COMPUTERWOCHE

Security-Anbietercheck

Wie sich gezielte Angriffe abwehren lassen

Datum: 24.02.2015
Autor(en): Stefan Strobel

Anwender erwarten die Zuverlässigkeit ihrer Security-Systeme und hoffen gleichzeitig, dass sie sie erst gar nicht brauchen. Je zielgerichteter heutige Cyberattacken werden, desto trügerischer ist diese Hoffnung. Wir geben Tipps, was IT-Verantwortliche gegen immer ausgefeiltere Angriffsvektoren tun können.

Firewalls und Virenschutzsysteme allein genügen nicht mehr, um in der heutigen Bedrohungslage sicher zu bleiben. Das zeigen bekannt gewordene Datendiebstähle und Spionagefälle der jüngsten Zeit. Zugleich bieten zahlreiche Hersteller von Sicherheitslösungen neue Produkte an, die vor sogenannten APTs **("Advanced Persistent Threats"**[1]) schützen sollen. Gemeint sind gezielte und nachhaltige Angriffe von professionellen Hackern, die als Mitglieder oder im Auftrag krimineller Vereinigungen in Unternehmen einbrechen, um dort Daten zu stehlen oder Anlagen zu sabotieren.

Heutige Attacken sind zwar selten komplexer und hinterhältiger als frühere, dafür aber umso zielgerichteter auf ein bestimmtes Netzwerk ausgelegt. Das macht sie so gefährlich.
Foto: Fotolia, Radim Strojek

Die Ausgangslage

Ein Angreifer, der gezielt in ein bestimmtes Unternehmen einbrechen möchte, wird sich Zeit nehmen und den einfachsten oder elegantesten Weg suchen, um die Kontrolle über die Server des Opfers zu übernehmen. Vor 15 bis 20 Jahren waren extern sichtbare Server oftmals noch voller Schwachstellen. Die Betriebssysteme wurden zu selten oder überhaupt nicht aktualisiert, Firewalls waren schlecht konfiguriert und ein Angreifer musste nur einen Schwachstellen-Scanner wie Nessus starten, um einen Schwachpunkt zu finden und dann mit öffentlich verfügbaren Angriffswerkzeugen die Server zu übernehmen. Diese Zeiten sind immerhin bei jenen Unternehmen vorbei, die einen kompetenten Sicherheitsbeauftragten und einen sinnvollen **Patch-Management-Prozess**[2] etabliert haben.

Seit mindestens zehn Jahren verschiebt sich daher der Fokus von Angreifern weg von der Betriebssystemebene hin auf die Applikationsebene. Die externen Web-Applikationen vieler - vor allem mittelständischer - Unternehmen sind jedoch auch heute noch mit Techniken wie **SQL Injection**[3] oder Cross-Site Scripting angreifbar. Bei zahlreichen mittelständischen Unternehmen sind Web Application Firewalls (WAFs) nach wie vor eher selten im Einsatz und viele Firme nehmen nicht einmal jährlich **Penetrationstests**[4] vor.

Ungeachtet dieser Defizite im Mittelstand haben Cyber-Kriminelle auch ihre Angriffstechniken auf Endgeräte von Benutzern weiterentwickelt. Dort kann man heute auch Unternehmen erfolgreich angreifen, die in den letzten Jahren ihre Hausaufgaben gemacht haben und bei denen externe Server und Web-Applikationen gut gesichert sind.

Anwender müssen in der Regel per Mail mit externen Personen kommunizieren können, und auch der Zugriff auf externe Webserver gehört heute zur alltäglichen Büroarbeit. Doch leider enthalten Hilfsprogramme wie PDF-Viewer, Flash Player, Java-Interpreter, die Office-Produkte, Webbrowser selbst und zahlreiche andere Plug-ins immer wieder neue Schwachstellen. Genau diese Schwachstellen nutzen Kriminelle aus: Sie versenden gezielte und echt aussehende **Phishing-Mails**[5] und locken Anwender auf Webseiten mit individueller Malware.

[Hinweis auf Bildergalerie: **So gehen die Phishing-Betrüger vor**] gal1

Virenscanner, die auf den PCs der Anwender oder auf Sicherheits-Gateways in der Firewall-Umgebung des Unternehmens installiert sind, können diese Probleme nicht lösen, denn sie erkennen nur bereits bekannte Malware. Die Angreifer entwickeln aber stets neue Varianten ihrer Viren, Trojaner und Rootkits und bleiben auf diese Weise lange Zeit unentdeckt.

Sandbox-Analyse

Die neuen Lösungen, die dieses Problem adressieren, setzen an unterschiedlichen Stellen an. Am bekanntesten ist momentan die Analyse von übertragenen Objekten in einer gesicherten virtuellen Maschine oder Sandbox in der Firewall-Umgebung, bezeichnet als "Sandbox-Analyse". Ein Sensor kopiert alle Dokumente beziehungsweise Objekte, die von Webseiten heruntergeladen werden oder an eingehenden Mails angehängt sind. Diese Objekte werden in einer abgeschotteten Sandbox auf

einem zentralen System gespeichert und dort automatisch geöffnet oder zur Ausführung gebracht. Dabei überwacht ein Sicherheitssystem alle Aktivitäten in der Sandbox. Wenn nun Systemeinstellungen manipuliert werden, Code aus dem Internet nachgeladen oder sonstiges bösartiges Verhalten erkannt wird, geht man davon aus, dass es sich um Malware handelt.

Damit diese Analyse nicht mehrfach nötig wird, speichert das System eine Prüfsumme mit dem Analyseergebnis. So lässt sich das Objekt wiedererkennen, wenn es ohne Veränderung nochmals heruntergeladen wird oder einer Mail angehängt ist. Im Wiederholungsfall kann ein bereits zuvor analysiertes und als gefährlich eingestuftes Objekt dann auch direkt blockiert werden.

Diese Information - das Analyseergebnis der Malware und seine Prüfsumme - fällt unter den Überbegriff **"Threat Intelligence"**[6]. Die meisten Hersteller bieten ihren Kunden zusätzlich zu dem Analyse-System auch eine Cloud-Plattform, über die Threat Intelligence ausgetauscht werden kann. Damit können die Kunden des Herstellers von Informationen über bereits analysierte Malware anderer Kunden profitieren.

[Hinweis auf Bildergalerie: **Threat Monitoring Tools & Services**] gal2

Beim ersten Auftreten einer neuen Malware steht jedoch eine neue Analyse an. Da diese Analyse einige Zeit benötigt, ist es üblich, die Anwender nicht warten zu lassen. Folglich kommt die erste Übertragung in der Regel beim Anwender an, bevor die Analyse fertiggestellt werden konnte. Eine Sandbox-Analyse-Funktion bietet deshalb lediglich einen begrenzten vorausschauenden Schutz und dient vielmehr der Erkennung von Malware.

Bereits wieder unsicher

Doch auch der Wert der Erkennung sinkt bereits, da die die Autoren von Malware und die Kriminellen, die diese verbreiten, inzwischen verstanden haben, wie eine Sandbox-Analyse funktioniert. Entsprechend ändern sie das Verhalten ihrer Angriffsprogramme, damit sie nicht mehr so einfach erkannt werden können. Dazu können sie beispielsweise eine Eingabe des Benutzers fordern, die von der automatisierten Sandbox-Analyse-Komponente nicht geliefert werden kann. Im einfachsten Fall kann das ein vorgetäuschter Lizenzschlüssel oder ein Passwort sein, das in einer separaten Mail an den Empfänger gesendet wird. Ein Anwender in der Personalabteilung wird sich vermutlich nicht einmal wundern, wenn ein Bewerber seine Unterlagen als verschlüsseltes Archiv sendet und das zugehörige Passwort in einer separaten Mail liefert. Sofern die Bewerbungsunterlagen Schadcode enthalten, kann der PC des Mitarbeiters nun kompromittiert werden. Für eine Sandbox-Analyse-Komponente wird es allerdings schwierig, das richtige Passwort automatisch einzugeben und den Schadcode zu erkennen.

Sandbox-Analyse-Funktionen werden heute von zahlreichen Herstellern angeboten. Firewall-Hersteller wie **Check Point**[7] oder **Palo Alto Networks**[8] haben eigene Module für ihre Firewalls. **WatchGuard**[9] integriert die **Lösung von Lastline**[10] in seine Firewall. Der Proxy-Hersteller **Blue Coat**[11] hat dafür die Norman-Sandbox aufgekauft. Cisco bietet sein **FireAMP-Produkt**[12], und Hersteller wie **FireEye**[13],**Cyphort**[14], **AhnLab**[15], Lastline und andere haben

eigenständige Appliances beziehungsweise Software-Lizenzen.

Ausgehenden Traffic analysieren

Eine andere Technik fokussiert nicht so sehr das eingehende Objekt, sondern die ausgehende Kommunikation. Die Ursprungsidee ist hier, dass Malware regelmäßig Kontakt zu einem Command-and-Control-Server (C&C-Server oder auch C2-Server) aufbaut, um dort entweder ausgespähte Daten abzuliefern, sich selbst zu aktualisieren oder Befehle abzuholen. Malware verwendet dafür oft **DNS Tunneling**[16]. Das DNS-Protokoll ist für die Auflösung von Namen, beispielsweise aus URLs zu IP-Adressen, zuständig. Bei einem DNS Tunnel wird die ausgehende Kommunikation in DNS-Abfragen versteckt und die IP-Adresse der Antwort enthält die eingehenden Daten. Da die meisten Unternehmen die Auflösung von externen Namen im internen Netz erlauben, kann somit ein ungehinderter Datenaustausch erfolgen, der von klassischer Sicherheitstechnik in der Regel weder bemerkt noch behindert wird.

Ebenso kann die Kommunikation zwischen dem Schadcode im internen Netz und dem externen C&C-Server über HTTPS, sprich mittels verschlüsselter HTTP-Kommunikation, erfolgen.

Spezialisierte Sicherheitsprodukte versuchen, genau diese versteckte Kommunikation anhand ihrer speziellen Eigenschaften zu erkennen. Die häufige Änderung des Host-Anteils einer Namensauflösung, die Herkunft und das Alter der angefragten Domäne, die Menge der übermittelten Daten und viele weitere Details fließen dabei in eine Bewertung ein.

Bekannte Hersteller, die diese Technik implementiert haben, sind FireEye und **Damballa**[17], wobei letzterer hier seinen Schwerpunkt setzt.

Verhaltensanalyse

Neben der Analyse von eingehender und ausgehender Kommunikation kann man auch versuchen, Malware an seinem tatsächlichen Verhalten auf den Endgeräten zu erkennen. Zwar wird dafür zusätzliche Software auf den Arbeitsplatz-PCs der Mitarbeiter benötigt, zugleich ist die Erkennung jedoch genauer und weniger fehleranfällig. Die tatsächlichen Manipulationen und das Verhalten von Malware lassen sich direkt erfassen und bewerten. Entsprechende Produkte klinken sich typischerweise in den Betriebssystem-Kern des Endgeräts ein und überwachen dort jegliche Kommunikation und Systemänderung von Programmen. Malware, die sich in das System einnistet, Daten extrahiert oder weitere Komponenten nachlädt, ist auf diese Weise recht zuverlässig aufzuspüren.

Die größte Hürde beim Einsatz solcher Sicherheitssysteme ist der Einsatz eines weiteren Software-Agenten auf den Arbeitsplatz-PCs der Mitarbeiter. Das Verteilen der Software schreckt viele Unternehmen ab und macht Systeme, die nur an zentraler Stelle im Netzwerk angeschlossen werden müssen, scheinbar attraktiver. Wird jedoch auch der spätere Betriebsaufwand berücksichtigt, so relativiert sich der vermeintliche Vorteil einer netzwerkbasierten Lösung schnell. Bedingt durch die ungenaue Erkennung im Netz, kommt es immer wieder zu Alarmen, die dann mit hohem Aufwand auf

den Endgeräten verifiziert werden müssen. Allein dafür wünschen sich die Betriebsverantwortlichen bald eine zusätzliche Analysekomponente auf allen Endgeräten. Diesen Weg hätte man jedoch auch von Anfang an gehen können.

[Hinweis auf Bildergalerie: **Hacker auf dem Server**] gal3

Direkt auf dem Endgerät

Noch effektiver sind Lösungen, die auf dem Endgerät verteilt werden und nicht nur Malware erkennen und Alarm auslösen, sondern auch eine Kompromittierung des betroffenen Endgeräts verhindern. Dadurch sinkt der Aufwand im späteren Betrieb deutlich. Das erreichte Sicherheitsniveau ist zudem höher als bei einer Erkennungskomponente im Netz. Um dies zu erreichen, existieren mehrere technische Varianten am Markt: Sandboxing, Mikrovirtualisierung und Exploit Mitigation beziehungsweise **Host Intrusion Prevention (HIPS)**[18].

Sandboxing auf Endgeräten und Host IPS sind keine neuen Ideen. Bereits vor etwa 15 Jahren brachten Aladdin mit seinem eSafe-Enterprise-Produkt und Finjan mit seinem Surfin Shield Sandbox-System Lösungen auf den Markt, die sich in das Betriebssystem einklinkt, um Schadcode daran zu hindern, sich in das System einzunisten oder auf sensible Daten zuzugreifen. Einige Jahre später kam mit dem StormWatch-Produkt von Okena ein erstes bekannteres Host-IPS-Produkt auf den Markt.

Keines der Produkte hat bis heute überlebt, denn die Hersteller waren offensichtlich ihrer Zeit voraus und der Markt war noch nicht bereit für derartige Lösungsansätze. Auch die damals verwendeten Betriebssysteme auf PC-Arbeitsplätzen waren Teil des Problems. Das Einklinken von Virenscannern, Personal Firewalls, VPN-Clients und ähnlichen Agenten in ein 32-Bit Windows XP führte nicht selten zu Kompatibilitätsproblemen und Systemabstürzen. Für die Hersteller von Sicherheitslösungen ist es heute einfacher, denn Windows 7 oder Windows 8.1 sind an dieser Stelle anders strukturiert.

Aladdin ist inzwischen in **SafeNet**[19] aufgegangen und die eSafe-Produktlinie ist verschwunden. Die Finjan-Produkte wurden 2009 von M86 gekauft und M86 wurde wiederum 2012 von **Trustwave**[20] übernommen. Okena wurde von Cisco gekauft - das Unternehmen machte aus dem StormWatch-Produkt den **Cisco Security Agent** [21]und stellte ihn ein paar Jahre später ein.

[Hinweis auf Bildergalerie: **10 Dinge, die Sie nach der Installation von Windows 8.1 tun sollten**] gal4

Sandboxing und Host IPS

Die Grundideen von Sandboxing und Host IPS sind durchaus miteinander verwandt. In beiden Fällen wird der Zugriff von Applikationen auf Betriebssystem-Ressourcen kontrolliert beziehungsweise manipuliert. Bei Sandboxen wird versucht, der jeweiligen Applikation eine eigene gekapselte Welt vorzutäuschen. In dieser Welt kann die Applikation nahezu beliebig agieren. Manipulationen werden jedoch nicht auf das darunter liegende Betriebssystem übertragen und bleiben in der Sandbox. Bei einem Host IPS dagegen verzichtet man, vereinfacht gesagt, auf das Vortäuschen einer eigenen Welt

Stattdessen werden lesende oder schreibende Zugriffe, die eine Gefahr darstellen könnten, einfach geblockt oder die verursachende Applikation wird beendet.

[Hinweis auf Bildergalerie: **Anzeichen für einen Cyber-Angriff**] gal5

Heute lässt sich eine Renaissance dieser Ideen am Markt beobachten. Getrieben durch die zuvor beschriebenen Probleme ist der Bedarf an Sicherheitslösungen auf dem Endgerät gestiegen. Zudem hat die Vernetzung und Mobilität in Unternehmen in den letzten Jahren weiter zugenommen. Auch dies unterstützt den Trend, dass zentrale Sicherheitslösungen im Unternehmensnetz die Probleme nicht mehr allein lösen können.

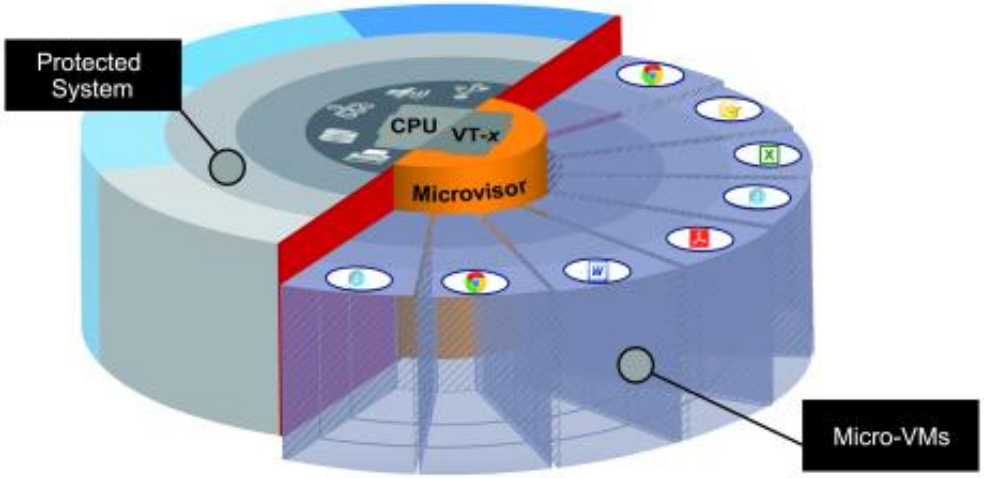
Der Hersteller Cyvera hat eine Idee aufgegriffen, die zuvor beispielsweise schon von eEye in seinem Blink-Produkt verfolgt wurde: das generische Erkennen und Verhindern der Ausnutzung von Sicherheitslücken mit Exploits.

eEye war jedoch ebenso wie Okena, Finjan oder Aladdin zu früh am Markt und konnte mit seiner Idee den Durchbruch damals nicht erreichen. Inzwischen wurde eEye von BeyondTrust übernommen und Blink fristet auch dort eher ein Nischendasein.

Cyvera dagegen wurde nach sehr kurzer Zeit von Palo Alto Networks gekauft. Das Unternehmen hat das Produkt in **Traps**[22] umbenannt und positioniert es zusammen mit der Netzwerk-Sandbox-Analyse **WildFire**[23] sehr aktiv als moderne Lösung gegen APTs.

Mikrovirtualisierung

Eine grundlegend neue Interpretation der ursprünglichen Sandbox-Idee findet man in der Mikrovirtualisierungstechnik, die vom Hersteller**Bromium**[24] erfunden wurde. Auch hier werden Applikationen in einer vorgetäuschten und gekapselten Umgebung "eingesperrt". Im Gegensatz zu klassischen Sandboxen, die bei Fehlern im Kern des Betriebssystems umgehbar sind, verwendet die Lösung von Bromium einen Hypervisor, der die Applikationen in einzelnen virtuellen Maschinen kapselt.



Bei Bromiums Lösung kapselt ein Hypervisor alle Applikationen in einzelnen virtuellen Maschinen. Foto: Bromium

Damit der Speicherbedarf der einzelnen virtuellen Maschinen insgesamt nicht zu einem Problem wird, hat Bromium im Gegensatz zu etablierten Virtualisierungslösungen eine "Copy-on-write"-Technik implementiert. So geht der Platzbedarf der einzelnen virtuellen Maschinen kaum über den Platzbedarf der Applikation selbst hinaus. Greift beispielsweise ein Anwender mit seinem Browser auf eine externe Website zu, so wird innerhalb von zehn Millisekunden eine neue Mikro-VM erzeugt. Sie kapselt die einzelne Browser-Session und sorgt dafür, dass Schadcode oder auch Angriffe auf den Flash Player, Adobe Reader oder andere Plug-ins nicht aus der virtuellen Umgebung ausbrechen können. Der Anwender bemerkt davon nichts und kann arbeiten wie zuvor auch.

Die Gründer von Bromium sind keine Unbekannten, sondern es handelt es sich um das Team, das auch maßgeblich bei der Entwicklung des Xen-Hypervisor vor vielen Jahren mitgewirkt hat. An Erfahrung mit Virtualisierungstechnik mangelt es dem Hersteller also nicht.

Was CISOs tun können

Die Herausforderung für den CISO besteht darin, bei den zahlreichen Sicherheitstechniken und in der geänderten Bedrohungslage den Überblick zu behalten und sein begrenztes Budget nicht in eher unwichtige Maßnahmen zu investieren. Leider korreliert der Hype um einzelne neue Hersteller nicht mit der Sinnhaftigkeit der jeweiligen Maßnahmen im einzelnen Unternehmen.

Der richtige Weg besteht darin, zunächst die individuell zu schützenden Objekte zu identifizieren. In manchen Unternehmen sind das vertrauliche Konstruktionsdaten, die die Grundlage des Geschäfts und den Vorsprung vor Mitbewerbern sichern. In anderen Organisationen ist die kontinuierliche Verfügbarkeit von Produktionsanlagen kritisch, während vertrauliche Daten vergleichsweise unspektakulär sind. Diese Situation variiert von Unternehmen zu Unternehmen.

[Hinweis auf Bildergalerie: **Alle Daten finden mit Gratis-Tools**] gal6

Im Anschluss sind die relevanten Bedrohungsszenarien zu betrachten. Dabei kann sich herausstellen, dass fortschrittliche Malware im Einzelfall gar kein wichtiges Thema ist, dass jedoch die Web-Plattform, ein Online-Shop oder ein Kunden-Portal bisher unzureichend geschützt sind. Die vorhandene Netzwerkstruktur, der Datenfluss im Unternehmen und die Bedeutung der jeweiligen IT-Systeme für

die Geschäftsprozesse müssen bei diesen Überlegungen berücksichtigt werden.

Erst dann ist eine Grundlage gegeben, um zu entscheiden, ob Sandbox-Analyse-Systeme, Mikrovirtualisierung auf den Arbeitsplätzen, Netzwerkzugangskontrolle im LAN oder eine WAF zur Absicherung der Web-Applikationen die richtige Lösung ist

Sollte sich bei dieser Analyse herausstellen, dass fortschrittliche Malware, gezielte Angriffe beziehungsweise APTs aktuell besonders große Bedrohungen sind, wird die Detailbetrachtung der verfügbaren Lösungsansätze spannend. Zwar mag die derzeit meistdiskutierte Technik der Sandbox-Analyse an zentraler Stelle im Netzwerk auf den ersten Blick als elegante und einfache Lösung erscheinen. Langfristig wird sie jedoch nur eine Nebenrolle spielen. Daher ist es empfehlenswert, diese Komponenten allenfalls als kostengünstige Erweiterung vorhandener Firewalls oder Proxies zu implementieren und früher oder später ohnehin notwendige Komponenten auf den Endgeräten mit höherer Priorität zu betrachten. (sh)