung ist und bleibt hier jedoch gesunde Skepsis – und die lässt sich schulen. Mit Fug und Recht wähnten sich die gehackten Banken in unserer Fallstudie (siehe Seite xx) hinter ihren dicken Netzwerkmauern sicher. Unsicher war etwas ganz anderes: die Smartphones und Tablets ihrer Manager. Hätten damals die normalen Netzwerkbenutzer keine Admin-Rechte gehabt, mit denen sich Programme installieren lassen, so hätten sich die Angreifer wohl die Zähne ausgebissen. Sicherheitstechnik und Menschen: Beides kann versagen, daran sollten Sie immer denken. Deshalb müssen Sie es der Technik und den Menschen so einfach wie möglich machen, Dubioses zu erkennen und den Schurken einen Strich durch die Rechnung zu machen.

IT-Anbietern eröffnet sich hier die Chance, Unternehmen im Kampf gegen Social Engineering zu unterstützen, beispielsweise durch Schulung der Mitarbeiter zu einem sicheren Umgang mit Internet, E-Mail und Netzwerk und durch jährliche Auffrischung dieses Wissens. Weiteres Geschäftspotenzial liegt im Anbieten von Penetrationstests und Red-Team-Services für Social Engineering, um Prozesse und Vorgehensweisen eines Unternehmens zu Finanztransaktionen und zum Schutz vertraulicher Daten sicherer zu machen.

Spear Phishing

Welche Technik wirkt

Natürlich ist auch beim Spear Phishing das technische Rüstzeug wichtig. Die beste Verteidigung ist und bleibt hier jedoch gesunde Skepsis – und die lässt sich schulen. Mit Fug und Recht wähnten sich die gehackten Banken in unserer Fallstudie (siehe Seite 30) hinter ihren dicken Netzwerkmauern sicher. Unsicher war etwas ganz anderes: die Smartphones und Tablets ihrer Manager. Hätten damals die normalen Netzwerkbenutzer keine Admin-Rechte gehabt, mit denen sich Programme installieren lassen, so hätten sich die Angreifer wohl die Zähne ausgebissen. Sicherheitstechnik und Menschen: Beides kann versagen, daran sollten Sie immer denken. Deshalb müssen Sie es der Technik und den Menschen so einfach wie möglich machen, Dubioses zu erkennen und den Schurken einen Strich durch die Rechnung zu machen.

Ins Security-Portfolio gehören hier Sicherheitsaudits und Schwachstellen-Scans. Beide fördern auch entscheidend die Compliance. Wenn Sie demonstrieren können, wie einfach Menschen hinters Licht zu führen sind, kann das wie ein Weckruf wirken. Dazu müssen Sie gar kein Experte sein. Zum Aufspüren von Sicherheitslücken gibt es einsatzfertige Tools, die sehr einfach zu bedienen sind (leider auch für Hacker mit bösen Absichten …).

> **“Wenn Sie demonstrieren können,** *wie einfach Menschen hinters Licht zu führen sind,* **kann das wie ein Weckruf wirken.”**

Wenn Sie erwägen, ein Security-Komplettpaket gegen Spear Phishing einzuführen, sollten Sie sich einmal mit dem Social-Engineer Toolkit (SET)* befassen. SET ist ein Open-Source-Tool, mit dem Sie prüfen können, ob Ihre IT-Infrastruktur wasserdicht ist. Sie können damit (mit ausdrücklicher Erlaubnis der Verantwortlichen, versteht sich) zur Probe Spear-Phishing-E-Mails im eigenen Netzwerk versenden, um zu sehen, wie diese bei den betreffenden Adressaten „ankommen“.

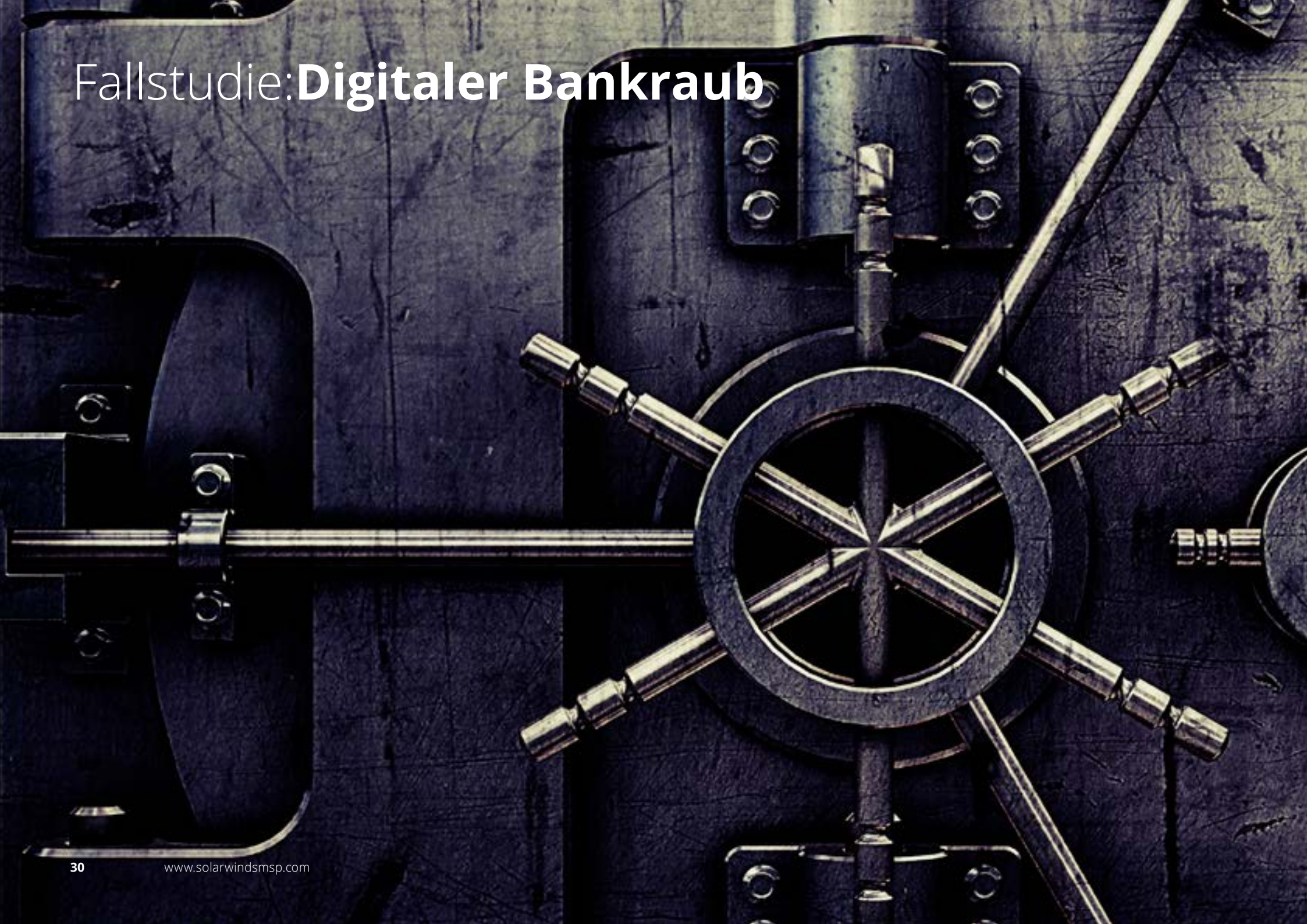
Mit SET können Sie ganz bequem viele Social-Engineering-Angriffsmaschen simulieren. Sie trainieren mit dem Tool sozusagen für den Ernstfall, denn Sie optimieren Ihren Umgang mit Social Engineering und haben irgendwann so viel Routine, dass Sie den dunklen Gestalten da draußen immer eine Nasenlänge voraus sind. Exploit-verseuchte Webseiten oder E-Mails erzeugen und über Metasploit-Payloads eine Rückverbindung mit einer Command Shell aufbauen, sobald die betreffende Seite geöffnet wird: All das geht mit SET ganz automatisch.

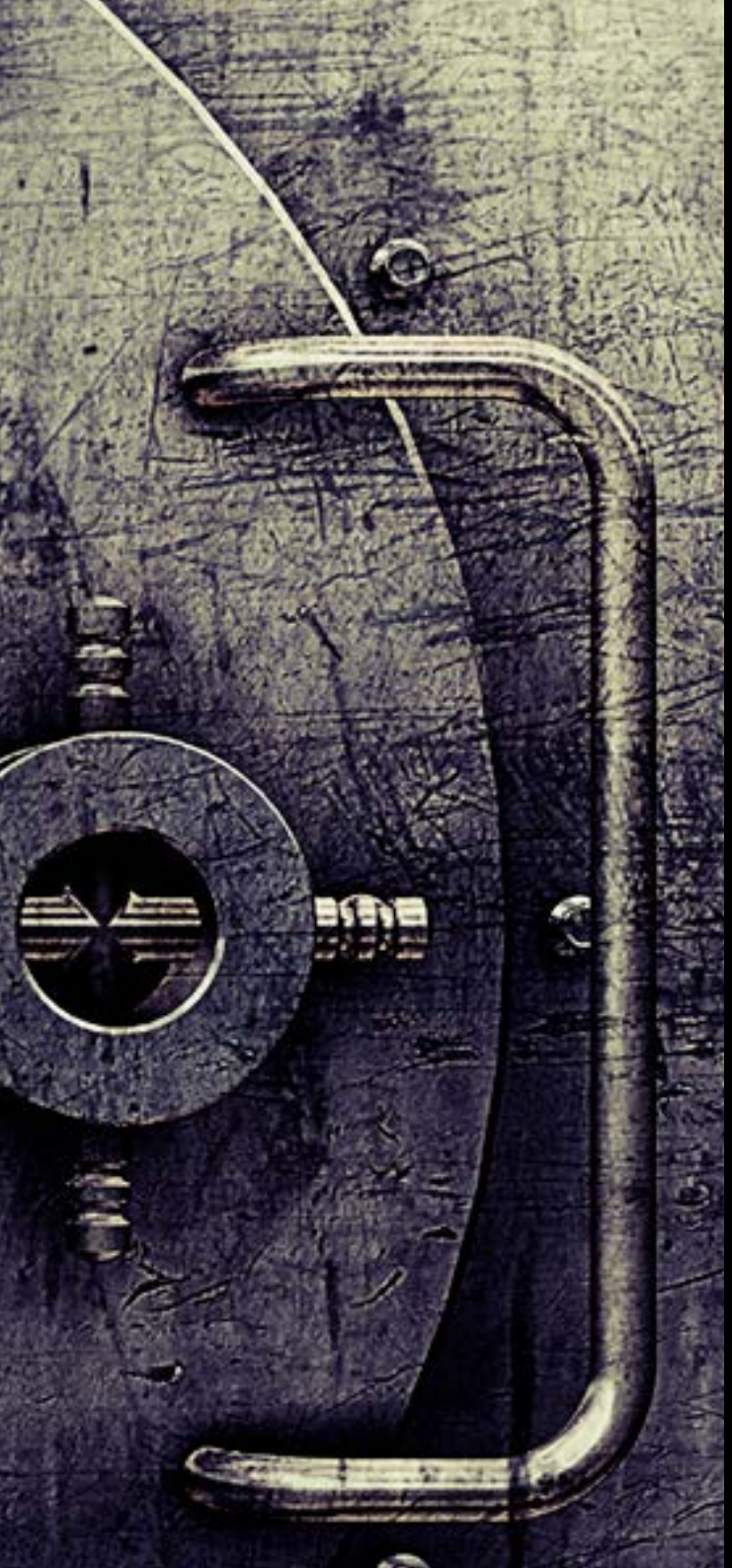
* https://www.trustedsec.com/social-engineer-toolkit/

Was in Ihr Sicherheits-Toolkit gehört

Schulung von Endbenutzern zum sicheren Umgang mit Web und E-Mail	
Risiko- und Schwachstellenanalyse	MSP Risk Intelligence
Patch-Management für das Betriebssystem und für Anwendungen	MSP RMM
Managed Antivirus	MSP RMM
Webschutz	MSP RMM
Managed Online Backup	MSP RMM / MSP Backup

Fallstudie:**Digitaler Bankraub**





Anfang 2015 wurde ein Cyberbankraub gigantischen Ausmaßes bekannt. Per Spear Phishing waren Hacker mit der Malware Carbanak in die Systeme vieler Banken weltweit eingedrungen. Über zwei Jahre hinweg sollen auf diese Weise zwischen 300 Millionen und einer Milliarde US-Dollar erbeutet worden sein. Weitere Untersuchungen ergaben: Die Angriffsserie hätte schon mit simplen und grundlegenden Sicherheitsmaßnahmen verhindert werden können.

Auf ordentlich gepatchten und aktuell gehaltenen Systemen hätte ein Spear-Phishing-Angriff wie dieser gar keine Chance gehabt. Eine sachkundige Quelle konstatierte: „In allen Vorfällen waren E-Mails mit Doc-Anhängen im Format Microsoft Word 97 bis 2003 oder CPL-Dateien verschickt worden. Diese Dateien nutzen Sicherheitslücken in Microsoft Office (CVE-2012-0158 und CVE-2013-3906) und Microsoft Word (CVE-2014-1761)."

Der verwendete Trojaner war bereits so alt, dass eine normale Antivirensoftware ihn höchstwahrscheinlich abgefangen hätte. Die Berichte legten außerdem nahe, dass die meisten der betroffenen Netzwerke schon zwei bis vier Monate zuvor infiltriert worden waren. Anders ausgedrückt: Bis zu vier Monate hätten die Banken Zeit gehabt, die Systeme zu patchen – und hatten dies ganz offensichtlich versäumt.

Genügend Zeit, in der die Bankräuber in aller Ruhe die Lücken im System auskundschaften und Daten über ihre Spear-Phishing-Ziele sammeln konnten, um dann E-Mails zu verfassen, die so echt aussahen, dass die Betreffenden darauf hereinfielen.

APT-Angriff – durch Cyberkriminelle/ Hacktivisten

> **APT-Angreifer peinigen ihre Opfer solange, bis sie Erfolg haben.**

Was ist das?

Im Februar 2015 bekannte sich eine APT-Gruppe namens Desert Falcons zum Hacking von etwa 3.000 Zielen in gut 50 Ländern. Die meisten davon befanden sich in Palästina, Ägypten, Israel und Jordanien; weitere Fälle gab es u. a. in Saudi-Arabien, den Vereinigten Arabischen Emiraten, den USA, Südkorea, Marokko und Katar. Betroffen waren Militär- und Regierungsorganisationen, Beauftragte bei Gesundheitsorganisationen und in der Geldwäscheprävention, Unternehmen, Banken, führende Medienhäuser, Forschungs- und Bildungseinrichtungen, Versorgungsunternehmen, Aktivisten und Politiker, Security-Unternehmen und andere Institutionen und Personen mit einem Zugang zu geopolitischen Informationen.

APT-Hacker „haben mehr Niveau" als gewöhnliche Cyberkriminelle. Sie agieren cleverer, sind stärker organisiert und verfügen über bessere Ressourcen. APT-Angreifer schießen sich auf einen bestimmten Akteur ein – ein Unternehmen, eine Institution – und traktieren ihr Opfer solange, bis sie das Gewünschte erreicht haben. Hartnäckig, anpassungsfähig, flexibel bei der Wahl der Angriffsform: Unter den Internetverbrechern sind APT-Hacker kurz gesagt die Crème de la Crème. Sie können Einzeltäter sein, agieren allerdings meist in Verbünden, die Unternehmen vergleichbar in Rollen, Funktionen und Geschäftsbereiche gegliedert und arbeitsteilig organisiert sind.

Varianten:
Gut 100 APT-Gruppen sind in Sicherheitskreisen bekannt. Ein bekannter Vertreter dieses Genres ist Anonymous, unter dessen Banner sich Tausende Hacktivisten sammeln. Zunächst einmal: Die Abgrenzung zwischen APT, Hacktivismus, staatlich gesponserten Angriffen und hochorganisierter Kriminalität ist sehr schwierig. Im Sammelbecken „APT" finden sich alle möglichen Schattierungen; drei Dinge jedoch haben alle gemeinsam:

- Sie haben es auf alles abgesehen, was Sie und Ihr Unternehmen im Internet ausmacht.
- Sie agieren entweder mit ideologischer, kultureller, politischer oder religiöser Motivation oder aber betreiben Industriespionage, um mit dem erbeuteten Wissen die vorgenannten Zwecke voranzutreiben oder schlicht geistiges Eigentum zu stehlen.
- Sie sind überaus hartnäckig. APT-Hacker bleiben immer am Ball: Sie sondieren Schwachstellen, betreiben Brute Forcing, Spear Phishing, schnüffeln Netze aus und verüben DDoS-Angriffe. Um ihren Opfern das Leben schwer zu machen, sind ihnen alle Mittel recht.

Was Sie unternehmen müssen

Als IT-Fachmann sollten Sie die Chancen, ein APT-Hackerkollektiv erfolgreich abzuwehren, das mutmaßlich eher groß ist und echte Profis in seinen Reihen zählt, möglichst nüchtern betrachten. Fragen Sie sich zuerst: Habe ich das Know-how und die Fähigkeiten, es mit diesen Leuten aufzunehmen? Und lohnt sich der Aufbau einer Abwehr zeitlich und finanziell? Häufige Hacktivismus-Opfer sind vor allem große Organisationen, die sich durch ihr Angebot und Wirken in politischer, kultureller, religiöser oder ideologischer Hinsicht zu Zielscheiben machen.

> **“Haben Sie das Know-how und die Fähigkeiten, es mit APT-Hackern aufzunehmen? Und lohnt sich der Aufbau einer Abwehr zeitlich und finanziell?”**

Welche Technik wirkt

Auch für große Sicherheitsorganisationen ist APT eine harte Nuss. Hier werden alle Geschütze aufgefahren, die die Security-Branche zu bieten hat.

Um hier Herr der Lage zu bleiben, müssen Sie hochspezielle und unspezifische Technik gleichermaßen bemühen. Software und Hardware müssen außerordentlich gut zu kontrollieren sein, und es ist eine Kombination von Lösungen gefragt. In den meisten Fällen sind sehr spezielle Security-Fertigkeiten gefordert, von Überwachung und 24-Stunden-Notfallservice ganz zu schweigen. Netzwerkisolierung, Einbruchserkennung, Whitelisting von Anwendungen und eine möglichst großflächige Verschlüsselung ruhender und übertragener Daten gehören zu den Spezialmaßnahmen, mit denen Sie im Kampf gegen APT Land gewinnen.

Kommt es hart auf hart, hilft manchmal nur noch „Aktion Molotow“: sämtliche Netzwerkstrukturen niederzubrennen und alles neu ohne die Schlupflöcher aufzubauen, über die Ihre Gegner zuvor eindringen konnten. Dies ist ein langwieriger und beschwerlicher Weg und ein entsprechend umfangreiches Projekt, bei dem Sie Design und Neubau des Netzwerks von vornherein sorgfältig und methodisch angehen müssen – am besten auf der Basis eines Rahmens, wie die Top 20 Sicherheitsmaßnahmen des SANS* ihn darstellen. In jeder Designphase müssen Sicherheitsaspekte, wirksame Kontrollen und Überwachungsmechanismen verankert werden, OSI-7-Schichten-Modell, Heizung, Lüftung, Klimatechnik und Gebäudesicherheit eingeschlossen. Spezialisten, die einen solchen Netzwerkbau in allen Belangen von A bis Z fachgerecht ausführen können, sind weltweit handverlesen. Sicher mit ein Grund, warum APT-Hacker bei Banken, Airlines, Regierungsorganisationen und Militärinstitutionen immer noch und immer wieder Erfolg haben.

* https://www.sans.org/critical-security-controls/

Diese Liste ist keinesfalls erschöpfend.
Eine gute Informationsquelle zu allen erforderlichen technischen Lösungen finden Sie hier:

http://www.asd.gov.au/infosec/mitigationstrategies.htm

	MSP RMM	MSP Risk Intelligence	Alien Vault	Amazon	App Locker	Aruba Networks	Azure	Becrypt	Bit 9	Checkpoint	Cisco	Cisco Meraki	CloudFlare	Due	Firmware updates	Goldren Images	Google	LogRythm	Metasploit	Microsoft	Nessus	NMap	NetFlow	Observium	PGP	RSA	SonicWall	Sophos	Snort	Splunk	Zonefox	WatchGuard	Webroot Secure DNS	Windows Bitlocker	Wire Shark
Whitelisting von Anwendungen					•				•																										
Management für Sicherheitslösungen																•																			
Benutzerdefinierte Ereignisprotokollprüfung	•																																		
Vollständige Datenträgerverschlüsselung (Entfernung nicht verschlüsselter Daten)								•																										•	
Verschlüsselung für Daten in Übertragung (Entfernung aller Klartextprotokolle)																									•			•							
E-Mail-Schutz	•																																		
Schwachstellenscan extern und intern	•	•																	•		•	•													
Anmeldeüberprüfung fehlgeschlagen	•																																		
Überwachung der Dateiintegrität																														•					
Host-Einbrucherkennung			•																								•		•						
Hosted Services Provider				•			•										•																		
Interne Netzwerksegmentierung																																			
Interne VPN-Lösung											•									•															
Protokollmanagement	•																	•											•						
E-Mail-Schutz	•																																		
Managed Antivirus	•																																		
Managed Online Backup	•																																		
Mobilgeräteverwaltung	•																																		
Netzwerk-Einbrucherkennung										•																						•			
Firewall der nächsten Generation mit DDoS-Schutz und SQL-Injection-Schutzfunktionen											•															•	•								
Lösung für die Paketanalyse/-inspektion																							•	•											•
Patchmanagement für Betriebssystem und externe Anwendungen	•																																		
Redundante Internetverbindungen, gehostete DDoS-Services													•																						
Scripting-Funktionen	•																																		
Sichere oder sehr bekannte öffentliche DNS-Server																	•			•														•	
SNMP-HLK-Überwachung	•																																		
SNMP-Monitoring der Router-, Firewall- und Switch-Infrastruktur	•																																		
Service-Desk Verfolgung und Überwachung	•																																		
Zwei-Faktor-Authentifizierung für alle Dienste														•												•									
Schwachstellenmanagement des jeweiligen Komponentenherstellers															•																				
Webschutz	•																																		
Wireless-Einbrucherkennung						•						•																							

All dies ergänzend zur kontinuierlichen Schulung zur Websicherheit für Endanwender und Service-Provider und interner Netzwerksegmentierung.

APT-Angriff – feindliche Spionage

> **“Im besten Fall werden Sie ausspioniert. Im schlimmsten Fall werden Ihre Systeme manipuliert oder unbrauchbar gemacht.”**

Was ist das?

Im Februar 2015 veröffentlichte das Kaspersky Lab Forschungsergebnisse zu Cyberangriffen der so genannten Equation Group, eines offensichtlich im Staatsauftrag agierenden Hackerkollektivs. Reuters zufolge bestätigten zwei frühere NSA-Mitarbeiter diese Analysen: Für die NSA seien „diese Spionageprogramme ähnlich wertvoll wie Stuxnet".

Dem Bericht zufolge waren die Equation Group und die Stuxnet-Entwickler entweder identisch oder aber sie arbeiteten eng zusammen; verschiedene Sicherheitsexperten brachten die USA und Israel mit den Angriffen in Verbindung. Die Hacker der Equation Group hatten offensichtlich die Firmware von Computerfestplatten infiziert und so umprogrammiert, dass normale Wiederherstellungsprozeduren (Festplatte austauschen und neu formatieren, Betriebssystem neu aufsetzen und Software neu installieren) wirkungslos blieben, da sich der Schädling auf der Festplatte verbergen ließ. Damit konnte er nicht entdeckt geschweige denn entfernt werden.

Normale APT-Hacker – ob kriminell oder anderweitig motiviert – mögen auf simples Phishing setzen, um Benutzer zum Download von Malware zu bewegen. Hacker, die im Auftrag von Geheimdiensten agieren, bemühen da schon ein ganz anderes Waffenarsenal. Im besten Fall werden Sie ausspioniert. Im schlimmsten Fall werden Ihre Systeme manipuliert oder unbrauchbar gemacht.

Varianten:

Welche Staaten in den Cyberkrieg verwickelt sind, ist nicht exakt bekannt; die meisten Industrieländer (und ein paar Entwicklungsländer) sind auf jeden Fall fleißig dabei, ihre diesbezüglichen Fertigkeiten auszubauen. Aktuell kann von etwa 50 bis 100 Staaten mit einem mehr oder weniger ausgefeilten Know-how ausgegangen werden. Die skrupellose Beteiligung von Staaten an kriminellen Akten im Cyberkrieg stellt APT in seiner schlimmsten Form dar. Die Raffinesse, mit der staatlich gesponserte Hacker ihre Opfer, ob Privatpersonen oder Institutionen, verfolgen, lässt einen schlicht gruseln. Abgesehen von millionenschweren physischen Schäden sind solche Akteure in der Lage, jederzeit flächendeckend Chaos und Panik zu verbreiten. Kriminelle dieses Zuschnitts erhalten von ihren Auftraggebern ein dezidiertes Budget und Zugang zu nahezu unbegrenzten Ressourcen. Dies sowie das Folgende unterscheidet die Spionage-Hacker von den Hacktivisten: Staatlich gesponserte APT-Hacker haben Zugang zu exzellenten Schulungsressourcen und keine Angst vor strafrechtlichen Konsequenzen. Sie operieren verdeckt und müssen kaum Vergeltung fürchten, da die Regierung, in deren Auftrag sie handeln, Deutungshoheit über die Legalität und Ethik ihres Verhaltens beansprucht.

Was Sie unternehmen müssen

Eine Organisation, die eine potenzielle Zielscheibe für Cyberspionage ist, weiß mit Sicherheit, wie sie ihre wesentlichen Ressourcen – in dem Fall alle, die auf keinen Fall Internetverbindung haben dürfen – konfigurieren muss. Als Security-Verantwortlicher müssten Sie in diesem Fall lediglich sicherstellen, dass diese Systeme auch strikt vom Internet getrennt sind und bleiben.

Keine Internetverbindung haben sollten die folgenden Infrastrukturen: geheime Computernetzwerke, Systeme von Militär und Regierung, Computersysteme von Finanzorganisationen und Börsen, computergestützte industrielle Steuersysteme auf Öl- und Gasfeldern, zentrale Systeme für die Steuerung von Atomkraftwerken, Computer in der Luftfahrt und computergesteuerte medizinische Instrumente.

> **“Zu viele zentrale Systeme sind mit dem Internet verbunden, und das gänzlich ohne grundlegende Schutzmechanismen.”**

Die traurige Wahrheit: Viele solcher Systeme sind sehr wohl mit dem Internet verbunden, und das gänzlich ohne grundlegende Schutzmechanismen. Durch Einrichtung wirksamer Security-Lösungen lässt sich sicherstellen, dass die Vorteile einer Internetverbindung nicht gleichzeitig Schwachstellen gebären, die Kriminelle mit entsprechenden Konsequenzen nutzen könnten.

Welche Technik wirkt

Ernsthaft überdacht werden sollten hier in jedem Fall Architektur und Internetverbindung des Netzwerks. Sinnvoll wären ein Netzwerk mit „Air Gap“ und gute physische Sicherungsmaßnahmen. Hinzu kämen all die bislang in diesem Leitfaden erwähnten technischen Lösungen – auch im Falle eines Air-Gap-Netzwerks. Ohne Verbindung mit dem Internet ist ein Netzwerk theoretisch gesprochen sicher. Für entsprechend ausstaffierte, staatlich gesponserte Hacker ist aber selbst Air Gap kein Hindernis.

Im Prinzip kann es auch ein großes Unternehmen unmöglich mit APT-Spionen im Staatsauftrag aufnehmen. Alle erdenklichen Sicherheitsmechanismen nur auf Verdacht hin zu implementieren, wäre höchst kostspielig. Andererseits sollten Organisationen, die primär dem Risiko der APT-Spionage ausgesetzt sind, große Investitionen nicht scheuen: in physische Sicherheit, eine großflächige Verschlüsselung und eine nicht persistente und stark verschlüsselte Verbindung mit dem Internet über TOR.

Diese Liste ist keinesfalls erschöpfend.
Eine gute Informationsquelle zu allen erforderlichen technischen Lösungen finden Sie hier:

http://www.asd.gov.au/infosec/mitigationstrategies.htm

	MSP RMM	MSP Risk Intelligence	Alien Vault	Amazon	App Locker	Aruba Networks	Azure	Becrypt	Bit 9	Checkpoint	Cisco	Cisco Meraki	CloudFlare	Due	Firmware updates	Goldren Images	Google	LogRythm	Metasploit	Microsoft	Nessus	NMap	NetFlow	Observium	PGP	RSA	SonicWall	Sophos	Snort	Splunk	Zonefox	WatchGuard	Webroot Secure DNS	Windows Bitlocker	Wire Shark
Whitelisting von Anwendungen					●				●																										
Management für Sicherheitslösungen																●																			
Benutzerdefinierte Ereignisprotokollprüfung	●																																		
Vollständige Datenträgerverschlüsselung (Entfernung nicht verschlüsselter Daten)								●																										●	
Verschlüsselung für Daten in Übertragung (Entfernung aller Klartextprotokolle)																									●			●							
E-Mail-Schutz	●																																		
Schwachstellenscan extern und intern	●	●																	●		●	●													
Anmeldeüberprüfung fehlgeschlagen	●																																		
Überwachung der Dateiintegrität																														●					
Host-Einbrucherkennung			●																								●		●						
Hosted Services Provider				●			●										●																		
Interne Netzwerksegmentierung																																			
Interne VPN-Lösung											●									●															
Protokollmanagement	●																	●												●					
E-Mail-Schutz	●																																		
Managed Antivirus	●																																		
Managed Online Backup	●																																		
Mobilgeräteverwaltung	●																																		
Netzwerk-Einbrucherkennung										●																					●				
Firewall der nächsten Generation mit DDoS-Schutz und SQL-Injection-Schutzfunktionen											●																●	●							
Lösung für die Paketanalyse/-inspektion																							●	●											●
Patchmanagement für Betriebssystem und externe Anwendungen	●																																		
Redundante Internetverbindungen, gehostete DDoS-Services													●																						
Scripting-Funktionen	●																																		
Sichere oder sehr bekannte öffentliche DNS-Server																	●			●														●	
SNMP-HLK-Überwachung	●																																		
SNMP-Monitoring der Router-, Firewall- und Switch-Infrastruktur	●																																		
Service-Desk Verfolgung und Überwachung	●																																		
Zwei-Faktor-Authentifizierung für alle Dienste														●												●									
Schwachstellenmanagement des jeweiligen Komponentenherstellers															●																				
Webschutz	●																																		
Wireless-Einbrucherkennung						●						●																							

All dies ergänzend zur kontinuierlichen Schulung zur Websicherheit für Endanwender und Service-Provider und interner Netzwerksegmentierung.

Datenzerstörung

> **“Bei manchen Hacks geht es nur darum, Eigentum zu zerstören und vertrauliche Daten offenzulegen.”**

Was ist das?

Der Angriff auf Sony Pictures Entertainment im Dezember 2014 hatte ein bis dato nicht gekanntes Schadensausmaß. Er hat gezeigt, was passieren kann, wenn Datensicherheit auf die leichte Schulter genommen wird. Dem Sicherheitsunternehmen Mandiant zufolge sollte dieser Hack Eigentum zerstören und vertrauliche Daten offenlegen. Als Reaktion auf die Vorfälle – das Bekanntwerden kompromittierender E-Mails und die Zerstörung von Daten – lancierte das FBI eine Eilmeldung, um andere Unternehmen vor der Gefahr zu warnen.

Fakt ist, dass Sony beträchtlichen Schaden nahm: an seinem geistigen Eigentum, durch Zerstörung von Daten, unbefugte Offenlegung von Verschlusssachen und Blockierung von Diensten. Nicht zuletzt erlitt das Unternehmen einen Imageschaden, der hochrangige Manager den Kopf kostete.

Varianten:

Die Häufung unterschiedlicher Vorfälle innerhalb einer so kurzen Zeitspanne ist neu in der Geschichte des Cybercrime, und so perfide wie im Fall von Sony ging es selten zu. Zu keinem Zeitpunkt war Sony mit Geldforderungen konfrontiert – es ging einzig und alleine darum, den digitalen GAU herbeizuführen. Angesichts des aktuellen Zustands der Cybersecurity und des anhaltenden Erfolgs skrupelloser Verbrecher würde es anderen Unternehmen bei ähnlich gelagerten Angriffen vermutlich kaum besser ergehen. Angeblich sei die Malware durch Antivirenprogramme nicht erkennbar gewesen. Das macht stutzig, soll aber wohl von der Tatsache ablenken, dass es bei Sony eine Datei namens Password.xls gab, die weder verschlüsselt noch kennwortgeschützt war: Sie enthielt sämtliche Kennwörter – auch die für Administratoren. Dass ein Großkonzern, dessen IT-Schutz lediglich aus der Antivirensoftware eines einzelnen Anbieters besteht, irgendwann gehackt wird, war abzusehen. Als Leser unseres Cyber Threat Guide wissen Sie spätestens jetzt: Dieses Unglück wäre vermeidbar gewesen.

Datenzerstörung

Was Sie unternehmen müssen

Entwerfen Sie unbedingt eine Sicherheitslösung, die zu den Risiken passt, denen das Unternehmen ausgesetzt ist. Es geht weniger darum, möglichst viel technisches Gerät zu haben, sondern eher darum, ein Netzwerk so einzurichten, dass es einfach zu verwalten und fortlaufend zu überwachen ist. Das ist in puncto Security schon mehr als die halbe Miete. Bei fast allen jüngeren Hackerangriffen hat es schon beim kleinen Einmaleins der Sicherheit gehapert und die Betroffenen haben sich zu stark auf ihre Perimeterabwehr verlassen.

Auf schaurigen Drohkulissen lässt sich dauerhaft kein Geschäft aufbauen, zumal es beim Thema Security ohnehin um viel mehr geht: ein sinnvolles Miteinander von Technik, Menschen und Prozessen nämlich. Idealerweise beginnen Sie ein diesbezügliches Vorhaben mit einer Bestandsaufnahme zur Sicherheit und einem Plan zum Beheben der gefundenen Knackpunkte. Auf dieser Grundlage lässt sich eine Lösung ausarbeiten, mit der sich ein System anforderungsgemäß überwachen und regeln lässt. Bekanntermaßen lässt sich das Meiste schon mit einfachen Mitteln erreichen, auch beim Thema Sicherheit – nachzulesen in einem Artikel von James Lewis zu Cybersecurity aus dem Jahr 2013*:

- Gut 90 % der erfolgreichen Hacks beruhten auf der Anwendung einfachster Mittel.
- Nur 3 % der Hacks wären ohne komplizierte und kostspielige Maßnahmen unvermeidbar gewesen.
- 96 % der erfolgreichen Hacks hätten durch das Vorhalten einfachster bis mittelkomplexer Sicherheitsmaßnahmen vermieden werden können.
- 75 % der Angriffe nutzen offiziell bekannte Sicherheitslücken in kommerzieller Software, die man durch reguläres Patching schließen könnte.

> **“Alle Bestrebungen in puncto Sicherheit nutzen nichts, wenn Leitung und Management eines Unternehmens nicht dahinterstehen.”**

Welche Technik wirkt

Für Sie als IT-Experte sollte Folgendes klar sein: Alle Bestrebungen in puncto Security, alle Sorgfalt und Sicherheitstechnik nutzen nichts, wenn Leitung und Management eines Unternehmens nicht dahinterstehen. Ist dem nicht so, dann kommt unweigerlich der Tag, an dem Sie Ihre Fähigkeiten beim Wiederherstellen von Daten brauchen werden.

Der Fall Sony ist ein Worst-Case-Szenario, das zeigen soll, was passiert, wenn ein Unternehmen sich nicht ausreichend rüstet. Die Sony-Angreifer setzten etwas fort, was in der Aramco- und der Stuxnet-Affäre seinen Anfang genommen hatte: die massive Zerstörung von Daten. Auch Angriffe jüngeren Datums in der Ukraine und in Israel zeigen, welches Motiv APT-Hacker antreibt: Sie wollen durch ihr Treiben schlicht handfesten Schaden anrichten. Mit Angriffen auf Unternehmen, Regierungen oder Organisationen, die Daten zerstören und Lösegeld erpressen sollen, steht nun eine ganz neue Bedrohung im Raum – vielleicht die bis dato übelste. Hier geht es nicht mehr nur um den Diebstahl von persönlichen Daten oder geistigem Eigentum, sondern darum, Daten zu zerstören oder ein Schutzgeld dafür zu erpressen, dass man sie nicht zerstört. Fest steht: Unternehmen, in denen IT-Sicherheit auf mehreren Ebenen herrscht und Backups den stabilen Geschäftsbetrieb garantieren, überstehen letztlich auch Attacken größten Ausmaßes.

* https://csis.org/files/publication/130212_Lewis_RaisingBarCybersecurity.pdf

Was in Ihr Sicherheits-Toolkit gehört

Ironie des Schicksals: Hätte Sony das kleine Einmaleins der Sicherheit beherrscht, wäre der Daten-GAU dort höchstwahrscheinlich nicht passiert. Sollten Sie Grund zur Annahme haben, da draußen will jemand Ihrem Netzwerk und Ihnen ans Leder, dann studieren Sie in aller Ruhe das APT-Toolkit in diesem Leitfaden.

SolarWinds MSP unterstützt weltweit MSPs jeder Größe dabei, hocheffiziente und profitable Geschäftsfelder aufzubauen, die einen maßgeblichen Wettbewerbsvorteil sichern. Mit integrierten Lösungen, u. a. für Automatisierung, Sicherheit, Netzwerk- und Service-Management vor Ort und in der Cloud, können MSPs ihre Arbeit dank datenbasierter Einblicke schneller und einfacher erledigen. SolarWinds MSP hilft MSPs, sich auf das Wesentliche zu konzentrieren: die Erfüllung ihrer SLAs und den Aufbau eines gewinnbringenden Geschäfts.

RMEB00067DE0517

recycle

Weitere Informationen finden Sie auf **www.solarwindsmsp.com**

solarwinds msp

www.solarwindsmsp.com