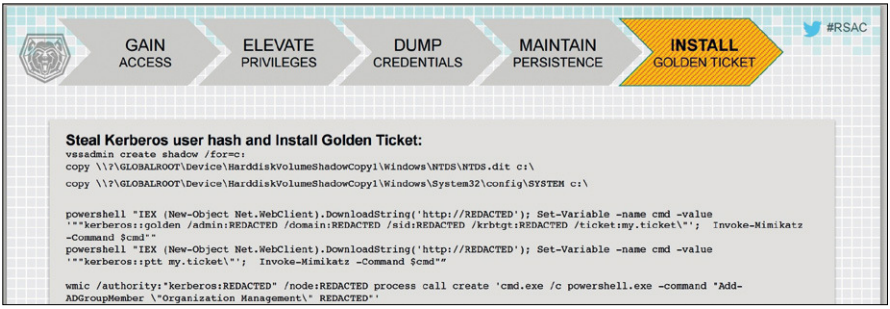
Sicherheit im Unternehmen

Hardware, Software, Anwendungen und Cloud-Dienste tragen zur IT-Sicherheit bei und verursachen andererseits selbst Sicherheitsprobleme. Wenn IT-Sicherheit nicht nur aus punktuellen Lösungen besteht, sondern ein ganzheitlicher Ansatz verfolgt wird, lässt sich das Risiko für Unternehmensnetze reduzieren. Dieses Kapitel wird Ihnen helfen, sich möglichst gut abzusichern. Wir liefern das Hintergrundwissen, um eine umfassende Security-Strategie für Ihr Unternehmen zu entwickeln.

Wie Kriminelle heute Unternehmen angreifen

Erfolgreiche Attacken auf Unternehmensnetze beruhen nicht auf den Programmierkünsten der Schadsoftware-Autoren. Bevor Malware zum Einsatz kommt, nehmen die Angreifer in aller Regel ein leicht verführbares Ziel ins Visier: die Mitarbeiter eines Unternehmens.

Das Muster scheint stets gleich: Erst werden einzelne Mitarbeiter eines Unternehmens per Spear-Phishing ihrer Login-Daten für Dienste im Unternehmensnetz beraubt. Anschließend werden mittels dieser Daten dann Arbeitsstationen und vor allem Rechner infiziert. Selbst für letzteres ist nicht immer Malware nötig, wie das Führungsteam der IT-Sicherheitsberater von **Crowdstrike** (*www.crowdstrike.com*) in einem Vortrag erläuterte: Nach dem Datenklau hangeln sich die Angreifer beispielsweise mittels gängiger Windows-Tools durch das Netzwerk.



› Keine Malware nötig: Bei einem von Crowdstrike analysierten Angriff kamen unter anderem die Windows Powershell und andere Windows-Tools zum Einsatz. (Quelle: Crowdstrike)

Der Vorteil: Der Aufruf dieser auf den attackierten Maschinen vorinstallierten Werkzeuge lässt die Antivirensoftware kalt. In einem von Crowdstrike beobachteten Angriff nutzten die Kriminellen beispielsweise unter anderem die Windows Powershell, wmic, vssadmin oder netdom, um sich nach und nach Zugang zu diversen Servern zu beschaffen. Dieses Treiben bleibt dann unter dem Radar der Sicherheitssysteme.

Alex Cox, leitender Mitarbeiter der Threat-Watch-Abteilung beim Verschlüsselungsspezialisten **RSA** (*www.rsa.com/de-de*), bestätigt, dass für den Einstieg ins Netzwerk zumeist Social Engineering verwendet wird. Neben dem Spear Phishing hat er auch verstärkt sogenannte Waterhole-Attacken gesehen. Dabei werden Webseiten infiziert, die die Mitarbeiter des zu attackierenden Unternehmens sehr wahrscheinlich frequentieren. Ein Besuch der Seite und ein nicht vollständig gepatchter Rechnern genügen, um die Maschine zu infizieren. Die dabei installierte Malware ist zum Absaugen der Daten nötig. Beispielsweise, um die Daten verschlüsselt per FTP nach außen zu transferieren. Per se ist das auch nichts Neues – aber es scheint immer noch zu funktionieren. Cox hat beobachtet, dass sowohl fertige Malware wie Poison Ivy oder Ghost zum Einsatz kommen. Aber auch eigens für den Angriff fabrizierte Schädlinge finden sich in der Praxis. Wenngleich diese im Vergleich zu ausgefuchster Online-Banking-Malware wie ZeuS oder Citadel vergleichsweise simpel gehalten ist und oft auch auf Verschleierungsmaßnahmen wie Packing verzichtet. Offenbar genügt eine so simple Malware, um die Aufgabe zu erledigen.

Social Engineering maßgeschneidert

Zwar sehen Fachleute wie Alex Cox nach wie vor bekannte Mechanismen zum Einbruch in die Netze: Vermeintlich von Unternehmen wie Amazon, Apple (iTunes) oder Google (Google Mail) stammende E-Mails mit Password-Reset-Links oder Links zu gefälschten Login-Seiten. Die hierzu verwendeten E-Mails seien inzwischen weitgehend frei von Rechtschreibfehlern und die infizierten Seiten beim Waterholing handverlesen. Bevor auch nur eine einzige Phishing-Nachricht versandt würde, hätten die Angreifer zuvor meist E-Mail- oder Chat-Konversationen im Unternehmen mitverfolgt, um überzeugendere Nachrichten formulieren zu können. Dem Verizon Data Breach Report zufolge liegt die Erfolgsrate beim Spear-Phishing bei gut elf Prozent. Jede zehnte Nachricht führt also zum Erfolg.

James Lyne, Chef-Malwareforscher bei **Sophos** (*www.sophos.com*), sagt für die kommenden Jahre sogar noch eine weitere Professionalisierung der Social-Engineering-Angriffe voraus. Der Grund: Immer höhere Codequalität in Anwendungen und Betriebssystemen sowie Schutzmechanismen wie der seit Windows 8.1 Update 3 verfügbare Control Flow Guard . Sie machen das Finden und Missbrau-

chen von Schwachstellen in Software schwieriger, so dass sich Angreifer laut Lyne auf das weichere Ziel „Mensch" konzentrieren.

Der Antiviren-Experte berichtet von einer Social-Engineering-Attacke, die selbst ihn beinahe hinters Licht führte: Ihn erreichte vor einer tatsächlich stattfindenden Geschäftsreise eine E-Mail, die vermeintlich von einem Kollegen stammte. Der Inhalt der Nachricht schlug ein Treffen vor Ort vor. Im Anhang: Eine Word-Datei mit der Beschreibung der Reiseroute des Kollegen und ein Vorschlag zum Treffpunkt. Das Word-Dokument hätte beim Öffnen mittels Makro die eigentliche Schadsoftware heruntergeladen, die dann – ganz ohne Exploit oder Admin-Rechte – die Maschine des Opfers übernommen hätte. Die Angreifer machten sich vor dem Versand der Spear-Phishing-Nachricht offensichtlich kundig, wo Lyne demnächst sein würde und mit wem er eventuell zusammenarbeitet.

Malware nicht zu verachten

Auch wenn bei Attacken auf Unternehmen die Social-Engineering -Komponenten eine wichtige Rolle spielen: Letztendlich muss auch immer Schadsoftware mit ins Spiel. Fachleute wie Lyne und Cox sagen zwar, dass die Qualität der Schädlinge oft nicht mit der von Banking-Malware mithalten kann. Aber sie sehen dennoch ausgefuchste Mechanismen. So weiß James Lyne von diversen Schädlingen, die über dynamisch verschlüsselte Kanäle (Command & Control) Kontakt halten zu ihrem „Mutterschiff". Hiermit hätten so gut wie alle Intrusion-Detection-Systeme in Unternehmen immense Probleme.

Und auch die Hersteller von Antiviren-Software hätten ihre liebe Mühe, da Analysen solcher Malware sehr aufwändig seien. Zum einen machen es die verschlüsselten Kanäle schwer. Zum anderen schützt sich die Malware selbst auch gegen gängigen Analysemethoden der Malware-Forscher. Selbst absolute Profis könnten bei manchen Infektionen zwar den Befall feststellen – jedoch nicht, welche Daten abgeflossen sind.

Cloud: Problem oder Lösung?

Die Fachleute sind sich einig: Insbesondere für kleinere und mittlere Unternehmen kann die Cloud entscheidend zum Erhöhen der Sicherheit beitragen. Denn in aller Regel haben die Anbieter eigene IT-Sicherheitsmannschaften, deren Expertise über das hinausgeht, was bei den Kunden zu finden ist. Dazu kommt, dass Unternehmensnetze unter anderem auch deswegen leicht(er) angreifbar sind, weil allzu oft die gleichen Komponenten (Betriebssystem, Firewall, Antivirensoftware etc.) ver-

wendet würde. Finden sich in diesen Bauteilen Lücken, können Angreifer quasi nach Anleitung in Netze auf der ganzen Welt eindringen. Bei Cloud-Providern finden sich keine derart homogenen Landschaften.

Alan Kessler gibt jedoch zu bedenken, dass Cloud-Kunden nicht nur auf die Zugriffsreche der eigenen, sondern auch die die der Administratoren beim Anbieter achten müssen. Zudem gilt: Verschlüsselungs-Keys dürfen niemals das Unternehmen des Kunden verlassen. Dann sei laut Kessler selbst ein US-Cloud-Anbieter in Ordnung. Denn die US-Regierung kann vom Provider dann auch mit Druck kein Material zum Entschlüsseln der Daten bekommen.

Grundsätzlich gelte bei der Auswahl eines Anbieters: Ist im eigenen Unternehmen nur wenig IT-Sicherheitsfachwissen vorhanden, dann sind SaaS (Software as a Service)-Provider die beste Wahl. Bare-Metal-Provider empfehlen sich nur für Fachleute. Zum Ermitteln des eigenen Risiko-Profils hat die Cloud Security Alliance (CSA, *https://cloudsecurityalliance.org*) diverse Werkzeuge auf ihrer Webseite parat. Unternehmen mit hohem Risikoprofil sollten beispielsweise unbedingt ein eigenes Key-Management-System für ihre Cloud-Dienste einsetzen.

› James Lyne, Leiter der weltweiten Sicherheitsforschung bei Sophos, sieht Social Engineering als großes Problem für Unternehmen. (Foto: Uli Ries)

› Die drohende Überforderung

Diese Werkzeuge könnten laut James Lyne viele kleinere Unternehmen jedoch überfordern. Insbesondere dann, wenn sie in Kontakt stünden mit großen Anbietern. Denn von außen sei es sehr schwer, deren Sicherheitskompetenz zu prüfen. Von daher empfiehlt auch Lyne, so viel wie möglich zu verschlüsseln. Nicht nur auf Dateisystemebene, sondern möglichst schon in der Anwendung. Wer selbst Anwendungen entwickelt, solle zum Verschlüsseln unbedingt auf fertige Frameworks zurückgreifen und sich aufgrund des komplexen Themas keinesfalls selbst daran versuchen.

Außerdem sehe der Malware-Spezialist einen Vorteil, wenn Kunden alle Schutzmechanismen aus einer Hand bezögen. Best-of-Breed sei nur für Konzerne handhabbar. Er empfiehlt kleineren und mittleren Unternehmen Lösungen, die sowohl auf den Endpunkten im Netzwerk, als auch auf dem Weg in die Cloud – und aus dieser zurück ins Unternehmensnetz – nach Gefahren und Anomalien suchen. Kombiniere man dies dann noch mit einem Dienstleister, der sich der Log-Analyse annimmt,

ergebe sich ein wirksamer Schutzwall, so Lyne. Beim Thema Datenbankverschlüsselung sehe es den Fachleuten zufolge leider nicht so rosig aus. Zwar würde seit Jahren an der homomorphen Verschlüsselung gearbeitet. Mit ihr lassen sich die Inhalte von Datenbanken in der Datenbank selbst verschlüsseln und beim Zugriff einer Anwendung wieder entschlüsseln. Noch befänden sich aber alle Anstrengungen im Entwicklungsstadium, kommerzielle Produkte seien noch keine in Sicht.

Abhilfe gegen den Datenklau

Angesichts des professionellen Vorgehens der Angreifer scheint es unausweichlich, dass ein Netzwerk kompromittiert wird. Und was dann? Laut Alan Kessler, President und CEO von **Vormetric** (*www.vormetric.com*), hielten laut eines Reports über 50 Prozent der Befragten die bewährten Produkte für Data Breach Prevention- für hinreichend. Bislang würden sie laut Kessler hauptsächlich verwendet, um Auditoren glücklich zu machen.

Inzwischen setzt sich die Erkenntnis durch, dass das Vermeiden von negativen Folgen, wie es solche Produkte ebenfalls böten, nach dem unvermeidlichen Einbruch wichtiger ist denn je. Laut Kessler sei ein vollständiges Absichern des Perimeters ohnehin utopisch. Daher müsse gelten: „Es ist leichter, die Lebensmittel im Haus vor dem Einbrecher zu verstecken, als das Haus hermetisch zu verrammeln."

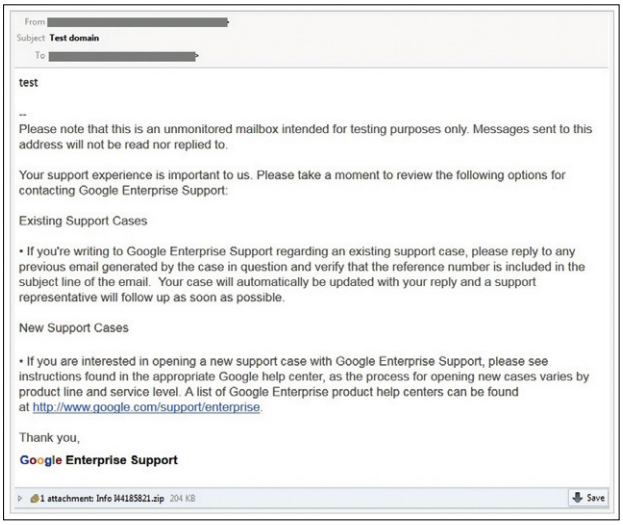
Sinnvollerweise entscheidet eine Data Leakage Prevention (DLP)-Lösung pro Nutzer und Datensatz, welche Aktionen erlaubt und welche zu unterbinden sind. Zeitgleich kann man die Rechte von Administratoren beschneiden. Laut Kessler greifen die gängigen Lösungen auf das „Least Privilege"-Prinzip zurück. Dieses sei sowohl auf Betriebssystemebene (Filesystem), als auch in der Anwendung durch zu setzen.

Zu diesem Pflichtprogramm kommt noch die Kür: das Überwachen der Zugriffe und das Erkennen von Anomalien. Weicht nach einem erfolgreichen Angriff das Verhaltensmuster einzelner Anwender oder Maschinen vom bisher gewohnten ab, schlägt die DLP-Lösung Alarm. Wurden zuvor Zugriffsrechte per Least Privilege vergeben, erleichtert dies das Erkennen von Anomalien und auch das zeitraubende Analysieren von Logfiles.

› Technik: Nur ein Teil der Lösung

Schutzmechanismen wie DLP sorgen aber keinesfalls für umfassenden Schutz. Sie mindern zwar das Risiko, kämpfen auf verlorenem Posten, wenn Kollege Mensch nicht ebenfalls auf der Hut ist. Und genau hier sehen die Fachleute in der Praxis die größten Lücken: Nur in wenigen Unternehmen sähen sie Aufklärungskampagnen,

die Mitarbeiter – am besten fortlaufend – über neue Angriffsmaschen informieren würden. Ohne das Wissen, wie eine Spear-Phishing-Kampagne aussieht und welche Raffinesse dabei an den Tag gelegt wird, hätten Mitarbeiter gute Chancen, zu Opfern einer solchen Kampagne zu werden.


From: [redacted]
Subject: **Test domain**
To: [redacted]

test

--
Please note that this is an unmonitored mailbox intended for testing purposes only. Messages sent to this address will not be read nor replied to.

Your support experience is important to us. Please take a moment to review the following options for contacting Google Enterprise Support:

Existing Support Cases

• If you're writing to Google Enterprise Support regarding an existing support case, please reply to any previous email generated by the case in question and verify that the reference number is included in the subject line of the email. Your case will automatically be updated with your reply and a support representative will follow up as soon as possible.

New Support Cases

• If you are interested in opening a new support case with Google Enterprise Support, please see instructions found in the appropriate Google help center, as the process for opening new cases varies by product line and service level. A list of Google Enterprise product help centers can be found at http://www.google.com/support/enterprise.

Thank you,

Google Enterprise Support

1 attachment: Info 144185821.zip 204 KB Save

› Gut gemacht: Eine vermeintlich vom Google Enterprise Support stammende, fehlerfrei formulierte Nachricht bringt ein infiziertes Attachment mit. (Quelle: Cyren)

Aber nicht nur die Kollegen in den Fachabteilungen benötigen Wissen. Auch die IT-Mitarbeiter selbst müssten laut RSA-Sprecher Alex Cox besser geschult werden. Denn ohne tiefgehendes Fachwissen seien moderne Schutzmechanismen gar nicht sinnvoll nutzbar. Auch fehle es so gut wie immer an der Expertise, die Wirkweise einer von der Software entdeckten Malware zu analysieren. Allzu oft würde zudem der Kardinalsfehler begangen: Das sofortige Säubern der infizierten Endgeräte. Damit nähmen sich Unternehmen laut Cox jegliche Chance, mehr über die Hintermänner beziehungsweise die erbeuteten Daten zu erfahren. Fehlt dieser Einblick, ist die nächste, noch wirksamere Spear-Phishing-Kampagne so gut wie sicher. Denn niemand im Unternehmen weiß, welche der eigenen Daten für die nächste Attacke missbraucht werden.

Uli Ries