Trend Micro Forschungsbericht

Empfehlungen für den Kampf gegen zielgerichtete Angriffe

Autor: Jim Gogolinski

Forward-Looking Threat Research Team

Inhalt

Einleitung

Dieses Forschungspapier stellt dar, wie Unternehmen ihr Netzwerk konfigurieren können, um eine Durchdringung für Angreifer zu erschweren bzw. diese leichter entdecken zu können. Des Weiteren geht es um die erforderlichen Vorbereitungen für den Umgang mit einer Infektion. Denn angesichts der zunehmend fortschrittlichen Vorgehensweise von Angreifern ist es für Unternehmen eher unwahrscheinlich, diese hochmotivierten und gleichzeitig geduldigen Gegner aus ihren Netzwerken heraushalten zu können . In den meisten Fällen können die Opfer nur hoffen, dass sie zielgerichtete Angriffe frühzeitig entdecken und den Zugriff auf möglichst viele, für Angreifer interessante Informationen einschränken.

Unternehmen muss es bewusst sein, dass der Umgang mit einem zielgerichteten Angriff kostspielig ist. Um mit einer Infektion fertig zu werden, müssen die Opfer mit monatelanger konzentrierter Arbeit eines dafür abgestellten Response Teams rechnen. Die Voraussetzung dafür, dass dieses Team effiziente Arbeit leisten kann, ist eine Netzwerkkonfiguration, die alle vom Team benötigten forensischen Daten liefern kann.

Vor den eigentlichen Detailinformationen gibt das Papier eine Definition von zielgerichteten Angriffen und beschreibt den typischen Ablauf eines Eindringversuches. Zudem werden Möglichkeiten aufgezeigt, warum eine Organisation abgesehen von seinem geistigen Eigentum Ziel solcher Angriffe werden könnte.

Das Forschungspapier gibt auch Empfehlungen zu Netzwerkwerkzeuge und Konfigurationen, die es einem Angreifer erschweren, ein Netzwerk zu durchdringen, und auf der anderen Seite dem Unternehmen dabei helfen, seine kritischen Ressourcen zu schützen. Des Weiteren wird die Arbeit von Response Teams bei der Untersuchung von Angriffen und der Säuberung beleuchtet sowie die Rolle von Erkenntnissen über Bedrohungen dargestellt.

Schließlich liefert das Forschungspapier Begründungen für den Einsatz von Penetrationstests im eigenen Netzwerk.Geeignete Tools und die Einführung einer “Custom Defense”-Strategie unterstützt Unternehmen in ihrem Kampf gegen zielgerichtete Angriffe.

Zielgerichtete Angriffe

Definition eines zielgerichteten Angriffs

Es gibt verschiedene Arten von Angriffen auf Computernutzer. Als Klassifizierungskriterium gilt beispielsweise die Absicht, die Angreifer bei der Wahl ihres Zieles haben, etwa um sich finanzielle Vorteile zu verschaffen. Bei einer solchen Attacke versucht der Eindringling entweder an Zugangsdaten für Online Banking-Konten heranzukommen, oder er sucht einen anderen Weg, um von seinem Opfer Geld zu bekommen (z.B. durch die Installation von Ransomware auf dem Computer des Nutzers).[1]

Unternehmenssysteme können ebenfalls monetäre Begehrlichkeiten wecken, denn entwendete Datenbanken etwa mit Kontaktinformationen lassen sich an Spammer oder andere Cyberkriminelle veräußern. Computer werden zum Angriffsziel, um sie einem Botnet hinzuzufügen, über das Cyberkriminelle eine große Gruppe infizierter Systeme aus der Ferne kontrollieren können.

Ein zielgerichteter Angriff ist eine langfristige Cyberspionage-Kampagne gegen eine Organisation. Die Angreifer haben die Absicht, sich einen permanenten Zugang zum Netzwerk des Opfers zu verschaffen. Dadurch haben sie die Möglichkeit, vertrauliche Unternehmensdaten abzuziehen und eventuell „logische Bomben“ zulegen, die das Netzwerk und die Infrastruktur beschädigen können. Ist die anvisierte Organisation mit dem Betrieb einer kritischer Infrastruktur beschäftigt, sind die Auswirkungen sind noch schlimmer. Ein dauerhafter Zugang erlaubt es Angreifern auch, die Infrastruktur des Opfers als Plattform für nachfolgende Angriffe auf andere Organisationen zu missbrauchen. Der Vorteil für die Kriminellen besteht darin, dass die neuen Versuche so den Anschein von Legitimität erhalten (z.B. von einem vertrauenswürdigen Partner kommen). Darüber hinaus lassen sich infizierte Netzwerke als Zwischenstopp im Rahmen von Angriffen auf andere Organisationen nutzen, um Spuren besser verwischen zu können.

Gründe für Angriffe auf Unternehmen

Bei Cyberspionage denken die meisten an Regierungsbehörden und die Verteidigungsbranche als Primärziele. Das ist auch richtig, aber viele andere Industrien wie Pharma, Petrochemie, Versorgungswesen, Fertigung und Bergbau sind ebenfalls attraktive Opfer. Andere Ziele sind nicht so offensichtlich, etwa Anwaltskanzleien, Think Tanks oder Menschenrechtsorganisationen. Mit anderen Worten, kein Unternehmen ist vor zielgerichteten Angriffen sicher.

1 Trend Micro Incorporated. (2013). Threat Encyclopedia. “Ransomware.” Last accessed August 29, 2013, http://about-threats.trendmicro.com/us/definition/ransomware/index.html

Industriespionage kann in einem Unternehmen großen Schaden anrichten, denn Unternehmensdaten können genauso wertvoll sein wie militärische Daten. Es ist beispielsweise viel einfacher und günstiger, die Ergebnisse jahrelanger Forschungsarbeit zu stehlen als selbst zu forschen. Damit kann eine Organisation, die sich in einem neuen Bereich etablieren will, viel günstigere Preise anbieten, schließlich musste sie keine Kosten für Forschung und Entwicklung aufbringen. Wird zudem bekannt, dass eine Organisation einem solchen Angriff zum Opfer gefallen ist, schmälert das Vertrauen der Investoren und führt zu fallenden Aktienkursen oder möglichen Gerichtsverfahren.

Ein Unternehmen mag für Cyberkriminelle nicht nur wegen der eigenen Produkte oder Informationen ein interessantes Ziel sein, sondern etwa wegen dessen Verbindungen zu dem eigentlichen Angriffsziel. Den Einbruch in Netzwerke über Schwachstellen und das Ausschnüffeln von Systemen innerhalb des Netzwerks oder auch „Island Hopping" gibt es schon seit Jahren.[2]

Gleiches gilt für das Eindringen in Organisationen. Ein Unternehmen, dessen Sicherheit weniger streng gehandhabt wird, und das auf irgendeine Weise mit dem eigentlichen Ziel in Verbindung steht, kann angegriffen und dazu genutzt werden, um Zugang zu dem besser abgeschotteten Ziel zu erlangen. Value Added Resellers (VARs) haben häufig Zugang zu den Netzwerken von Unternehmen, denen sie Produkte oder Dienstleistungen liefern. Ein Unternehmen mag vielleicht nur einfaches Zubehör herstellen, verkauft dieses aber an große Integratoren, die es in ihren Produkten verwenden Auch gibt es in diesen Firmen Mitarbeiter, die zu denselben Gruppen gehören, wie einige Mitarbeiter aus dem Zielunternehmen. Angreifer nutzen die Infrastruktur, hauptsächlich über kompromittierte Mail-Konten und den Verbindungen zum „tatsächlichen" Ziel, um einfacher Zutritt zu letzterem zu erlangen. Erinnert sich ein Mitarbeiter etwa vage daran, in der Vergangenheit bereits mit dem Absender der Mail zusammengearbeitet zu haben, so ist es wahrscheinlicher, dass er dieser E-Mail vertraut, speziell dann, wenn sich der Inhalt auf die Zusammenarbeit bezieht.

2 Trend Micro Incorporated. (2013). "Trend Micro™ Intrusion Defense Firewall." Last accessed September 13, 2013, http://www.trendmicro.com/cloud-content/us/pdfs/business/datasheets/ds02_osce.pdf

Typische Zeitschiene und Beispiele aus der Praxis

Sobald ein Unternehmen Ziel eines Einbruchversuchs geworden ist, muss es sich darauf einstellen, dass diese Versuche solange wiederholt werden, bis einer erfolgreich ist. Doch auch ein erfolgreicher Einbruch ins Netzwerk bedeutet nicht unbedingt, dass die Angriffe aufhören. Es gibt Gründe dafür, dass Angreifer auch nach einem Erfolg weitermachen: Zum einen könnte der Einbruch entdeckt und damit dieser Verbindungsweg verschlossen werden. Mit einem zweiten Eintrittspunkt wäre man hier abgesichert. Zum anderen kommt es vor, dass verschiedene Teams oder Untergruppen derselben kriminellen Organisation versuchen, sich zum selben Netzwerk Zutritt zu verschaffen. Unter Umständen suchen diese Gruppen unterschiedliche Informationen und merken gar nicht, dass andere bereits dieselbe Einheit im Visier haben.

Ein typischer Angriff beginnt häufig mit einem Spear-Phishing-Versuch.[3] Die Kriminellen senden Spear-Phishing-Mails üblicherweise an eine kleine Gruppe von Mitarbeitern gesendet. Sie sind täuschend echt gestaltet, sodass sie den Empfängern glaubwürdig erscheinen. Sie tarnen sich als Nachricht von einem Absender, von dem eine Mail nicht unwahrscheinlich ist, etwa von dem Vorgesetzten oder einem Kollegen. Die Mails beinhalten häufig einen Link auf eine bösartige Website oder einen Anhang mit bösartigem Inhalt. Der Anhang kann eine Sicherheitslücke u. a. in Microsoft™ Word®, Excel® oder in einem Adobe®-Produkt ausnutzen. Beliebt sind auch .ZIP-Dateien, die den Empfänger beim Öffnen in dem Glauben lassen, ein Dokument vor sich zu haben. Tatsächlich handelt es sich aber um eine ausführbare Datei, die das System des Opfers missbraucht, falls der Empfänger die scheinbar harmlose Datei öffnet. Zumeist merkt er gar nicht, was tatsächlich passiert ist. Angreifer können dieselben Techniken auch für Attacken auf private Mail-Adressen eines Nutzers anwenden, weil Angestellte häufig sowohl private als auch geschäftliche Nachrichten auf ihren Arbeitscomputern abrufen.

Neben Spear-Phishing-Mails nutzen Kriminelle aber auch andere Mittel, um sich Zutritt zu einem Netzwerk zu verschaffen. Alle Computer, die Verbindung nach draußen haben, können nach Sicherheitslücken überprüft werden. Auch lassen sich Social Engineering-Techniken einsetzen, um in eine Organisation einzudringen, bösartige Software zu installieren, nach offenen Wireless Access Points (WAPs) zu scannen oder die eigenen WAPs ins Netzwerk einzuschleusen. Eine andere Taktik besteht beispielsweise darin, einen mit bösartigem Inhalt versehenen USB-Stick auf dem Parkplatz des Ziels abzulegen und darauf zu setzen, dass ein neugieriger Mitarbeiter ihn an sich nimmt und mit seinem Computer verbindet, um zu sehen, wem er gehört und was sich darauf befindet.

3 TrendLabsSM APT Research Team. (2012). "Spear-Phishing Email: Most Favored APT Attack Bait." Last accessed September 2, 2013, http://www.trendmicro.com/cloud-content/us/pdfs/security-intelligence/white-papers/wp-spear-phishing-email-most-favored-aptattack-bait.pdf

Unabhängig davon, wie eine bösartige Software ins Netzwerk gekommen ist, versucht sie, Verbindung zu einem Command-and-Control (C&C)-Server aufzunehmen, um weitere Anweisungen zu empfangen. Die Software versucht, entweder gleich die Kommunikation zu initiieren oder verhält sich stundenlang ruhig, um nicht aufzufallen.

Sobald die Software auf den C&C-Server zugreift, passiert Verschiedenes: Es gibt die so genannten „Downloader", die versuchen, zusätzliche Malware automatisch herunterzuladen und zu installieren. Eine andere Möglichkeit: Die Software kommuniziert mit dem C&C-Server. Eine Person, die den C&C-Server überwacht, bemerkt die neue Verbindung und startet eine bestimmte Aktion. Diese Art von Software, auch als Remote Access Trojan (RAT) bekannt, ermöglicht es den Hintermännern beispielsweise, ein System zu untersuchen, Dateien zu extrahieren, neue Dateien herunterzuladen und auf dem infizierten System auszuführen, die Video-Kamera und das Mikrofon einzuschalten, Screenshots und Tasteneingaben festzuhalten oder eine Command Shell auszuführen.

Als Nächstes versucht der Feind, das kompromittierte Netzwerk zu durchdringen, um weitere dauerhafte Zugangspunkte zu finden oder nach wertvollen Daten zu suchen. Dabei entwenden die Eindringlinge alle Zugangsdaten, deren sie habhaft werden können, um damit Zugriff auf zusätzliche Systeme und Daten im Netz zu erlangen. Die gesammelten Daten transferieren sie aus dem Netzwerk an einen anderen Speicherort, von wo aus sie die Sammlung zur weiteren Untersuchung in ihre eigene Umgebung bringen können.

Die erste Reaktion des Eindringlings auf den Kontakt mit der Angriffssoftware erfolgt zumeist sehr schnell. Die nächsten Schritte aber folgen nur langsam, um möglichst unentdeckt zu bleiben. Bei dem Verdacht enttarnt worden zu sein können die Feinde wochen- oder monatelang untätig abwarten, bevor sie ihre Aktivitäten wieder aufnehmen. Gelingt es einer Organisation diesen Eindringling komplett aus dem Netzwerk zu entfernen, so startet er den Zyklus wieder von vorne.

Es gibt einige bekannte Beispiele für zielgerichtete Angriffe, wie etwa die Google Aurora-, ShadyRAT-, DUQU- und FLAME-Attacken sowie den erst kürzlich erfolgten zielgerichteten Angriff auf Saudiarabien.[4]

4 Valerie Boquiron. (January 19, 2010). *TrendLabs Security Intelligence Blog.* "Cyber Attacks on Google and Others—Who Is Really at Risk?" Last accessed September 2, 2013, http://blog.trendmicro.com/trendlabs-security-intelligence/cyber-attacks-on-google-and-others-who-is-really-at-risk/; Nart Villeneuve. (January 26, 2012). *TrendLabs Security Intelligence Blog.* "Top APT Research of 2011 (That You Probably Haven't Heard About)." Last accessed September 2, 2013, http://blog.trendmicro.com/trendlabs-security-intelligence/top-apt-research-of-2011-that-you-probably-havent-heard-about/; Karl Dominguez. (November 2, 2011). *TrendLabs Security Intelligence Blog.* "Zero-Day Exploit Used for DUQU." Last accessed September 2, 2013, http://blog.trendmicro.com/trendlabs-security-intelligence/zero-day-exploit-used-for-duqu/; Trend Micro Incorporated. (May 31, 2012). *TrendLabs Security Intelligence Blog.* "Update on FLAME." Last accessed September 2, 2013, http://blog.trendmicro.com/trendlabs-security-intelligence/update-on-flame/; Kelly Jackson Higgins. (August 22, 2012). *Dark Reading.* "Shamoon, Saudi Aramco, and Targeted Destruction." Last accessed September 11, 2013, http://www.darkreading.com/attacks-breaches/shamoon-saudi-aramco-and-targeted-destru/240006049.

Infrastruktur

Was ein Unternehmen dagegen tun kann

Ohne eine geeignet konfigurierte Infrastruktur, haben Unternehmen keine Chance, sich vor zielgerichteten Angriffen zu schützen. Eine solche Netzwerkkonfiguration bringt kurzfristig zwar keine finanziellen Vorteile, im Gegenteil sie erhöht wahrscheinlich die IT-Gesamtkosten. Doch müssen diese Mehrkosten gegen die Aufwände bei einem Einbruch und dem Diebstahl wertvoller Informationen gegeneinander aufgewogen werden.

Segmentierung

Unternehmen sind gut beraten, ihre Netzwerke in so viele sinnvolle Segmente wie nötig zu unterteilen. Ein Netzwerksegment kann beispielsweise aus einer Ansammlung von Workstations, Servern, Druckern und weiteren Geräten bestehen, die aufeinander zugreifen können. In einem privaten Netzwerk oder einem einfachen Unternehmensnetzwerk liegen alle Komponenten einer Infrastruktur normalerweise in einem einzigen Segment. Doch jedes komplexere Netzwerk sollte in logische Segmente unterteilt sein. Diese werden durch Firewalls voneinander abgeschirmt, die den im Segment ankommenden und abgehenden Netzwerkverkehr kontrollieren. Die Segmente stellen also eine Reihe sicherer Räume innerhalb eines großen offenen Gebäudes dar. Sind diese Räume nicht vorhanden, kann jeder, der das Gebäude betritt, auf alles innerhalb der Außenmauern zugreifen. Die sicheren Räume hingegen erschweren es Eindringlingen, sich Zugang auf das komplette Netzwerk zu verschaffen. Das Gleiche gilt auch für Mitarbeiter, die auf Daten zugreifen wollen, für die sie keine Berechtigung haben.

Netzwerke sollten in so viele logische Segmente wie möglich unterteilt werden. Als Kriterium für eine Unterteilung kann beispielsweise die Funktion (Finanzabteilung, Marketing, Engineering, Vertrieb usw.) darstellen. Eine andere Möglichkeit ist die Segmentierung nach geografischem Standort oder Sicherheits-Level (z.B. unclassified, classified, secret, top secret oder PII -- Personally Identifiable Information). Jedes einzelne Segment wird so sicher wie möglich gestaltet, mit einer Firewall, die einen nicht autorisierten Zugriff auf Systeme verhindert. Das bedeutet im Normalfall, dass etwa eine Maschine im Marketing-Netzwerk keinen direkten Zugriff auf das Engineering-Netzwerk haben sollte und auch der Zugriff vom Engineering-Netzwerk aus auf das Finanz-Netzwerk nicht möglich sein sollte.

Logging

Logging und Log-Analysen sind Schlüsselmethoden, die beim Aufdecken eines Einbruchs helfen. Auch unterstützen sie das Response-Team dabei zu verstehen, wohin die Angreifer im Netzwerk gehen und wonach sie suchen. In einer großen Unternehmensumgebung liefern die Logging-Daten zudem Einblicke in die Aktivitäten und den Zustand des Netzwerks. Aufmerksame Analysten, die das tägliche Auf und Ab des Datenflusses im Netz kennen, können schon frühzeitig eine zielgerichtete Attacke erkennen und reagieren, bevor die Angreifer sich im Netzwerk festsetzen. Anderenfalls sind die Log-Daten häufig das Einzige, was dem Response-Team für seine forensische Analyse zur Verfügung steht. Natürlich müssen Logs aktiv überwacht werden, und dafür bedarf es Werkzeuge, wie Security Information and Event Management (SIEM)-Systemen.

Welche Arten der Informationen sollten Unternehmen aufzeichnen? Verwendet die Organisation Network Address Translation (NAT), sollten die Einträge zum internen Mapping auf physische Maschinen aufbewahrt werden. Es bringt nämlich nichts zu wissen, dass 192.168.1.27 auf einen bekannten C&-Server zugegriffen hat, wenn jede Maschine in einem großen Subnetz die mit NAT umgewandelte Adresse genutzt haben kann. Auch Web-Proxy und Domain Name System (DNS)-Anfragen sollten aufgezeichnet werden, desgleichen Nutzerzugriffe (sowohl An- als auch Abmeldung) – physische, über Remote Desktop Protocol (RDP), Virtual Private Network (VPN) und andere. Das Logging von externem und internem Netzwerkverkehr ist ebenfalls zu erwägen, wenn es gesetzliche oder vernünftige Gründe dafür gibt. Lassen sich keine Full Packet Captures (pcaps) speichern, so sollten zumindest die Datenflüsse im Netzwerk aufgezeichnet werden. E-Mails mit den vollständigen Headern und Anhängen sollten für eine längere Zeit archiviert werden. Zudem sollten Firewall-Regeln aufgezeichnet werden, denn sie umfassen eine Vielfalt an Informationen über welche Systeme versucht wurde, Angriffe über Nicht-Standardports zu initiieren..

Logging sollte auf hohem "Verbose"-Level aufgesetzt sein, denn es ist besser, zuviel Information zu haben, als Schlüsseldaten zu verpassen. Idealerweise sollten alle Systeme in einer Organisation ihre Uhren mit einem zentralen Zeit-Server synchronisieren, sodass die Zeitstempel aller Log-Dateien über alle geografischen Bereiche einer Zone identisch sind.

Log-Daten sollten außerdem innerhalb einer Organisation zentral vorgehalten werden. Organisationen mit Netzwerken in verschiedenen geografischen Regionen müssen ein vernünftiges Maß an Zentralisierung festlegen sowie eine Möglichkeit, bei Bedarf alle Logs schnell von einem zentralen Ort zu erhalten.

Unternehmen sollten die Daten so lang wie möglich aufbewahren, aber zumindest ein Jahr lang nach Aufzeichnung müssen sie sofort zugänglich sein. Die meisten Logs sind textbasiert und können daher für die Langzeitaufbewahrung einfach komprimiert werden. Für den Fall, dass es einem Angreifer gelingt, auf ein zentrales Logging-System zuzugreifen, sollte ein Backup der Logs offline gespeichert sein.

Beim Aufsetzen der Logging-Strategie ist es wichtig zu beachten, die Daten in einem Format zu speichern, das sich einfach durchsuchen lässt und Korrelationen erlaubt. Eine Datei mit Werten, die durch Komma getrennt sind (.CVS), kann einfach durchsucht und geparst werden. Viele Geräte loggen standardmäßig in ein Binärformat. Wenn möglich, sind die Geräte so zu konfigurieren, dass sie in Klartext schreiben. Ist das nicht machbar, so können im Rahmen eines Prozesses die Daten in ein Textformat exportiert werden.

Obwohl die fachgerechte Konfiguration einer Logging-Infrastruktur etwas höhere Kosten mit sich bringt, zahlt sich das mehrfach aus, wenn nur ein einziger zielgerichteter Angriff damit abgewehrt wird. Eine Untersuchung läuft viel schneller ab, wenn über eine Suche in den DNS-Logs Maschinen aufgedeckt werden können, die versucht haben, auf bösartige C&C-Server zuzugreifen. Interne IP-Adressen können dann mit einzelnen Maschinen im Netzwerk in Verbindung gebracht werden. Sobald diese Maschinen identifiziert sind, können sie die Netzwerk-Verkehrsfluss-Logs anderer Maschinen, auf die zugegriffen wurde, durchsuchen. Die Verfügbarkeit dieser Daten erlaubt kürzere und schnellere Recherchen und senkt so die Wiederherstellungskosten.

Manche Experten sind der Meinung, Logging erfordere zuviel Speicherplatz. Doch angesichts der sinkenden Kosten für Speicher und den hohen Aufwänden für die Ressourcen für Analysen können es sich Organisationen nicht leisten, auf Daten zu verzichten. Zumindest sollten die Daten der letzten drei Monaten unkomprimiert aufbewahrt werden, alle restlichen Daten können komprimiert und archiviert werden. Auch in der Archivierungsstrategie ist es wichtig darauf achten, Daten in einer vernünftigen Kurzzeitarchivierung vorzuhalten, um deren Dekomprimierung und Durchsuchung zu erleichtern.

Nutzerkonten und Workstations

Grundsätzlich wollen Nutzer auf alles zugreifen können und überall hingehen dürfen – auch wenn sie für den Moment diesen Zugriff nicht brauchen. Häufig sind sie es von zu Hause gewöhnt, ihre Computer selbst zu verwalten und jede gewünschte Software installieren zu können. Leider sind diese „Privilegien" auf die Unternehmensumgebung nicht übertragbar. Es mag für die IT-Abteilung mehr Aufwand bedeuten, Nutzer dazu zu zwingen, den Zugriff auf neue Datenquellen zu beantragen, doch langfristig wird damit die Umgebung viel sicherer.

Wie bereits erwähnt, versuchen Eindringlinge so viele Zugangsdaten wie möglich abzugreifen. Deshalb sollten IT-Sicherheits-Teams dies soweit als möglichst erschweren und gleichzeitig sicherstellen, dass jedes kompromittierte Konto möglichst wenige Rechte und Zugriffsmöglichkeiten hat. Damit lässt sich ein potenzieller Schaden minimieren. Gelingt es nämlich einem Angreifer, gültige Kennwort-Hashes zu stehlen, so gibt es keinen Schutz vor Pass-the-Hash-Techniken.[5]

Die hier vorgestellten Regeln bezüglich Nutzerkonten und Workstations erhöhen garantiert nicht die Beliebtheit des IT-Teams bei den Mitarbeitern und führen zudem zu mehr Arbeit für die Teams. Sie müssen sich um nicht vermeidbare Probleme kümmern. Doch auch hier gilt es, diesen Mehraufwand gegen die Kosten bei Datenverlust und Wiederherstellung abzuwägen.

Nutzerkonten sollten im Least-Privilege-Modell laufen, sichere Kennwörter und -- wenn möglich -- die Zwei-Faktor-Authentifizierung fordern. Kennwörter sollten regelmäßig geändert werden und deren Wiederverwendung für mehrere Konten (z.B. Domänen- und VPN-Login) untersagt sein. Empfehlenswert ist es auch, die Kennwörter mit Rainbow-Listen zu vergleichen und diejenigen, die nicht auf den Listen sind, mit Passwort-Cracking-Software zu prüfen. Die Nutzer, deren Kennwörter in den Listen gefunden oder geknackt wurden, sollten gezwungen werden, diese sofort zu ändern. Zudem sollten lokale Administratorenkonten deaktiviert oder entfernt werden, sowie Zugangsdaten von Domän-Administratoren niemals im Cache vorgehalten werden dürfen. Ist ein Administratorenzugriff erforderlich, sollte dieser remote erfolgen. Nach Beendigung der Arbeit empfiehlt es sich, die Maschine neu gestartet werden. Die Kennwortregeln sollten nach einer Reihe von fehlgeschlagenen Versuchen das Aussperren des Kontos mit langen Reset-Zeiten vorsehen. Möglicherweise könnte der ausgesperrte Nutzer auch dazu gezwungen werden, den Helpdesk zur Freischaltung des Kontos anzurufen.

5 Bashar Ewaida. (January 21, 2010). "Pass-the-Hash Attacks: Tools and Mitigation." Last accessed September 11, 2013, http://www.sans.org/reading-room/whitepapers/testing/pass-the-hash-attacks-tools-mitigation-33283?show=pass-the-hash-attacks-tools-mitigation-33283&cat=testing

Workstations sollten nach Möglichkeit vor unbefugten Zugriffen gesperrt sein. Jeder Computer sollte zudem immer die aktuellste Software-Version installiert und das vollständige Logging aktiviert haben. Wenn die Umgebung es zulässt, sollten die Verantwortlichen eine Whitelist-Lösung für Nutzer-Workstations und Laptops erwägen. Das Trend Micro™ OfficeScan™ Intrusion Defense Firewall-Plugin verwendet beispielsweise Kontrollfilter für Anwendungen, um Systemadministratoren bei bestimmtem Datenverkehr (Instant Messaging, Medien-Streaming) zu benachrichtigen oder um diesen zu blockieren und die „schlechten" Daten so aus dem geschäftskritischen Datenverkehr herauszufiltern.[6] Zudem empfiehlt sich der Einsatz Werkzeugen zur Integritätsüberwachung, um Änderungen an Dateisystemen und Registries zu erkennen.

Eine weitere Überlegung wäre der Einsatz spezieller Monitoring-Agenten, die aus der Ferne Statistiken und Informationen von jeder Maschine sammeln und die Daten an einen zentralen Server weiterleiten. Mit einer solchen Software können IT-Teams schnell jedes System prüfen, das eventuell kompromittiert wurde. Diese Vorgehensweise hilft dabei, einen Angriff noch im Keim zu ersticken, und erhöht zudem die Effizienz eines forensischen Teams bei einer Untersuchung. Das Team kann Systeme nach Indizien für bösartige Software scannen, etwa Hashes, Mutexe, Zeichenketten oder Änderungen an der Registry.

6 Trend Micro Incorporated. (2013). "Trend Micro™ Intrusion Defense Firewall." Last accessed September 13, 2013, http://www.trendmicro.com/cloud-content/us/pdfs/business/datasheets/ds02_osce.pdf

Schutz der Daten

Bei der Durchdringung des Netzwerks des Opfers versucht ein Angreifer in den meisten Fällen, Daten zu stehlen. Bewahrt ein Unternehmen alle Daten an einem zentralen, schwach gesicherten Ort auf, so kann sie diese auch genauso gut verpacken und an den Angreifer schicken. Eindringlinge sind geduldig und suchen so lange, bis sie finden, was sie wollen. Je länger eine solche Suche dauert, desto mehr Zeit hat die Organisation, um die Angriffsaktivitäten aufzudecken, die Bedrohung zu beseitigen und alle vom Angreifer genutzten Wege zu sichern.

Datensegmentierung

Nicht alle Daten entstehen auf die gleiche Art und Weise. Mitarbeiter erzeugen täglich eine Riesenflut an Arbeitsinformationen, doch die meisten davon sind für den Erfolg einer Organisation nicht kritisch. Jede Geschäftseinheit muss deshalb genau prüfen, welche Informationen Schaden anrichten können, wenn sie in die falschen Hände geraten. Mit diesen Daten, den „Kronjuwelen“ des Unternehmens, sollten Organisationen anders umgehen, sie besser schützen als die alltäglichen Informationen. Diese Daten sollten etwa zum Herunterladen auf eine Workstation nicht zur Verfügung stehen. Der Zugriff darf nur auf dem Dateiserver erfolgen und zwar lediglich durch Mitarbeiter mit besonderen Zugriffsrechten. Auch sollten sie verschlüsselt lagern.

Alltägliche und möglicherweise irreführende Daten können auf einzelnen Workstations verbleiben und „geopfert“ werden . Die Zeitspanne, bis ein Eindringling feststellt, dass die Daten für ihn wertlos sind, ist unter Umständen nützlich, um die Bedrohung zu erkennen und mit der Säuberung zu beginnen.

Jedes sensible Dokument, das per E-Mail verschickt wird, sollte vom Absender mit vorhandenen Tools wie GPG separat vom E-Mail-System verschlüsselt werden. Verschafft sich ein Eindringling Zugang zum Desktop eines Mitarbeiters und kann dessen Mail-Client öffnen, so ist er dennoch nicht in der Lage, die Informationen dort zu entziffern.

Unternehmen müssen jede einzelne Information, so gut es geht, schützen. In einer pharmazeutischen Produktionsumgebung beispielsweise werden bestimmte Informationen in der Werksumgebung verteilt. Doch jedes Teil für sich genommen, ergibt noch nicht das ganze Rezept. Wenn aber ein geduldiger Eindringling die gesamte Werksumgebung untersucht, so könnte er möglicherweise die Einzelteile so zusammensetzen, dass er die ganze Formel und die Prozessinformation bekommt.

Infrastruktur für den Schutz der Daten

Daten mit einem hohen Schutzbedarf können in einem abgetrennten Netzwerk vorgehalten werden, für das physische Zugangsrechte nötig sind. Die nächste Ebene für die Datenspeicherung ist ein sicherer Server, der eine andere Zwei-Faktor-Authentifizierung erfordert als der normale lokale Netzwerkzugriff. Der Server akzeptiert keine Zugangsdaten aus dem Cache und erlaubt es auch nicht, Daten abzuziehen. Die Zugriffs-Logs für einen solchen Server werden sehr genau überwacht. Die dritte Datenkategorie liegt auf einem normalen Dateiserver. Diese Schicht enthält Informationen, die keinen großen Schaden anrichten können, sollten sie entwendet werden.

Die Einführung von Wassserzeichen für kritische Dokumente sowie ein Schutz über Data Loss Prevention (DLP) für die Infrastruktur ist ebenfalls eine Überlegung wert. Damit lassen sich ebenfalls unautorisierte Dokumentenbewegungen erkennen.

Response Team

Gründe für den Einsatz eines Response Teams

Sobald der Verdacht besteht, dass ein Einbruch stattgefunden hat, wird Zeit zum wichtigsten Gut. Zu diesem Zeitpunkt ist es zu spät, ein Team zusammenzustellen, dessen Mitglieder die nötigen Kenntnisse mitbringen, um auf den Einbruch zu reagieren. Ein Response Team benötigt ganz besondere Fähigkeiten, die nur schwer zu erwerben sind, während es sich mit einer Untersuchung befasst. Befindet sich der Eindringling schon seit längerer Zeit im Netzwerk, so ist mit einer langen und teuren Wiederherstellung zu rechnen. Ein geeignetes Team wiederum verkürzt diesen Prozess.

Wie funktioniert ein Incident Response-Prozess

Verantwortliche suchen in solchen Situation häufig nach Antworten auf Fragen, die mit „wer“, „was“ und “warum“ anfangen und dies lange bevor ein forensisches Team in der Lage ist, sachliche Schlussfolgerungen zu ziehen. Falls die Nachricht über einen Einbruch nach draußen gelangt, so wird der Druck durch die Medien und Investoren noch größer. Ohne eine fachkundige Handhabung können die ersten Tage der Untersuchung chaotisch verlaufen, voll von irreführenden Informationen und falschen Schlussfolgerungen.

Deshalb muss das betroffene Unternehmen überlegen, ob Mitarbeiter zur Verfügung stehen, die eine solche Untersuchung qualifiziert leiten können. Ist das nicht der Fall muss darüber entschieden werden, wen man gegebenenfalls mit der Untersuchung beauftragt. Zu dem könnte es Sinn machen Strafverfolgungsbehörden oder ähnliche Institutionen frühzeitig zu involvieren.

Sobald das Team steht, benötigt es erst einmal Zeit für Gespräche mit beteiligten Personen, um eine Untersuchung zu starten. Wie gut eine Untersuchung läuft, hängt häufig davon ab, wie gut die Infrastruktur einer Organisation konfiguriert ist. Wurden alle bisher dargestellten Schritte berücksichtigt, so hat das Team gute Chancen, eine erfolgreiche forensische Untersuchung zu führen und die einzelnen Aktivitäten des Eindringlings zusammenfügen zu können, und somit auch zu erkennen, was gestohlen wurde. Aber es ist auch wichtig zu verstehen, dass selbst mit einer optimalen Infrastruktur, Untersuchungen noch immer länger als erwartet oder erhofft dauern können. Steht keine geeignete Umgebung zur Verfügung, wird das Team sehr leicht ins Schwimmen geraten und wahrscheinlich nicht sehr erfolgreich sein.

Das Team

Incident Response Teams sollten aus Mitgliedern verschiedener Funktionen bestehen und getrennt vom normalen Netzwerk- oder IT-Betriebs-Team betrachtet werden. Das Team sollte so schnell wie möglich zusammengestellt sein und nicht erst wenn es gilt, auf einem Sicherheitsvorfall zu reagieren. Rollen, Verantwortlichkeiten sowie Befugnisse sollten dokumentiert werden und müssen für alle klar verständlich sein.

Team Zusammenstellung

Folgende Funktionsbereiche sollten im Incident Response Team vertreten sein:

- **Technik:** Mitarbeiter aus jeder vorhandenen Sicherheitsgruppe (z.B. Computer und physische Sicherheit), Netzwerkbetrieb oder Workstation-Management, die sich um die technische Seite der Untersuchung kümmern.
- **Bedrohungsaufklärung:** Mitarbeiter, die sich mit der Bedrohungslandschaft beschäftigen und die daher Fragen beantworten können wie, wer der Angreifer sein könnte, warum die Attacke erfolgt ist, welche Techniken er nutzt usw.
- **Personalabteilung:** Mitglieder, die zu allen Fragen in Bezug auf die Mitarbeiter und Richtlinien im Unternehmen Rede und Antwort stehen können

- **Rechtsabteilung:** Mitglieder, die Fragen zur Rechtmäßigkeit einer Untersuchung oder zur Meldepflicht eines Sicherheitsvorfalls beantworten können.
- **Presseabteilung:** Mitarbeiter, die sich um die externe Kommunikation zum Vorfall kümmern.
- **Geschäftsleitung:** Manager, die die Sicht der Unternehmensebene liefern.

Experten zur Thematik können nach Bedarf hinzugezogen werden. Das Team benötigt einen technischen Leiter, der die Schnittstelle zum restlichen „nichttechnischen" Team bildet. Er sollte die Befugnis erhalten, Entscheidungen bezüglich aller technischen Details sowie zum Personal zu treffen. Zusätzlich bedarf es eines übergreifenden Incident-Leiters, der sich um die Koordination zwischen internen und externen Einheiten kümmert. Er muss Entscheidungsbefugnis für alles haben, was den Vorfall anbelangt. Leiter müssen Entscheidungen treffen können, weil etwa der Versuch, technische Details einem nichttechnischen Manager zu erklären, zuviel Zeit in Anspruch nimmt und auch nicht alle Nuancen vermittelbar sind. Außerdem, je höher die Entscheidungse desto schwieriger wird es, ein Meeting aufzusetzen – und Zeit ist ein entscheidender Faktor!

Funktionsweise des Teams

Während der Reaktionszeitspanne auf einen Sicherheitsvorfall sollte sich das Team regelmäßig treffen und das obere Management über die Fortschritte und Probleme informieren. Alle Interaktionen sollten dabei über die Incident-Leiter gehen. Updates von einzelnen Mitgliedern zu erfragen, ist kontraproduktiv für den Informationsfluss des technischen Teams und sollte unter allen Umständen vermieden werden. Am Anfang einer Untersuchung sollten die Treffen des Teams häufiger stattfinden und können später in größeren Abständen, doch immer regelmäßig erfolgen,.

Team-Training

Das technische Team sollte frühzeitig zusammengestellt werden und erhält die Möglichkeit, außerhalb der normalen Verantwortlichkeit zusammen zu arbeiten und zu lernen. Für die Mitglieder ist es sinnvoll, den Prozess und ihre individuellen Rollen dabei schon vorher zu kennen, denn im Fall eines Sicherheitsvorfalls ist der Erfolgsdruck auf das Team immens hoch. Die Erkenntnisse aus der Trainingsphase sollten an die IT-Gruppen weitergegeben werden, damit diese die allgemeine Sicherheitslage in der Organisation verbessern können.

Erkenntnisse über Bedrohungen

Was ist unter diesen Erkenntnissen zu verstehen

Einfach gesagt umfassen Erkenntnisse über Bedrohungen Daten zu potenziellen Feinden und ihren Verhaltensmustern. Sie entstehen durch die Analyse vieler Rohdaten, die danach zu einem Gesamtbild zusammengesetzt werden. Dieses Wissen kann dazu beitragen, erste Eindringversuche zu verhindern oder festzustellen, wo im Netzwerk ein Angreifer bereits war und welche Ziele er im Netz anvisiert.

Warum es aktueller Erkenntnisse über Bedrohungen bedarf

Rohdaten ohne Analyse sind nur bedingt wertvoll. Um einen Angreifer in einem Netzwerk aufzuspüren, müssen zwei Dinge geschehen: Erstens kann ein Analyst ungewöhnliche Verkehrsmuster oder eine Reihe von Ereignissen innerhalb des Netzwerks erkennen. Er sieht zum Beispiel, dass die Workstation eines Nutzers auf die eines anderen zugreift, dass eine Reihe Anmeldeversuche zu einer ungewöhnlichen Tageszeit fehlgeschlagen sind oder er sieht eine angestoßene Deny-Regel einer Firewall oder gar die Meldung eines Nutzers über ungewöhnliche Vorkommnisse auf dessen Workstation. Ein anderer Fall wäre eine Workstation, die versucht, auf einen bekannten C&C-Server zuzugreifen oder eine .RAR-Datei an einen unbekannten entfernten Ort zu senden.

In beiden Fällen muss ein Analyst wissen, wonach er suchen soll. Hier helfen bestehende Erkenntnisse über Bedrohungen. Es gibt viel zu viele Internetadressen, als dass jemand wissen könnte, welche legitim und welche bösartig sind. Es wird sogar noch schlimmer, wenn man die Gültigkeit jeder E-Mail prüfen will, die ein Mitarbeiter bekommt. Sobald ein Angreifer in ein Netzwerk eindringt, ist es für die Abwehr entscheidend, seine Taktik, Techniken und Prozeduren zu verstehen.

Angreifer verfeinern ihre Kenntnisse immer weiter, erzeugen neue unerkannte Tools und nutzen verschiedene Wege, um dasselbe Ziel zu erreichen. Viel von dem Wissen, wie Angreifer vorgehen, wird unter Verschluss gehalten. Sobald diese Informationen öffentlich sind, wissen auch die Angreifer, dass sie andere Wege suchen müssen, um ihre Ziele zu erreichen. Einige der Angreifer ändern sogar dem Ziel entsprechend ihre TTPs (Tactics, Techniques, Procedures). Es wird zu einem Katz- und Mausspiel, und je mehr Wissen eine Organisation sammeln kann, desto besser sind die Chancen, Attacken erfolgreich abzuwehren.

Externe Informationsquellen zu Bedrohungen

Eine Organisation kann externe Informationen zu Bedrohungen über zwei Kanäle erhalten – entweder über eine Partnerschaft mit einem Anbieter solcher Informationen oder über den Einsatz von automatisierter Software.

Anbieter von Informationen zu Bedrohungen haben fähige Mitarbeiter, die die Bedrohungsakteure und deren Taktiken, Techniken und Vorgehensweisen verstehen sowie die vorhandenen Puzzlesteine zusammenfügen können. Sie liefern ihren Kunden typsicherweise Reports und Feeds. Reports konzentrieren sich im Wesentlichen auf ein einziges Thema. Sie sind kurz gehalten, wenn es etwas Neues gibt oder detaillierter, wenn die Zeit für Analysen vorhanden war. Mögliche Themenbereiche sind neue Kampagnen (z.B. Angriffe, die mehrere Unternehmen oder geografische Bereiche gleichzeitig getroffen haben), Diskussionen über eine neu entdeckte TTPs oder Schadsoftware sowie Beschreibungen eines Bedrohungsakteurs. Feeds wiederum sind Datenquellen, die typischerweise in eine automatisierte Netzwerkverteidigung integriert sind. Es können Listen mit bösartigen URLs, E-Mail-Absendern oder Betreffzeilen, sowie Hash-Darstellungen von bösartigen Dokumenten oder Schädlingen sein.

Auch die Produkte von Sicherheitsanbietern, die immer aktuelle Bedrohungsindikatoren liefern, können dabei helfen, Netzwerke zu schützen. Trend Micro™ Deep Discovery beispielsweise liefert eine hochentwickelte Bedrohungserkennung sowie Echtzeitinformationen, die eine Organisation dafür benötigt, um zielgerichtete Angriffe zu entdecken und darauf zu reagieren. Die spezielle Netzwerkerkennung von Deep Discovery deckt verschleierte Bedrohungen auf und liefert eine tiefergehende Analyse sowie weiterführende Erkenntnisse zur Art eines Angriffs. Wird Deep Discovery in die Sicherheitsinfrastruktur einer Organisation integriert, so entsteht eine „Custom Defense"-Lösung, also eine vollständige Netzwerksicherheitsstrategie zur Erkennung, Analyse, Anpassung und Reaktion auf Angreifer.[7]

7 Trend Micro Incorporated. (2013). "Deep Discovery Advanced Network Security." Last accessed September 5, 2013, http://www.trendmicro.de/grossunternehmen/erweiterter-schutz-vor-gezielten-angriffen/index.html

Interne Gruppe zur Identifizierung von Bedrohung

Unabhängig davon, ob eine Organisation Informationen zu Bedrohung von einem Anbieter bezieht oder nicht, sollte sie nach Möglichkeit eine eigene interne Gruppe aufsetzen, die sich mit der Identifizierung von Bedrohung befasst. Eine solche Gruppe, die sich nur mit Forensik und der Sammlung von Erkenntnissen über Bedrohung beschäftigt, ist von unschätzbarem Wert. Das Team hat zwei Verantwortungsbereiche: Sie sind dafür zuständig, das Web nach Verbindungen zum Unternehmen zu untersuchen. Zudem sollten sie jede Gruppe oder jeden Akteur überprüfen, falls der Verdacht auf eine Bedrohung besteht.

Die Team-Mitglieder prüfen Blogs, Pastebin und Untergrundforen auf alles, was mit der Organisation oder der entsprechenden Branche zu tun hat. Auch untersuchen sie alle Webseiten, auf denen Unternehmensmitarbeiter genannt werden. Das können Konferenzseiten mit Teilnehmerlisten sein, die für Spear-Phishing-Angriffe genutzt werden können.

Zudem ist es für das Team wichtig, möglichst viel über Exploits und Schadsoftware zu lernen, sowie über Taktiken, Techniken und Vorgehensweisen, die gegen die Organisation und ihre Netzwerke verwendet werden. Zu Exploits und Schadsoftware gibt es viele Informationsquellen, doch nur wenige zu Taktiken, Techniken und Vorgehensweisen, die Eindringlinge in einem Zielnetzwerk einsetzen. Ein sehr nützlicher Ort, an dem Teams lernen können, was Eindringlinge vorhaben, ist ein Sicherheitsbereich, der getrennt von der Unternehmensinfrastruktur betrieben wird und als eine Art „Spielplatz“ zur Erweiterung von Kenntnissen für Sicherheitsfachleute fungiert.

Hat eine Organisation beispielsweise eine Spear-Phishing-Mail abgefangen, bevor sie geöffnet wurde, so können IT-Mitarbeiter diese dort öffnen und den Exploit anstoßen, sodass der Gegner eine Backdoor zum abgeschotteten Sicherheitsbereich erzeugt. Ein entsprechend aufgesetzter „Spielplatz“ macht es möglich, alle Aktionen des Eindringlings zu überwachen, alle genutzten Tools zu erfassen und die Techniken für die Durchdringung des Netzwerks zu beobachten. Ist der Bereich groß genug und entspricht der Realität, so bietet er die Möglichkeit einer enormen Wissenserweiterung. Die gewonnenen Erkenntnisse können an das Netzwerk zurückgegeben und Sicherheitsmaßnahmen entsprechend angepasst werden. Die Überwachung aller Aktivitäten führt dazu, dass die Organisation den Gegner an jedem Punkt aufspüren und die Umgebung so säubern kann, dass der Akteur davon ausgehen muss, entdeckt worden zu sein. Es ist nicht einfach, einen solchen Bereich aufzusetzen. Machen die Teams dabei Fehler, so wird der Gegner den Bereich sofort verlassen, oder schlimmer noch, Aggressionen entwickeln.

Penetrationstests

Auch wenn ein Unternehmen nicht einer Branche angehört, in der regelmäßige Penetrationstests erforderlich sind, sollten diese durchgeführt werden. Die Tests dienen mehreren Zwecken: Zum einen helfen sie, Netzwerkbereiche zu finden, die verbessert und aktualisiert werden müssen, und zum anderen können sie dazu beitragen, Lücken in der Überwachung bestimmter Bereiche zu finden. Schließlich bieten sie Sicherheits- und Überwachungsteams die Chance, Erfahrungen in realistischen Szenarien zu sammeln.

Beim Festlegen von Regeln und Vorgehensweisen für Penetrationstests empfiehlt es sich, den Teams möglichst viel Spielraum zu lassen. Schließlich sind Penetrationstests dazu da, Erfahrungen zu sammeln, und nicht damit die Sicherheitsteams eine gute Figur abgeben. Natürlich darf dabei kein Schaden entstehen und bestimmte kritische Systeme sind für alles, was ein Risiko birgt, tabu. Doch sollten die Tester Beweise ihrer Anwesenheit hinterlassen dürfen.

Es bleibt jedem Unternehmen selbst überlassen, ob es seine Sicherheitsmitarbeiter über die Penetrationstests informiert oder nicht. Falls aber nicht vom Management ausdrücklich gewünscht, sollten Penetrationstests nicht zum Wettkampf zwischen den Test-Teams und den IT-Teams ausarten. Die Sicherheits-Teams dürfen mit dem Monitoring die Aktivitäten der Test-Teams nicht behindern. Bei Penetrationstests gibt es mehrere Wege, um dasselbe Ziel zu erreichen. Wehrt das Netzwerksicherheitsteam einen Versuch ab, so führt das dazu, dass die Organisation nichts über größere Schwachstellen erfährt, die tiefer im Netzwerk liegen. Das Test-Team hat keine realistische Zeitachse, denn es muss innerhalb nur einer oder zwei Wochen alle Aktivitäten abschließen, während ein geduldiger, zielstrebiger Angreifer wochen- oder monatelang dafür zur Verfügung hat. Das bedeutet, dass das Schließen des ersten Wegs eines Angreifers, den Testern die Möglichkeit nimmt, weitere Wege zu verfolgen.

Forensik-Teams können Penetrationstests auch als Trainingsmöglichkeit nutzen. Die Tester liefern eine vollständige Dokumentation über den Ablauf, sodass die Organisation die Antworten kennt, bevor die forensische Übung startet. Die Forensiker können ohne die Antworten zu kennen arbeiten, wobei die Organisation den Fortschritt des Prozesses begleitet und dem Team mit zusätzlichen Daten helfen kann.

Schlussfolgerung

Die bittere Realität für viele Unternehmen: Es geht nicht darum, ob sondern lediglich wann sie das Ziel eines Angriffs werden. Die hier angebotenen Ideen und Empfehlungen sind nicht revolutionär, doch leider wenden die meisten Organisationen sie nicht an. Viele der Empfehlungen führen nicht zu einem Happyend für Nutzer oder IT-Abteilungen, doch sind sie von entscheidender Bedeutung für die Verbesserung der Sicherheit und ermöglichen die Entdeckung eines Einbruchs sowie die nachfolgende Wiederherstellung. Angreifer haben die Zeit auf ihrer Seite, denn sie müssen lediglich einen Nutzer oder Administrator dazu bringen, einen Fehler zu machen, damit sie ins Netzwerk eindringen können.

Sobald der Angreifer aber ins Netzwerk eingedrungen ist, beginnt für die Organisation der Wettlauf mit der Zeit. Je länger der Eindringling im Netzwerk verweilen kann, desto mehr fasst er dort Fuß und kann Informationen entwenden. In manchen Fällen nutzt er ein Unternehmen lediglich, um sein tatsächliches Ziel anderswo zu erreichen. Man könnte meinen, damit wäre der Schaden weniger groß, doch auch dieses Szenario hat negative Auswirkungen, angefangen vom Vertrauensverlust der Partner oder Investoren bis zu Gerichtsverfahren.

Alle Verteidigungsmaßnahmen, die ein Unternehmen gegen zielgerichtete Angriffe einsetzt, können auch dazu beitragen, Insider-Angriffe aufzudecken und zu verhindern. Es ist schließlich eine bedauernswerte Realität, das der Diebstahl von Insider-Informationen für eine Organisation genau so viel Schaden anrichten kann wie ein zielgerichteter Angriff.

Die Empfehlungen führen nicht zu mehr Effizienz für das Unternehmen, verschlankten Prozessen oder besseren Nutzererfahrungen. Die Kosten für die Implementierung sollten als “Geschäftskosten” betrachtet werden, ähnlich wie der Abschluss einer Versicherung. Passiert nämlich etwas, so wiegen die Vorteile die Kosten bei weitem auf.

Referenzen

- Bashar Ewaida. (January 21, 2010). "Pass-the-Hash Attacks: Tools and Mitigation." Last accessed September 11, 2013, http://www.sans.org/reading-room/whitepapers/testing/pass-the-hash-attacks-tools-mitigation-33283?show=pass-the-hash-attacks-tools-mitigation-33283&cat=testing
- Jesper M. Johansson. (January 2008). TechNet Magazine. "Island Hopping: The Infectious Allure of Vendor Swag." Last accessed September 11, 2013, http://technet.microsoft.com/en-us/magazine/2008.01.securitywatch.aspx
- Karl Dominguez. (November 2, 2011). TrendLabs Security Intelligence Blog. "Zero-Day Exploit Used for DUQU." Last accessed September 2, 2013, http://blog.trendmicro.com/trendlabs-security-intelligence/zero-day-exploit-used-for-duqu/
- Kelly Jackson Higgins. (August 22, 2012). Dark Reading. "Shamoon, Saudi Aramco, and Targeted Destruction." Last accessed September 11, 2013, http://www.darkreading.com/attacks-breaches/shamoon-saudi-aramco-and-targeted-destru/240006049
- Nart Villeneuve. (January 26, 2012). TrendLabs Security Intelligence Blog. "Top APT Research of 2011 (That You Probably Haven't Heard About)." Last accessed September 2, 2013, http://blog.trendmicro.com/trendlabs-security-intelligence/top-apt-research-of-2011-that-you-probably-havent-heard-about/
- TrendLabs APT Research Team. (2012). "Spear-Phishing Email: Most Favored APT Attack Bait." Last accessed September 2, 2013, http://www.trendmicro.com/cloud-content/us/pdfs/security-intelligence/white-papers/wp-spear-phishing-email-most-favored-apt-attack-bait.pdf
- Trend Micro Incorporated. (2013). "Deep Discovery Advanced Network Security." Last accessed September 5, 2013, http://www.trendmicro.com/us/enterprise/security-risk-management/deep-discovery/index.html
- Trend Micro Incorporated. (2013). Threat Encyclopedia. "Ransomware." Last accessed August 29, 2013, http://about-threats.trendmicro.com/us/definition/ransomware/index.html
- Trend Micro Incorporated. (2013). "Trend Micro Intrusion Defense Firewall." Last accessed September 13, 2013, http://www.trendmicro.com/cloud-content/us/pdfs/business/datasheets/ds02_osce.pdf
- Trend Micro Incorporated. (May 31, 2012). TrendLabs Security Intelligence Blog. "Update on FLAME." Last accessed September 2, 2013, http://blog.trendmicro.com/trendlabs-security-intelligence/update-on-flame/
- Valerie Boquiron. (January 19, 2010). TrendLabs Security Intelligence Blog. "Cyber Attacks on Google and Others—Who Is Really at Risk?" Last accessed September 2, 2013, http://blog.trendmicro.com/trendlabs-security-intelligence/cyber-attacks-on-google-and-others-who-is-really-at-risk/

Über TREND MICRO

Trend Micro, der international führende Anbieter für Cloud-Security, ermöglicht Unternehmen und Endanwendern den sicheren Austausch digitaler Informationen. Als Vorreiter bei Server-Security mit mehr als zwanzigjähriger Erfahrung bietet Trend Micro client-, server- und cloud-basierte Sicherheitslösungen an. Diese Lösungen für Internet-Content-Security und Threat-Management erkennen neue Bedrohungen schneller und sichern Daten in physischen, virtualisierten und Cloud-Umgebungen umfassend ab. Die auf der Cloud-Computing-Infrastruktur des Trend Micro Smart Protection Network basierenden Technologien, Lösungen und Dienstleistungen wehren Bedrohungen dort ab, wo sie entstehen: im Internet. Unterstützt werden sie dabei von mehr als 1.000 weltweit tätigen Sicherheits-Experten. Trend Micro ist ein transnationales Unternehmen mit Hauptsitz in Tokio und bietet seine Sicherheitslösungen über Vertriebspartner weltweit an.

http://www.trendmicro.de/
http://blog.trendmicro.de/
http://www.twitter.com/TrendMicroDE

Securing Your Journey
to the Cloud

TREND MICRO DEUTSCHLAND GMBH

Central & Eastern Europe
Zeppelinstraße 1
85399 Hallbergmoos
Tel: +49 811 88990-700
Fax: +49 811 88990-799
www.trendmicro.com