Die verschiedenen Arten von Cyberangriffen und was Sie dagegen tun können

E-BOOK

Einführung

Gewiefte Cyberkriminelle verfeinern ihre bereits komplexen Verschleierungsmethoden immer weiter, um unerkannt in Netzwerke einzudringen. Ihre Motive sind vielfältig, häufig auch finanzieller Natur. Sie zielen unter anderem darauf ab, geistiges Eigentum zu stehlen, Opfer auszuspionieren, Geschäftsprozesse zu stören oder Lösegeld für Dateien zu erpressen. Dabei nutzen sie modernste Techniken, um unbemerkt fremde Netzwerke zu infiltrieren und ihren bösartigen Aktivitäten nachzugehen.

Hat sich ein Hacker erfolgreich Zugang zu einem System verschafft, versucht er normalerweise, Malware zu laden und zu installieren. Oft kommen dabei neue Malware-Varianten zum Einsatz, die von herkömmlichen Virenschutzlösungen nicht erkannt werden.

Das vorliegende E-Book erläutert, mit welchen Angriffsstrategien und -tools Cyberkriminelle Ihr Netzwerk infiltrieren und was Sie tun können, um sie zu stoppen.

Cyberkriminelle sind sieben Tage die Woche rund um die Uhr aktiv.

Cyberangriffsstrategie 1 Dauerbombardement von Netzwerken mit Malware

Das Malware-Volumen wächst, wobei manche Länder mehrere Millionen Angriffe verzeichnen. Um Ihr Netzwerk zu kompromittieren, nutzen Angreifer alle möglichen Vektoren, wie E-Mails, Mobilgeräte, Webverkehr und sogar automatisierte Exploits. Die Größe Ihres Unternehmens spielt dabei keine Rolle. Für den Hacker sind Sie lediglich eine IP-Adresse, eine E-Mail-Adresse oder ein potenzielles Opfer für einen Watering-Hole-Angriff. Cyberkriminelle nutzen automatisierte Tools, mit denen sie rund um die Uhr Exploits ausführen oder Phishingmails versenden können.

Das Problem ist, dass viele Organisationen nicht über die richtigen Instrumente verfügen, um sich gegen die Angreifer zur Wehr zu setzen. Oft fehlen etwa automatisierte Tools, um den Datenverkehr zu durchleuchten, Endpunkte zu schützen oder bedenkliche E-Mails herauszufiltern. Manche Unternehmen nutzen Firewalls, die den verschlüsselten Verkehr nicht auf verborgene Bedrohungen überprüfen können, oder verlassen sich auf ihre begrenzten Systemspeicher, um Malware-Signaturen abzulegen.

Gegenmaßnahme 1
Schützen Sie Ihr Netzwerk zu jeder Tages- und Nachtzeit

Stündlich bringen Cyberkriminelle Hunderte brandneuer Malware-Varianten in Umlauf. Organisationen benötigen deshalb einen wirksamen Echtzeitschutz, um jederzeit gegen die neuesten Bedrohungen gewappnet zu sein. Effektive Sicherheitslösungen nutzen die neuesten Technologien, um Gefahren in Echtzeit zu erkennen und Unternehmen rund um die Uhr zu schützen. Aufgrund der großen Anzahl von Malware-Typen und -Varianten verfügt allerdings keine Firewall über genügend Speicher. Sicherheitsservices mit Technologien wie Real-Time Deep Memory Inspection (RTDMI™) sind in der Lage, breit angelegte Zero-Day-Bedrohungen und unbekannte Malware-Varianten aktiv zu erkennen und abzuwehren.

Firewalls sollten mit einer cloudbasierten Sandbox arbeiten, um einen größtmöglichen Einblick in Malware zu gewähren und brandneue Varianten zu identifizieren. Da Hacker IoT-Geräte als Einstiegspunkt nutzen können, ist es außerdem wichtig, dass Ihre Sicherheitslösung einen dynamisch aktualisierten Schutz nicht nur am Firewall-Gateway, sondern auch an mobilen und Remote-Endpunkten unterstützt.

Setzen Sie auf eine Sicherheitsplattform, die alle Vorteile der Cloud nutzt und eine automatisierte Lösung zur Echtzeiterkennung und -prävention der neuesten Malware-Bedrohungen bietet.

Cyberkriminelle nutzen alle möglichen Arten von Malware, um ihre Chancen zu erhöhen.

Cyberangriffsstrategie 2 Infizierung von Netzwerken mit verschiedenen Malware-Varianten

Cyberkriminelle nutzen verschiedene Angriffsvektoren und Malware-Varianten, um Netzwerke zu kompromittieren. Zu den fünf häufigsten Formen von Malware gehören Viren, Würmer, Trojaner, Spyware und Ransomware.

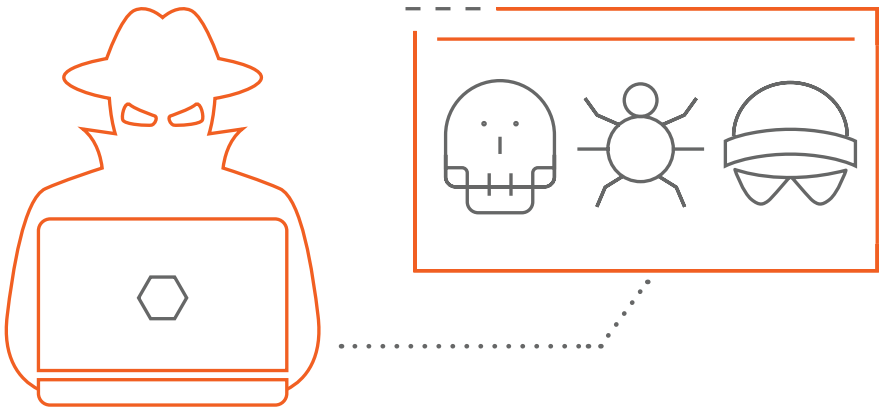
Ursprünglich wurden Computerviren durch die Weitergabe infizierter Datenträger verbreitet. Mit der Weiterentwicklung der Technik veränderten sich auch die Verbreitungsmethoden. Heute findet die Verbreitung von Viren üblicherweise durch reguläre Programme, Filesharing, Internetdownloads und E-Mail-Anhänge statt. Werden sie geöffnet oder ausgeführt, können verschiedene bösartige Aktionen ausgelöst werden, angefangen bei der Beschädigung von Daten bis hin zum Ausfall ganzer Systeme.

Computerwürmer existieren seit den späten 1980er-Jahren, traten aber erst mit dem flächendeckenden Einsatz von Netzwerken in Organisationen häufiger auf. Im Gegensatz zu Computerviren können sich Würmer ohne menschliches Zutun eigenständig in Netzwerken ausbreiten. Sie können schnelle Infektionen auslösen und somit Netzwerke mit Datenverkehr überlasten.

Trojaner sind bösartige Programme, die sich als unbedenkliche Software oder Dateien ausgeben. Sie sind speziell dafür konzipiert, sensible Daten in Netzwerken zu finden und zu erbeuten. Viele Arten von Trojanern übernehmen die Steuerung des infizierten Systems und öffnen dem Angreifer eine Hintertür für spätere Zugriffe. Häufig werden mithilfe von Trojanern mehrere Computer zu einem Botnet zusammengeschlossen.

Spyware ist in der Regel nicht schädlich, stellt jedoch ein großes Ärgernis dar, weil Webbrowser nach einer Infizierung oft kaum mehr funktionsfähig sind. Manchmal ist Spyware auch als seriöse Anwendung getarnt, die dem Benutzer bestimmte Vorteile vorgaukelt, während sie im Hintergrund Tastaturanschläge und Browserverlauf aufzeichnet, persönliche Daten stiehlt oder Benutzerverhalten und Nutzungsmuster ausspioniert. Die gestohlenen Daten werden dann wieder zum Angreifer übertragen, was die Privatsphäre und Sicherheit der Opfer gefährdet.

Ransomware ist eine Schadsoftware, bei der häufig die Dateien auf einem Endgerät oder kompletten Server verschlüsselt werden, sodass sie nicht mehr geöffnet werden können. Im Tausch gegen den Chiffrierschlüssel verlangen Cyberkriminelle von ihren Opfern Lösegeld, in der Regel in Form von Bitcoins. Verbreitet sich die Ransomware auf geschäftskritische Systeme, kann das Kosten im sechsstelligen Bereich oder höher bedeuten.



Setzen Sie auf einen mehrschichtigen Malware-Schutz, um Bedrohungen immer einen Schritt voraus zu sein.

Gegenmaßnahme 2
Schützen Sie Ihr Netzwerk vor den unterschiedlichsten Arten von Malware

Eine Firewall sollte Organisationen gegen sämtliche Arten von Cyberbedrohungen wappnen. Idealerweise vereint sie dazu alle Schutzmechanismen in einem latenzarmen Single-Pass-Ansatz, mit dem sich Angriffsvektoren nicht nur am Gateway, sondern auch an den Endpunkten außerhalb der traditionellen Netzwerkgrenzen blocken lassen. Folgende Funktionen sind besonders wichtig:

- Netzwerkbasierter Malware-Schutz: hindert Angreifer daran, Malware in ein kompromittiertes System zu laden oder zu übertragen
- Laufende und zeitnahe Updates: stellen sicher, dass Netzwerke vom ersten Augenblick an rund um die Uhr vor Millionen neuer Malware-Varianten geschützt sind
- Intrusion-Prevention-Service (IPS): verhindert, dass Angreifer Schwachstellen ausnutzen
- Sandboxing: verdächtiger Code wird an eine isolierte cloudbasierte Umgebung zur Detonation und Analyse weitergeleitet, um komplett neue Malware zu finden
- Zugriffssicherheit: der Benutzerzugriff auf mobile und Remote-Endpunkte wird mittels entsprechender Kontrollen gesteuert, sowohl innerhalb als auch außerhalb der Netzwerkgrenze
- E-Mail-Sicherheit: Blockieren von Trojanern sowie Phishing-, Spam- und Social-Engineering-Angriffen, die via E-Mail übertragen werden

Sie können Ihr Netzwerk noch besser vor Malware schützen, indem Sie jedes Gerät, das Zugriff darauf hat, mit einer aktuellen Virenschutzsoftware ausstatten. Um Cyberkriminellen das Leben schwerer zu machen, können Sie zudem PCs mit einer umfangreichen Virenschutzsoftware ausrüsten und mit Netzwerk-Firewalls kombinieren.

Cyberangriffsstrategie 3
Aufspüren und Infizieren schwacher Netzwerke

Viele Firewall-Anbieter werben zwar damit, dass ihre Lösungen einen erstklassigen Schutz vor Bedrohungen bieten, jedoch können sich im Praxiseinsatz nur wenige bewähren. Während sich Organisationen mit veralteten Firewalls in Sicherheit wiegen, umgehen gewiefte Hacker mithilfe komplizierter Algorithmen unzureichend ausgestattete Appliances und infizieren unbemerkt das Netzwerk.

Bei vielen Firewalls geht die Sicherheit zulasten der Performance. Nicht selten deaktivieren die Anwender deswegen Schutzfunktionen oder setzen die Sicherheitsstufe herab, um die benötigte Netzwerkperformance aufrechtzuerhalten – eine äußerst riskante Praxis, von der dringend abzuraten ist.

Eine weitere Schwachstelle in der Netzwerksicherheit ist der Faktor Mensch. Kriminelle sind darauf angewiesen, dass Personen durch falsche Aktionen oder Verhaltensweisen unbeabsichtigt die Integrität, Vertraulichkeit und Verfügbarkeit eines Netzwerks beeinträchtigen. Es gibt viele Faktoren, die Risiken begünstigen und die Sicherheit schwächen können, wie etwa Phishing-Betrug, Social Engineering, falsch konfigurierte Systeme, ungepatchte Software und ignorierte Sicherheitsregeln. Bedrohungsakteure nutzen diese gezielt, um an Anmelde- und andere Autorisierungsinformationen zu gelangen. Damit können sie Angriffe von innen heraus starten und so ganz einfach die Schutzmechanismen der Firewall umgehen. Hinzu kommt, dass Mitarbeiter hin und wieder ihre privaten Geräte mit dem Unternehmensnetzwerk verbinden, ohne geeignete Sicherheitsmaßnahmen zu beachten. Werden solche Geräte unbeaufsichtigt gelassen oder gehen sie verloren, können sich Dritte unerlaubt Zugriff verschaffen – für Organisationen ein deutliches Sicherheitsrisiko, wenn sie sich außerhalb der Netzwerk-Sicherheitsgrenze befinden.

> Cyberkriminelle wählen ihr Angriffsziel oft anhand der identifizierten Schwachstellen im Netzwerk.

> Alle Firewalls benötigen eine Engine, die Netzwerke vor internen und externen Angriffen schützt, und zwar ohne die Leistung zu beeinträchtigen.

Gegenmaßnahme 3
Wählen Sie eine umfassende Sicherheitsplattform mit überragendem Bedrohungsschutz, starker Performance und einer zentralisierten Verwaltung.

Sie sollten sich für Sicherheitslösungen entscheiden, die unabhängig getestet und für netzwerkbasierten Malwareschutz zertifiziert wurden.

Zusätzlich sollten Sie eine Multicore-Plattform in Betracht ziehen, mit der Sie Dateien jeder Größe und jeden Typs überprüfen und auf Änderungen im Datenverkehr reagieren können. Alle Firewalls benötigen eine Engine, die Netzwerke vor internen und externen Angriffen schützt, und zwar ohne die Leistung zu beeinträchtigen.

Achten Sie auch darauf, dass die Firewall eine cloudbasierte Sandbox bietet, um brandneue Malware aufzuspüren, die vielleicht auf Ihre Umgebung zielt. Können Sie ganz normal Ihren Geschäftsaktivitäten nachgehen oder werden Sie bald von Cyberkriminellen erpresst, ein Lösegeld für Ihre digitalen Ressourcen zu zahlen? Diese Entscheidungen könnten genau diesen Unterschied machen.

Wichtig ist auch, dass Ihre Sicherheitsstrategie mobile und Remote-Endpunkte sowohl innerhalb als auch außerhalb der Netzwerkgrenze schützt, um einen sicheren mobilen Zugriff zu ermöglichen.

Darüber hinaus sollte Ihre E-Mail-Security-Lösung Schutz vor Phishing-, Spam-, Viren- und Social-Engineering-Angriffen und anderen Bedrohungen bieten, die via E-Mail übertragen werden. Nutzen Sie Tools wie das kostenlose Phishing-Quiz von SonicWall, um Ihre Mitarbeiter für dieses Thema zu sensibilisieren.

Cyberangriffsstrategie 4
Weltweite Angriffe mit ständig neuen Malware-Varianten

Oft sind Cyberkriminelle mit ihren Angriffen erfolgreich, weil sie kontinuierlich neue Malware erfinden und mit ihren weltweiten Verbündeten austauschen – mit dem Ergebnis, dass alle paar Sekunden auf allen Kontinenten neue Sicherheitsbedrohungen auftauchen. Viele Hacker führen Blitzangriffe durch: Sie verschaffen sich Zugriff auf das System, nehmen, was sie bekommen können, und sind wieder weg, bevor jemand Alarm schlagen kann – und ehe Sie überhaupt merken, was passiert ist. Andere lassen sich mehr Zeit und versuchen, über einen längeren Zeitraum eine größere Menge an Daten zu erbeuten. Manche Angriffe werden über das Internet oder über E-Mails ausgeführt, andere zielen direkt auf das Netzwerk ab und nutzen infizierte Geräte, die sich zuvor außerhalb der Netzwerk-Sicherheitsgrenze befanden.

> Alle paar Sekunden tauchen auf allen Kontinenten neue Sicherheitsbedrohungen auf.

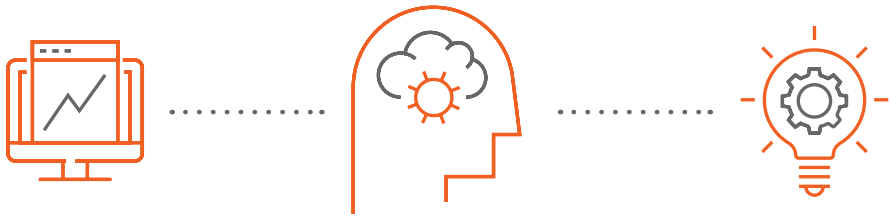
Rundumschutz vor den neuesten weltweiten Angriffen erhalten Sie nur mit einer Sicherheitslösung, die auf globale Bedrohungsdaten zurückgreift.

Gegenmaßnahme 4
Wählen Sie eine Firewall, die Schutz vor globalen Bedrohungen bietet

Für einen größtmöglichen Schutz ist es äußerst wichtig, schnell auf Bedrohungen zu reagieren. Achten Sie daher darauf, dass Ihr Anbieter von Sicherheitslösungen über ein eigenes Threat-Intelligence- und -Research-Team verfügt, das Abwehrmechanismen gegen neue Bedrohungen in kürzester Zeit implementiert. Außerdem sollte dieses Team mit anderen Experten aus der Security-Community zusammenarbeiten, um seine Reichweite zu vergrößern, wie etwa für den SonicWall Cyber Threat Report der Fall.

Breit aufgestellte Lösungen nutzen einen globalen cloudbasierten Malware-Katalog, um die lokale Firewall-Analyse zu ergänzen.

Einfache Firewalls identifizieren und blocken verdächtige Aktivitäten nach geografischer Region. Modernere Next-Generation-Firewalls blockieren auch den Datenverkehr aus gefährlichen Domains sowie eingehende und ausgehende Verbindungen zu verdächtigen Orten. So profitieren Sie zusätzlich von Funktionen zur Botnet-Filterung, die das Risiko durch bekannte globale Bedrohungen reduzieren.



Fazit

Für einen effektiven Schutz vor netzwerkbasierten Cyberangriffen brauchen Sie eine ganzheitliche Strategie, die starke Sicherheitspraktiken und wirksame Tools vereint. So können Sie ungewöhnliche Aktivitäten im Netzwerk aufspüren und angemessen darauf reagieren, ohne die Performance zu beeinträchtigen. Um Ihre Organisation vor unbekannten Bedrohungen zu schützen, müssen Sie sich proaktiv an die sich ständig verändernden Risiken anpassen.

Sie möchten wissen, welche Abwehrmechanismen sich am besten für die Anforderungen Ihrer Organisation eignen? Kontaktieren Sie einfach Ihren SonicWall-Ansprechpartner oder besuchen Sie uns auf unserer Website, um mehr über unsere Next-Generation-Firewalls (NGFWs) zu erfahren.

Weitere Informationen

Kontaktieren Sie uns, wenn Sie mit einem SonicWall-Sicherheitsexperten sprechen möchten.

Werfen Sie einen Blick auf unsere Livedemos für unsere SonicWall-Produktlinie.

Besuchen Sie unsere Webseite zu unseren Next-Generation-Firewalls.

Erhalten Sie aktuelle Informationen zu den neuesten Angriffen in unserem Capture Labs Security Center.

Über SonicWall

SonicWall bietet grenzenlose Cybersicherheit für eine extrem dezentrale Arbeitswelt, in der jeder remote, mobil und potenziell gefährdet ist. Durch die Identifizierung unbekannter Bedrohungen, moderne Echtzeit-Überwachungsfunktionen und eine herausragende Wirtschaftlichkeit hilft SonicWall großen Unternehmen, Behörden und KMUs weltweit, die Cybersicherheitslücke zu schließen. Weitere Informationen erhalten Sie unter www.sonicwall.de.

SonicWall, Inc.
1033 McCarthy Boulevard | Milpitas, Kalifornien 95035, USA
Weitere Informationen erhalten Sie auf unserer Website.
www.sonicwall.com

Ebook-TypesofCyberattacks-JK-8854