N-ABLE™

Diese 5 Cyberthreats sind zu raffiniert für herkömmliche Antivirenprogramme

E-Book

Inhaltsverzeichnis

Diese 5 Cyberthreats sind zu raffiniert für herkömmliche Antivirenprogramme

Der erste dokumentierte Computervirus war Creeper im Jahr 1971, der in einem akademischen Umfeld entwickelt wurde, um die Übertragungsfähigkeit einer Datei in einem Netzwerk zu demonstrieren. Erst nach geschlagenen sechs Monaten hatten Computerprogrammierer ein wirksames Antivirenprogramm namens Reaper geschrieben. Die Abwehr hinkte diesem ersten Angriff also gewaltig hinterher.

Seitdem sind Sicherheitsexperten und Computerprogrammierer im ständigen Wettlauf mit Bedrohungen und die Aufgabe unserer Branche ist es, diese zu ermitteln und immer neue Verteidigungsmaßnahmen zu ersinnen.

Viele herkömmliche Antiviren(AV)-Programme arbeiten signaturbasiert: Beim Ermitteln schädlicher Software legen sie eine Beschreibung der Datei an – die Signatur. Diese wird in eine Datenbank geschrieben, die auf das zu schützende System übertragen wird. Erkennt das Antivirenprogramm eine Datei auf Ihrem Rechner, die zu einer Signatur passt, so wird diese Datei in die Quarantäne verschoben oder entfernt. Im Dezember 2018 hatte Malware das bedrohliche Ausmaß von 350.000 neu erkannten Bedrohungen erreicht – pro Tag.[1] Angesichts stetig weiter steigender Zahlen stoßen signaturbasierte AV-Lösungen schnell an ihre Grenzen, dann sind Geräte nicht umfassend geschützt.

Die Entwicklung immer neuer Verteidigungsmechanismen bewirkt regelmäßig, dass auch die Kriminellen ihre Taktik ändern. Es ist ein ständiger Wettlauf. Zu den neuen Angriffsmethoden zählt Malware, die nicht nur Schwachstellen nutzt, sondern das Antivirenprogramm austrickst. Die Corona-Pandemie hat das Arbeiten im Homeoffice zum neuen Standard gemacht. Der Schutz von Geräten jenseits der Grenzen von Unternehmensnetzwerken ist dadurch wichtiger denn je geworden.

Homeoffice-Umgebungen sind jedoch viel anfälliger für Bedrohungen, zumal dann, wenn Endbenutzer nicht zu möglichen Gefahren aufgeklärt wurden. Im Zweifelsfall sind dann nicht nur die Daten des Benutzers, sondern auch das gesamte Unternehmen in Gefahr, und oft genug wird für aufgetretene Fehler der zuständige Managed Services Provider (MSP) verantwortlich gemacht. Morphisec zufolge erhielten 20 % der Angestellten, die ins Homeoffice wechselten, von der IT-Abteilung ihres Unternehmens vorab keinerlei Verhaltensanweisungen.[2] Ein alarmierendes Ergebnis, das zeigt: Unumstößliche Sicherheit ist heute so wichtig wie nie zuvor.

Von den genannten Gefahren abgesehen entwickeln sich vor dem Hintergrund der Corona-Pandemie neue Angriffswege, wie jüngste Untersuchungen ans Licht brachten. RiskIQ zufolge werden pro Minute 35 neue Spam-Mails entdeckt und 14,6 betrügerische Websites im Zusammenhang mit Corona erstellt.[3] Alle 15 Minuten wird eine dieser Corona-Domains gesperrt.[4]

[1] „Malware“, AV-TEST. https://www.av-test.org/de/statistiken/malware/ (aufgerufen September 2020).
[2] „Increasing Cybersecurity Gaps and Vulnerabilities due to Remote Work During COVID-19“, Security Magazine. securitymagazine.com/articles/92571-increasing-cybersecurity-gaps-and-vulnerabilities-due-to-remote-work-during-covid-19 (aufgerufen September 2020).
[3] „Evil Internet Minute 2020“, RiskIQ. riskiq.com/resources/infographic/evil-internet-minute-2020/ (aufgerufen September 2020).
[4] „Evil Internet Minute 2020“, RiskIQ. riskiq.com/resources/infographic/evil-internet-minute-2020/ (aufgerufen September 2020).

Gegen die folgenden fünf Angriffsarten sind herkömmliche Antivirenprogramme machtlos:

1. Polymorphe Malware

Wie eingangs erwähnt, stützen sich gängige AV-Programme auf die signaturbasierte Erkennung von bösartigem Code. Dabei wird eine Datei mit einem bekannten Eintrag in einer Bedrohungsdatenbank (also einer Signatur) verglichen.

Dieser Ansatz hat jedoch seine Schwächen: Der AV-Benutzer muss stets die aktuelle Signaturliste haben, sprich regelmäßige Updates durchführen. Sind die Virendefinitionen nicht auf dem aktuellen Stand, ist der Benutzer gegen neuere Dateien machtlos. Darüber hinaus ist diese Schutzmaßnahme rein reaktiv: Das AV-Programm muss die Signatur erst einmal kennen, bevor es sie der Liste hinzufügen kann. Doch Malware ist ja eigens so angelegt, dass sie von Schutzmaßnahmen nicht enttarnt wird.

Der gravierendste Nachteil bei diesem Ansatz besteht aber in der zeitlichen Verzögerung, bis der Schutz greift. Und genau hier setzt polymorphe Malware an: Wird Malware von einem Antivirenprogramm erkannt, dann generiert sie sich neu mit frischen Eigenschaften, die keiner bekannten Signatur entsprechen. Signaturbasierte AV-Programme haben so kaum eine Chance, der Infektion Herr zu werden. Außerdem werden Tag für Tag etwa 350.000 neue Malwarevarianten erstellt[5]. Mit signaturbasierter AV kann man also nur hinterherhinken.

2. Als Waffe genutzte Dokumente

Um ein System zu entern, nutzen Kriminelle auch Schwachstellen verschiedener Dokumentformate, insbesondere solcher, die eingebettete Skripte nutzen. In solchen Dokumenten verstecken Kriminelle dann ein bösartiges Skript oder Code. Selbst für das geübte Auge sieht eine solche Datei harmlos aus. Das AV-Programm schlägt nicht an, da es nur das Dokument selbst und nicht den Code oder das Skript nach der Ausführung scannt. Nach dem Start wird der Angriff ohne Wissen des Benutzers im Hintergrund ausgeführt.

Cyberkriminelle können mithilfe von Adobe® PDF-Dateien mit eingebettetem JavaScript® Betriebssystembefehle ausführen oder ausführbare Dateien herunterladen, um die geenterten Geräte und Netzwerke zu manipulieren. Mithilfe eingebetteter Skripte führen Hacker häufig PowerShell®-Befehle aus. Da PowerShell in das Windows®-Betriebssystem integriert ist, können dieses Angriffe nicht nur Endpunkte, sondern sogar ganze Netzwerke beschädigen. Aber PDF-Dateien sind nicht die einzige mögliche Schwachstelle: Auch XML-, HTML- und Office®-Dokumente können versteckte Skripte enthalten. Eine AV-Lösung, die sich auf den Vergleich ausführbarer Signaturen stützt, ist nicht in der Lage, solcherart manipulierte Dateien zu erkennen, da sie nur das Dokument selbst scannt, nicht den Schadcode, den es startet.

[5] „Malware“, AV-TEST. av-test.org/de/statistiken/malware/ (aufgerufen September 2020).

3. Schwache Browser: Drive-by-Downloads

Bei Drive-by-Downloads werden Dateien unter Ausnutzung von Schwachstellen im Browser oder einem Browser-Add-in auf den Endpunkt heruntergeladen – Antivirenprogramm und Benutzer merken nichts. Der Download kann dabei entweder von einer vertrauenswürdigen Website mit einem manipulierten Skript oder Werbedienst oder von einer bösartigen Website stammen, die speziell zum Start des Downloads dient. Ausgangspunkt für diese Angriffe: Phishing per E-Mail oder auf sozialen Medien oder auch gut getarnte Popup-Links, die den Benutzer zu einer Website leiten. Die Cyberkriminellen nutzen dann Exploits in Browsern oder Plug-ins, um die Malware herunterzuladen, und können danach angreifen und gehörigen Schaden anrichten – ob per Cryptominer, Remote-Access-Trojaner oder Ransomware.

4. Dateilose Angriffe

Die meisten Antivirenprogramme untersuchen Dateien, sobald diese auf ein Gerät gelangen. Wenn es jedoch gar keine Datei gibt, kann das AV-Programm auch nichts aufspüren.

Bei dateilosen Angriffen wird kein Schadcode auf dem System installiert. Das macht sie für AV-Programme so extrem schwierig zu erkennen. Ausgeführt werden sie meist im Arbeitsspeicher des Endgeräts. Zum Infizieren dienen dabei PowerShell, rundll32.exe oder andere integrierte Systemressourcen.

Dateilose Angriffe gehen häufig mit Dokumenten oder bösartigen Skripten auf einer Website einher, aber das ist längst nicht die einzige Möglichkeit, Geräte zu infizieren. Wenn beispielsweise ein Endpunkt RDP (Remote Desktop Protocol) aktiviert hat, bleibt ein Listening-Port offen, mit dem jemand eine Verbindung zum Gerät herstellen und Schaden anrichten kann – dateibasierte Malware herunterladen, Registryeinträge ändern oder Daten stehlen.

Und damit nicht genug: SentinelOne® ermittelte für das erste Halbjahr 2018 für dateilose Angriffe einen Anstieg um satte 91 %.[6] Aus diesem Grund müssen Unternehmen auf mehr als nur dateibasierte Angriffe achten, um ihre Daten und Systeme besser zu schützen.

[6] „Fileless Malware Attacks | How They Can Be Detected and Mitigated“, SentinelOne. sentinelone.com/blog/fileless-malware-attacks-can-detected-mitigated/ (aufgerufen September 2020).

5. Perfekt getarnte Malware

Die folgende Angriffstaktik ist nur ein weiteres Beispiel für den ständigen Wettlauf zwischen Sicherheitsexperten bzw. Programmierern und Cyberkriminellen. AV-Unternehmen setzen zur Malware-Erkennung verschiedene Verfahren ein, unter anderem das Sandbox-Verfahren, bei dem Dateien in einer abgeschotteten Umgebung ausgeführt und auf bösartiges Verhalten untersucht werden. Eine weitere gängige Maßnahme besteht darin, den Code auf typische Anzeichen für bösartige Absichten zu scannen.

Cyberkriminelle haben jedoch auch hier Mittel und Wege gefunden, das zu umgehen. So wie Sicherheitsexperten ihre Daten und Anlagen schützen, sind auch Hacker bestrebt, ihre „Ressourcen" zu schützen – den Schadcode in der Malware.

Neuere Malware erkennt Sandbox-Umgebungen und bleibt dort inaktiv; sie greift nur in einem Produktivsystem an. Dadurch ist es für das AV-Programm schlicht unmöglich, anhand von Verhaltensanalysen Malware in einer Sandbox-Umgebung zu entlarven.

Antivirenprogramme können auch mit sogenannten Packern umgangen werden, die die Datei so verschlüsseln und komprimieren, dass ihr Inhalt nicht inspiziert werden kann. Auch lässt sich Malware in harmlosen Code einbetten, um sie zu verbergen.

All diese Vorgehensweisen erschweren es Sicherheitsexperten und Programmierern, schädliche Dateien (und ihre verborgenen Mechanismen) überhaupt zu erkennen. Wird ein AV-Programm mit heuristischen Scans in einer Sandbox-Umgebung eingesetzt, dann hilft dies der Malware sogar noch, sich bis zum Einschleusen in das Produktivsystem zu tarnen.

Die Lösung: N-able

Zum Schutz vor modernen Bedrohungen brauchen MSP überlappende Sicherheitsmaßnahmen auf mehreren Ebenen, die die Gefahr, zum Opfer zu werden, auf ein Minimum reduzieren. N-able™ bietet zwei Plattformen für das Remote-Monitoring und -Management: N-able RMM und N-able N-central®. Mit beiden können Sie mehrstufige Sicherheit bei Ihren Kunden implementieren. Angenommen, der Virenschutz erkennt eine Bedrohung nicht. In diesem Fall haben Sie weitere Abwehrmechanismen zur Hand: Webschutz, damit keine schädlichen Websites besucht werden, E-Mail-Schutz zur Abwehr von Spam und Phishing und Patch-Management zum Schließen von Sicherheitslücken in Betriebssystemen und Anwendungen. Und ist ein Angriff wider Erwarten doch erfolgreich, können Sie Dateien und Systeme dank der integrierten Funktion für Backup und Wiederherstellung retten.

Beide Plattformen verfügen zudem über N-able Endpoint Detection and Response (EDR) mit SentinelOne. N-able EDR sorgt zuverlässig für die Vermeidung, Erkennung und Bekämpfung von Cyberangriffen auf die Endgeräte Ihrer Kunden. Sein signaturloser Ansatz ist herkömmlichen Antivirenprogrammen weit überlegen: Wartezeiten für Virenscans oder die Aktualisierung von Signaturdefinitionen entfallen hier. Im Falle eines Angriffs leitet die EDR die erforderlichen Schritte zur Eindämmung ein, beseitigt Angriffsspuren und versetzt die befallenen Endgeräte und Dateien automatisch wieder in einen einwandfreien Zustand zurück. Damit ist EDR also eine elegante Lösung, die erstaunlich einfach einzurichten und zu verwalten ist und zudem sämtliche Benutzer Ihrer Kunden auch ortsunabhängig absichern kann.

Über N-able

Mit N-able können Managed Services Provider (MSP) kleine und mittelständische Unternehmen effektiv bei der Digitalisierung unterstützen. Eine flexible Technologieplattform und leistungsstarke Integrationen erleichtern MSP die Überwachung, Verwaltung und Sicherung der Systeme, Daten und Netzwerke ihrer Endkunden. Unser wachsendes Portfolio an Sicherheits-, Automatisierungs- sowie Backup- und Wiederherstellungslösungen richtet sich an Fachleute für das IT-Servicemanagement. N-able vereinfacht komplexe Umgebungen und sorgt dafür, dass Kunden ihre Probleme selbst in die Hand nehmen können. Wir bieten umfassenden, proaktiven Support in Form von hilfreichen Partnerprogrammen, praktischen Schulungen und wachstumsfördernden Ressourcen. So können MSP hochwertige Services liefern und ihren Erfolg ausbauen.

n-able.com