SOPHOS
Security made simple.

Advanced Persistent Threats: Erkennung, Schutz und Abwehr

Autorin: **Barbara Hudson**, Senior Product Marketing Manager

Die vielen unterschiedlichen Definitionen für Advanced Persistent Threats (APT), mit denen uns Branchenexperten in jüngster Vergangenheit konfrontiert haben, sorgen oft eher für Verwirrung als für Klarheit. In diesem Whitepaper geben wir Ihnen einen Einblick in die allgemeinen Eigenschaften von APTs, ihre Funktionsweise und mögliche Abwehrmaßnahmen. Netzwerksicherheit bedeutet in erster Linie, alle Schlupflöcher zu stopfen, damit Angreifer gar nicht erst in Ihr Netzwerk gelangen. Wichtig ist jedoch auch, dass Sie die Anzeichen eines gerade stattfindenden Angriffs erkennen, damit Sie ihn erfolgreich abwehren können. Auf den folgenden Seiten erklären wir Ihnen, wie Sie mit einem mehrdimensionalen Konzept Ihr Angriffsrisiko gezielt minimieren können.

Die Bedrohungslandschaft wandelt sich, oder etwa nicht?

Viele Veröffentlichungen zum Thema APTs beginnen mit ominösen Bezugnahmen auf die sich wandelnde Bedrohungslandschaft und Schilderungen raffinierter Cyberangriffe, die sich immer mehr ausweiten. Das kann irreführend sein. Denn tatsächlich kommen bei den meisten Angriffen nach wie vor Techniken zum Einsatz, die schon seit Jahren bestens bekannt sind – vornehmlich Social Engineering, Phishing-E-Mails, Backdoor Exploits und Drive-by-Downloads. Solche Angriffe sind weder fortgeschritten noch besonders raffiniert, wenn man ihre einzelnen Bestandteile betrachtet, und setzen oft auf das schwächste Glied im Unternehmen – den Benutzer. Was APTs von anderen Angriffen unterscheidet, ist vielmehr die Kombination verschiedener Techniken und die Hartnäckigkeit der Angreifer.

68 %

ALLER IT-MANAGER WISSEN NICHT, WAS EIN APT IST

Quelle: Ponemon Institute, The Risk of an Uncertain Security Strategy, Nov. 2013

Advanced Persistent Threats

Der Begriff APT ist den letzten Jahren flächendeckend gebraucht und missbraucht worden. Wahrscheinlich wird Ihnen auch der Begriff Advanced Targeted Attack (ATA) begegnet sein, mit dem meist das Gleiche gemeint ist. Als APT und ATA wurde in der Vergangenheit so ziemlich alles bezeichnet – von medienwirksamen Angriffen auf Unternehmen und Nationalstaaten, über diverse Cybercrime-Kampagnen und Hacking-Techniken bis hin zu einzelnen Malware-Samples. Für viele Unternehmen ist es daher zunehmend schwierig, diesen Hype von tatsächlichen Sicherheitsanforderungen zu unterscheiden. Sie sind nicht sicher, was ein APT tatsächlich ist und was nicht, und was getan werden kann, um APTs zu erkennen und abzuwehren.

APTs zeichnen sich im Allgemeinen durch folgende Eigenschaften aus:

1. **Gezielt**
   Die Angriffe richten sich meist gezielt an eine bestimmte Firma, Gruppe oder Branche. Vor dem eigentlichen Angriff müssen die Angreifer unter Umständen umfassende Recherchearbeit leisten, um Informationen über ihr Ziel einzuholen. Solche Gruppen von Angreifern sind meist kapitalkräftig und gut organisiert.

2. **Zielorientiert**
   Die Angreifer wissen meist relativ genau, was sie erreichen oder auf welche Bereiche sie zugreifen möchten, bevor sie sich Zugang zum Netzwerk verschaffen. Geschickten Angreifern bieten sich zahlreiche Möglichkeiten, um in Netzwerke einzudringen und an die gewünschten Informationen und Systeme zu gelangen.

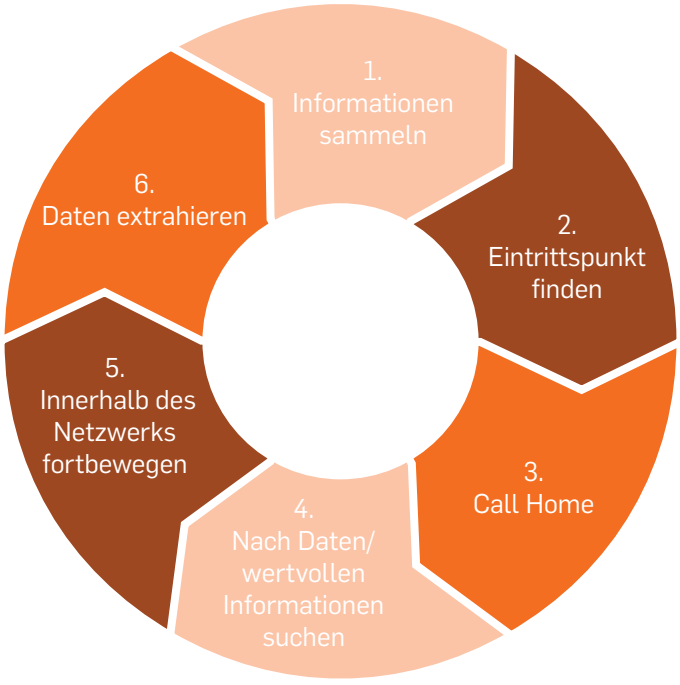
3. **Andauernd**
   Nach einem erfolgreichen Einbruch ins Netzwerk ist der erste infizierte Computer nicht zwangsläufig von großem Interesse, sondern vielmehr Mittel zum Zweck. Sobald die Angreifer ins Netzwerk gelangt sind, arbeiten sie sich aller Wahrscheinlichkeit nach weiter im Netzwerk vor und versuchen auf Systeme zuzugreifen, auf denen wertvollere Daten gespeichert sind, z. B. Computer von IT-Administratoren oder Führungskräften mit Zugangsdaten für hochwertigere Systeme.

4. **Geduldig**
   Viele Cyberangriffe sind darauf ausgelegt, Schaden anzurichten, indem sie den Zugriff auf Systeme sperren und Daten extrahieren. Nicht so APTs. Sie verhalten sich am Anfang meist ruhig. Denn der Angriff soll unbemerkt vonstatten gehen. Um das zu erreichen, ist es am besten, von Anfang an so wenig Aufmerksamkeit wie möglich zu erregen. Diese Nicht-Aktivität kann über Tage, Wochen, Monate oder sogar Jahre hinweg andauern.

5. **Es erfolgen Call-Home-Versuche**
   Kein Angriff läuft ohne Kommunikation zur Außenwelt ab, auch ein APT nicht. Früher oder später starten die Angreifer Call-Home-Versuche. Entweder nach Infektion des ersten Systems oder nachdem sie die gewünschten Daten gefunden und zusammengetragen haben bzw. die infizierten Systeme hinreichenden Zugriff auf diese Daten besitzen. Die Kommunikation mit dem Command and Control (C&C) Host wird meist über einen längeren Zeitraum aufrechterhalten, um weitere Anweisungen entgegenzunehmen oder Daten in „mundgerechten" Stücken zu extrahieren.

Ein typischer APT-Lebenszyklus

Der übliche Lebenszyklus eines APTs kann am einfachsten anhand von Beispielen derjenigen Techniken erläutert werden, die in der Vergangenheit erfolgreich angewendet wurden. Den im Folgenden beschriebenen APT gibt es nicht wirklich, er basiert jedoch auf realen Beispielen. Die Abfolge der einzelnen Phasen ist in vielen Fällen austauschbar – die Fortbewegung innerhalb des Netzwerks kann beispielsweise auch vor der Suche nach Daten beginnen. Andere Phasen wiederum erstrecken sich über den gesamten Lebenszyklus, wie z. B. die Kommunikation mit dem C&C Host.



1. Informationen sammeln

Eine Gruppe von Angreifern hat es auf ein Unternehmen in der Pharmaindustrie abgesehen. Ihr Ziel besteht darin, an Daten zu einem neuen, sich gerade in der Entwicklung befindenden Medikament zu gelangen, das dem Unternehmen einen klaren Wettbewerbsvorteil verschaffen würde. Die Angreifer recherchieren im Internet, u. a. in sozialen Netzwerken, und besuchen Messen, um ein Profil des Unternehmens zu erstellen und an die Namen führender Mitarbeiter zu gelangen.

➔ **Die besten Informationsquellen sind das Internet und soziale Medien:** Mitarbeiter müssen keine vertraulichen Unternehmensinformationen posten. Posts über Geschäftsreisen und Unternehmensveranstaltungen reichen oftmals schon aus, um Angreifern das Schlupfloch zu liefern, nach dem sie suchen.

2. Eintrittspunkt finden

Auf Grundlage der in Schritt 1 gesammelten Informationen wissen die Angreifer, dass das Unternehmen im Frühjahr eine Vertriebskonferenz in Las Vegas geplant hat. Sie sind also darüber informiert, dass eine Vielzahl von Mitarbeitern aus allen Ebenen des Unternehmens zur selben Zeit am selben Ort sein wird. Sie besuchen den Veranstaltungsort während der Konferenz und hinterlassen im Tagungsraum und in anderen Bereichen, in denen sich Mitarbeiter des Unternehmens aufhalten, eine Reihe von USB-Sticks. Sie hoffen, dass die Neugier siegen und jemand einen USB-Stick an seinen Firmencomputer anschließen wird – entweder, um herauszufinden, was auf dem Stick gespeichert ist, oder um den Besitzer zu ermitteln.

➔ **Ein Beispiel aus dem echten Leben:** Eine ähnliche Taktik wurde bei Stuxnet angewendet, einem APT, der 2010 auf das iranische Atomprogramm abzielte. USB-Sticks wurden auf einem Parkplatz hinterlassen, von dem der Angreifer wusste, dass er von Mitarbeitern des Atomkraftwerks genutzt wird.

3. Call Home

In unserem Beispiel hat einer der Mitarbeiter tatsächlich einen USB-Stick an seinen Computer angeschlossen. Die auf dem Stick gespeicherte Malware möchte nun den Angreifer informieren, dass sie ins Netzwerk gelangt ist. Zu diesem Zweck baut sie eine Call-Home-Kommunikationsverbindung zu einem „Command-and-Control"-Server (C&C) auf, um ihren Standort zu melden oder neue Anweisungen entgegenzunehmen. In vielen Fällen dient der erste Call-Home-Versuch auch dazu, die Malware zu aktualisieren und sie damit geeigneter für die folgenden Angriffsschritte zu machen.

In einem typischen APT-Lebenszyklus ist die Kommunikation mit dem C&C-Host ein Vorgang, der sich über den gesamten Lebenszyklus erstreckt. So kann die Malware immer wieder angepasst werden, sobald neue Informationen vorliegen.

➔ **Vertrauen Sie keinem ausgehenden Datenverkehr:** Call Home ist der Punkt, an dem viele Sicherheitslösungen versagen – wenn Sie Ihren eingehenden und ausgehenden Datenverkehr nicht prüfen, können Kommunikationen stattfinden, die nicht in Ihrem Interesse sind.

4. Nach Daten/wertvollen Informationen suchen

Nachdem der erste Computer infiziert ist, kann die Malware sich zum ersten Mal direkt im Netzwerk umsehen. Ein solcher Einblick lässt sich mit keiner noch so aufwändigen Recherchearbeit erzielen – außer es liegt Insider-Wissen vor. Je nach Zugangsdaten des Benutzers haben die Angreifer bereits Zugriff auf die gewünschten Systeme oder nutzen den ersten manipulierten Computer als Sprungbrett, um sich Zugriff zu weiteren Systemen zu verschaffen. Im vorliegenden Fall gehört der infizierte Computer einem Mitarbeiter in der Verwaltung, der keinen Zugriff auf Systeme mit Daten über das Medikament hat. Der nächste Schritt für die Angreifer besteht also darin, zu ermitteln, welche Systeme von Interesse sind und wer auf diese Zugriff hat. Auf Grundlage dieser Informationen ergeben sich dann die folgenden Schritte.

➔ **Vorsicht vor Portüberwachung:** Portüberwachung ist eine weit verbreitete Technik, mit der sich ermitteln lässt, auf welche Systeme mit möglicherweise interessanten Daten ein Computer Zugriff hat. Mit Antivirus, Application Control und Intrusion Prevention Systems können eine Reihe schädlicher Portüberwachungsanwendungen erkannt werden.

5. Innerhalb des Netzwerks fortbewegen

Das ideale Ziel für einen APT-Angriff ist die IT-Abteilung, da diese meist über Zugriffsberechtigungen verfügt, die über die eines herkömmlichen Mitarbeiters hinausgehen. Sobald die Angreifer herausgefunden haben, wer die IT-Mitarbeiter sind und wie leicht es ist, Zugriff auf ihre Systeme zu erlangen, geschieht meist entweder a) oder b):

a) Die Angreifer infizieren weitere Systeme und nutzen diese als Sprungbrett zu ihrem endgültigen Ziel.

b) Die Angreifer starten einen weiteren Angriff, um sich schneller Zugriff auf die gewünschten Systeme zu verschaffen – z. B. über Social Engineering oder die Ausnutzung einer Web-Schwachstelle, jeweils gezielt an die IT-Abteilung gerichtet.

➔ **Patchen, patchen, patchen:** Oft genügt bereits eine bekannte, aber noch ungepatchte Schwachstelle, um Angreifern ein Schlupfloch zum Infizieren des Netzwerks zu liefern. Deshalb ist es so wichtig, immer und auf allen Systemen die neuesten Sicherheitspatches einzuspielen.

6. Daten extrahieren

Sobald unsere Angreifer die Systeme ihres Interesses erreicht und die gewünschten Daten gefunden haben, besteht die nächste Hürde für sie darin, die Daten zu extrahieren. In diesem Stadium des Angriffs wird die Malware verstärkt mit dem C&C-Host kommunizieren, da die Daten mit hoher Wahrscheinlichkeit in kleinen, verschlüsselten Paketen extrahiert werden, um unerkannt zu bleiben.

➔ **Achten Sie auf ungewöhnliches Verhalten:** Ausgehenden Datenverkehr zu kontrollieren, ist wichtig. Sie benötigen jedoch auch Sicherheitssysteme, die ungewöhnliche Verhaltensmuster aufzeigen. Mit umfassenden und einfach zugänglichen Echtzeit-Reportingfunktionen (einschließlich Vergangenheitsdaten) können Sie Spitzen beim Datenverkehr zu bestimmten Hosts oder bestimmte Datentypen wie verschlüsselte Dateien identifizieren.

NUR 36 %

ALLER KLEINUNTERNEHMEN INSTALLIEREN SICHERHEITSPATCHES

Quelle: Naked Security

Zwei große Mythen über APTs

1. APTs greifen nur große Unternehmen und Nationalstaaten an

Ganz gleich, wie groß das Unternehmen ist, in dem Sie arbeiten. Als IT-Manager oder Chief Security Officer ist es Ihre Aufgabe, wertvolle Daten vor unbefugten Zugriffen zu schützen. Ihr Unternehmen und wahrscheinlich auch Ihr Job hängen davon ab.

- Wenn Daten innerhalb Ihres Unternehmens als wertvoll gelten, könnten sie auch für andere Unternehmen wie Wettbewerber interessant sein.
- Wenn Sie personenbezogene Daten jeglicher Art verarbeiten, sind Sie in den meisten Ländern gesetzlich dazu verpflichtet, unbefugte Zugriffe auf die Daten zu unterbinden.
- Große Unternehmen und Behörden nutzen oft eine breitgefächerte Lieferkette, die sich aus kleineren Unternehmen zusammensetzt. Wenn Sie ein solcher Zulieferer sind, könnten Sie haftbar sein, wenn die von Ihnen verarbeiteten Daten veruntreut werden, auch wenn es nicht Ihre eigenen sind.
- APTs haben in der Vergangenheit bewiesen, dass Angriffe durchaus auf andere Unternehmen überspringen können, die ursprünglich nicht Ziel des Angriffs waren.

2. Herkömmliche Abwehrmaßnahmen sind ungeeignet

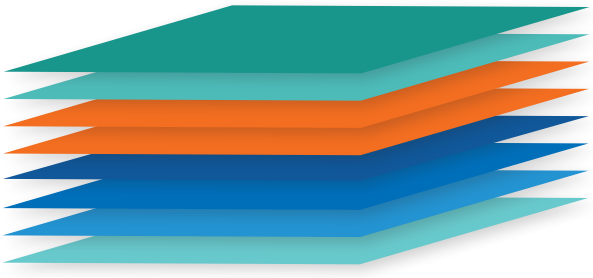
Da viele Anbieter von Sicherheitslösungen die Abwehr von APTs als erfolgreiches Geschäftsmodell für sich entdeckt haben, behaupten nicht wenige, nur ihre Lösung biete ausreichenden Schutz und herkömmliche Sicherheitslösungen wie Antivirus-Software seien überflüssig. Solche Behauptungen sind schlichtweg falsch.

- Keine einzelne Lösung kann Sie komplett vor APTs schützen.
- Um eine erfolgreiche Abwehr verschiedenster Bedrohungen zu ermöglichen, sollten Sie stets auf mehrere Schutzschichten setzen.
- Web-Exploits, Phishing-E-Mails und Remote-Access-Trojaner sind allesamt beliebte Elemente von APTs. Herkömmliche Sicherheitssysteme sind für die Erkennung von Angriffen im Frühstadium und zum Verhindern ihrer weiteren Ausbreitung also nach wie vor wichtig.

SO FUNKTIONIERT COMMAND & CONTROL
Video

Technologien für Advanced Threat Protection

Was auch immer Anbieter von Speziallösungen uns glauben machen wollen: Gegen APT-Angriffe gibt es keine Wunderwaffe. Intelligente Sicherheitsvorkehrungen, die auch eine End-to-End-Strategie umfassen, stellen immer noch die wirksamste Methode zum Schutz vor herkömmlichen und modernen Cyberangriffen dar.



Firewall
Intrusion Prevention Systems (IPS)
Erkennung von Command and Control/ Botnets
Sandboxing
Web Protection
Email Protection
Web Application Firewall
Antivirus
Sichere WLAN- und Remoteverbindungen

WEITERE INFOS ÜBER NETZWERK-BEDROHUNGEN

Kurze 3-Minuten-Videos zum Thema Hacking ansehen

Folgende Schutzschichten sind unverzichtbar:

Firewall
Die erste Verteidigungslinie Ihres Netzwerks sollte eine Paketfilter-Firewall sein. Sie ist eine praktische Methode, die häufigsten Sicherheitslücken (oder Ports) zu schließen.

Intrusion Prevention Systems (IPS)
Netzwerkbasierte IPS prüfen den Netzwerkverkehr genauer und fungieren als zusätzliche Schutzschicht an der Netzwerkgrenze. Host Intrusion Prevention Systems, oder kurz HIPS, sind meist in Antivirus-Lösungen enthalten. Durch konstante Überprüfungen können IPS eine Vielzahl von Schwachstellen erkennen. Es lohnt sich immer, darauf zu achten, wie viele Signaturen ein Anbieter verwendet und wie flexibel die Einstellungen sind. Schließlich möchten Sie keine Signaturen für Betriebssysteme prüfen müssen, die Sie gar nicht verwenden, oder unnötige Prüfungen vornehmen, die Ihre Performance beeinträchtigen.

Erkennung von Command and Control/Botnets
Wie bereits erwähnt halten APTs die Kommunikation zu ihrem Host aufrecht, um neue Befehle und Updates entgegenzunehmen. Durch Scans auf schädliche Hosts können Sie ausgehenden Datenverkehr sperren und so die Kommunikation mit dem C&C Host unterbinden. Anbieter, deren Lösungen eine C&C-Erkennung beinhalten, benötigen eine eigene oder eine durch einen OEM-Partner bereitgestellte professionelle Laborinfrastruktur, um die Aktualität der Sicherheitsdaten zu gewährleisten. Die meisten Lösungen setzen auf eine Kombination aus Mechanismen zur Datenverkehrsanalyse auf Basis von DNS-Suchen, IP-Tabellen und Engines zur Anwendungskontrolle.

Sandboxing
Im Zusammenhang mit APT-Schutz wird immer wieder Sandboxing genannt. Eine Sandbox ist entweder eine physische oder eine virtuelle Umgebung, die dazu dient, Code und Programme zweifelhafter Herkunft unter abgesicherten Bedingungen auszuführen und zu testen. Die Sandbox ist von allen Produktionsumgebungen getrennt, in denen sie Schaden anrichten könnte, und kann daher auch zum Testen und Analysieren von Schadcode verwendet werden. Es gibt verschieden Arten von Sandboxing mit jeweils sehr unterschiedlichen Verwaltungs- und Performance-Anforderungen.

- **Selektives Sandboxing**
  Selektives Sandboxing dient dazu, unbekannte Dateien zur Analyse auszuwählen und zu identifizieren. Stellt sich die Datei als schädlich heraus, wird eine neue Definition erstellt und verteilt, um zukünftige Infektionen zu verhindern. Analysen dieser Art stützen sich normalerweise auf eine bestehende Laborinfrastruktur wie die SophosLabs. Innerhalb der Sophos UTM kann die Übermittlung von Dateien an die SophosLabs deaktiviert werden. Ein Austausch anonymisierter Daten zur Optimierung des Bedrohungsschutzes kann jedoch der gesamten Sicherheitscommunity zu Gute kommen. Selektives Sandboxing als Teil einer bestehenden Next-Generation Firewall-Lösung kann den Schutz erheblich erhöhen, wenn die Implementierung einfach ist und das Sandboxing vollständig mit anderen Sicherheitssystemen integriert werden kann. Viele der führenden Netzwerksicherheitsanbieter haben solche Sandboxing-Verfahren im Angebot und nutzen in den meisten Fällen eine cloudbasierte Infrastruktur, mit der die Systemperformance nur minimal beeinträchtigt wird.

- **Vollständiges Sandboxing**
  Einige Systeme setzen den Schwerpunkt auf elektronische Beweise und analysieren alle Daten in einer Sandbox. Die Funktionsweise der einzelnen Systeme ist sehr unterschiedlich, weshalb es nicht sinnvoll ist, sie alle gemeinsam zu beurteilen. Meist bestehen Lösungen für vollständiges Sandboxing aus dedizierten Appliances, die lokal gehostet werden und keine weiteren Sicherheitslösungen beinhalten. Bei der Auswahl einer solchen Lösung sollten Sie sich folgende Fragen stellen:

  - Wiel viel Training ist für die Einrichtung der Lösung erforderlich?
  - Ist die Lösung auf meine Unternehmensgröße und Anforderungen skalierbar?
  - Verfüge ich über die notwendigen Ressourcen und Kenntnisse, um eine solche Lösung erfolgreich zu implementieren?
  - Welche anderen Sicherheitsfunktionen bietet die Lösung?
  - Wie beeinträchtigt die Lösung die übergreifende Performance meines Netzwerks?

Im Normalfall ist eine Sandboxing-Lösung nicht darauf ausgelegt, eine Next-Generation Firewall zu ersetzen. Um umfassenden Schutz zu erhalten, müssen Sie also nach wie vor eine weitere Netzwerksicherheits-Appliance implementieren.

Web Protection

Das regelmäßige Einspielen von Patches ist unverzichtbar. Genauso wichtig ist es zu prüfen, ob Internetrichtlinien wirksam sind – und zwar auch dann, wenn Mitarbeiter sich außerhalb des Unternehmensnetzwerks befinden. Die hohe Anzahl mobiler Mitarbeiter stellt IT-Abteilungen heutzutage vor neue Herausforderungen. Es gibt jedoch einfache Methoden, mit denen Sie Benutzer immer und überall schützen können – unabhängig davon, wie diese auf das Netzwerk zugreifen.

Webfunktionen können je nach Lösung stark variieren. Webfilter und Application Control können Benutzer vor Schad-URLs und Exploit-Code schützen. Zur Abwehr neuester Bedrohungen sind moderne Lösungen zum Schutz vor Web-Malware mit leistungsstarken Emulationsfunktionen erhältlich.

Whitepaper-Empfehlung: Die fünf Phasen eines Web-Malware-Angriffs

PHISHING – DEN SCHWACHPUNKT IM VISIER
Video

Email Protection
E-Mails sind für viele Angreifer immer noch der beliebteste Übertragungsweg für Malware. Denn die Menschheit ist von Natur aus neugierig und kann der Versuchung, auf Links zu klicken oder Anhänge zu öffnen, vielfach nicht widerstehen. Moderne Phishing-E-Mails sind zudem immer schwieriger als solche zu erkennen – die Zeiten schlecht gefälschter Logos und Rechtschreibfehler sind definitiv vorbei.

Selbst Sicherheitsanbieter sind bereits Opfer solcher Angriffe geworden. Eine Sicherheitspanne vor einigen Jahren bei RSA begann z. B. mit Phishing-E-Mails, die schädliche Anhänge enthielten. Ein wirksame Email Protection sollte neben Funktionen zur Spam- und Malware-Erkennung auch Optionen zur E-Mail-Verschlüsselung und Data Loss Prevention (DLP) beinhalten. Das Thema E-Mail-Verschlüsselung wurde in der Vergangenheit allzu oft vernachlässigt, weil die bei herkömmlichen Lösungen am Absender- und Empfängerstandort erforderliche Public-Key-Infrastruktur (PKI) gescheut wurde. Es gibt jedoch Lösungen, die ohne den Einsatz spezieller Schlüsselmanagementsysteme eine einfache, nahtlose und sichere Kommunikation ermöglichen und darüber hinaus eine richtlinienbasierte DLP beinhalten, mit der vertrauliche E-Mails automatisch verschlüsselt oder blockiert werden können.

Whitepaper-Empfehlung: Wer liest Ihre E-Mails mit?

Web Application Firewall
Websites gehören zu den häufigsten Malware-Quellen und viele Unternehmen vernachlässigen die Sicherheit ihrer eigenen Website. Systeme, die in einer Demilitarized Zone, kurz DMZ, ausgeführt werden, müssen hinreichend geschützt werden. Ansonsten drohen Angriffe auf Ihre Website, bei denen nicht nur Ihre eigenen Computer, sondern auch die Computer von Besuchern Ihrer Website infiziert werden könnten. Da viele Unternehmen außerdem webbasierte Anwendungen wie SharePoint, Outlook Web Access und Saleforce nutzen, greifen Benutzer nun auf Systeme zu, die sich jenseits der Netzwerkgrenze befinden.

SQL-Injection-Angriffe wurden in den vergangenen Jahren häufig mit bedeutenden Datenpannen in Verbindung gebracht. Durch die Ergänzung einer weiteren Schutzschicht zwischen Webservern und dem Internet (z. B. Reverseproxy-Authentifizierung) lassen sich wichtige Unternehmenssysteme noch besser absichern. Auch durch den Einsatz einer Zwei-Faktor-Authentifizierung mit Einmalpasswort kann verhindert werden, dass sich formular- oder browserbasierte Anmeldungen auf Webservern zum Sicherheitsschwachpunkt entwickeln.

Whitepaper-Empfehlung: Sicherheitsrisiko Webserver: So schließen Sie die Hintertüren

Antivirus
Host- und Client-Antivirussysteme sind nach wie vor entscheidende Komponenten in Sicherheitsstrategien aller Art und können bei entsprechender Aktualisierung viele Angriffe bereits im Keim ersticken. Hier ist es äußerst wichtig, zwischen den verschiedenen Lösungsarten zu unterscheiden.

Rein signaturbasierte Lösungen können lediglich schon bekannte Malware erkennen. Daher ist eine Lösung erforderlich, die auch das Verhalten des Datenverkehrs beobachtet, auf Echtzeit-Daten zur Erkennung neuerer Bedrohungen zugreift und die Möglichkeit bietet, potenziell schädliche Inhalte zu analysieren.

Es sollte auch darauf hingewiesen werden, dass Anbieter in vielen UTMs und Next-Generation Firewalls zur Bereitstellung der Antivirus-Funktion fluss- oder strombasierte Scanverfahren anwenden. Solche Lösungen sind zwar ressourcenschonender, prüfen jedoch nur die ersten paar Bytes eines Datenpakets und können bestimmte Arten von Malware demzufolge nicht erkennen. Außerdem können sie keine verschlüsselten Dateien prüfen und scannen nur ausgewählte Archivdateitypen. Eine höhere Performance ist also verglichen mit proxybasierten Antiviruslösungen, die Pakete vollständig prüfen und verschlüsselte oder komprimierte Dateien scannen können, mit sicherheitstechnischen Nachteilen verbunden.

Sichere WLAN- und Remoteverbindungen
Unabhängig davon, welche anderen Technologien implementiert sind, kann die Sicherheit durch ein unsicheres WLAN oder eine unsichere Verbindung zu Unternehmensdaten beeinträchtigt werden. Da mobile Mitarbeiter heutzutage von überall und mit verschiedenen Geräten auf Daten zugreifen, ist der Schutz Ihrer Daten sowieso schon eine Herausforderung.

Daher sollten Sie als Allererstes dafür sorgen, dass Ihr eigenes WLAN über eine sichere Verschlüsselung verfügt und Besuchern und Gästen Internetzugriff gewährt, ohne Ihre Sicherheit zu gefährden. Mitarbeiter im Homeoffice und in kleinen Außenstellen sollten nicht zum Schwachpunkt Ihres Sicherheitskonzepts werden. Mit einer sicheren Standort-zu-Standort-VPN-Lösung müssen Sie keine sicherheitstechnischen Kompromisse eingehen, wenn Mitarbeiter außerhalb der Unternehmenszentrale arbeiten.

Whitepaper-Empfehlung: 5 Tipps für sichere WLANs

Sophos Complete Security

Sophos bietet eine Reihe von Sicherheitslösungen zum Schutz Ihres Netzwerks, Ihrer Server und Computer an. Mit individuellen Einzellösungen, cloudbasiertem Schutz, Network Security Appliances und virtuellen Optionen können wir Ihnen dabei helfen, den Schutz zu finden, der am besten auf Ihre Anforderungen, verfügbaren Ressourcen und Ihr Budget abgestimmt ist. Viele unserer Lösungen bieten Integrationsmöglichkeiten. So gewährleisten wir eine bessere Abstimmung der einzelnen Komponenten und ermöglichen ein zentrales und einheitliches IT-Sicherheitskonzept.

Sophos UTM

Wir bei Sophos gehen sehr pragmatisch an das Thema Advanced Threat Protection heran und bieten mehrere Schutzschichten in einer einfach verwaltbaren Lösung. Wir verstehen, dass viele IT-Abteilungen nicht über die nötigen Ressourcen verfügen, um eine Vielzahl von Einzellösungen effektiv verwalten zu können. Das sollte jedoch nicht bedeuten, dass Sie bei der Sicherheit Kompromisse eingehen müssen. Wir vereinen eine Vielzahl von Technologien in einem System und gestalten die Bereitstellung so einfach wie das Umlegen eines Schalters. Unsere Sicherheit hält, was sie verspricht – unabhängig von der Größe Ihres Unternehmens. Darüber hinaus umfasst unser Angebot eine Plug-and-play-Lösung zum Schutz von Außenstellen und Remotestandorten.

Sophos UTM ist eine modulare Lösung, die bei Bedarf beliebig erweitert werden kann.

Zu den optional erhältlichen Features gehören:

- **Network Protection** einschließlich Advanced Threat Protection, IPS und Application Control
- **Web Protection** mit allen Features eines Secure Web Gateway in einer zentralen UTM
- **Webserver Protection** mit Reverseproxy-Authentifizierung
- **Email Protection** mit Anti-Spam, E-Mail-Verschlüsselung und DLP
- **Wireless Protection** mit weitreichender Hotspot-Unterstützung für Gastnetzwerke
- **Endpoint Protection** mit zwei in die UTM integrierten Antivirus-Scan-Engines

Sophos UTM

Kostenlose Testversion unter
www.sophos.de/utm-testen

Sales DACH (Deutschland, Österreich, Schweiz)
Tel.: +49 611 5858 0 | +49 721 255 16 0
E-Mail: sales@sophos.de

2/14.NP.wpde.simple

SOPHOS