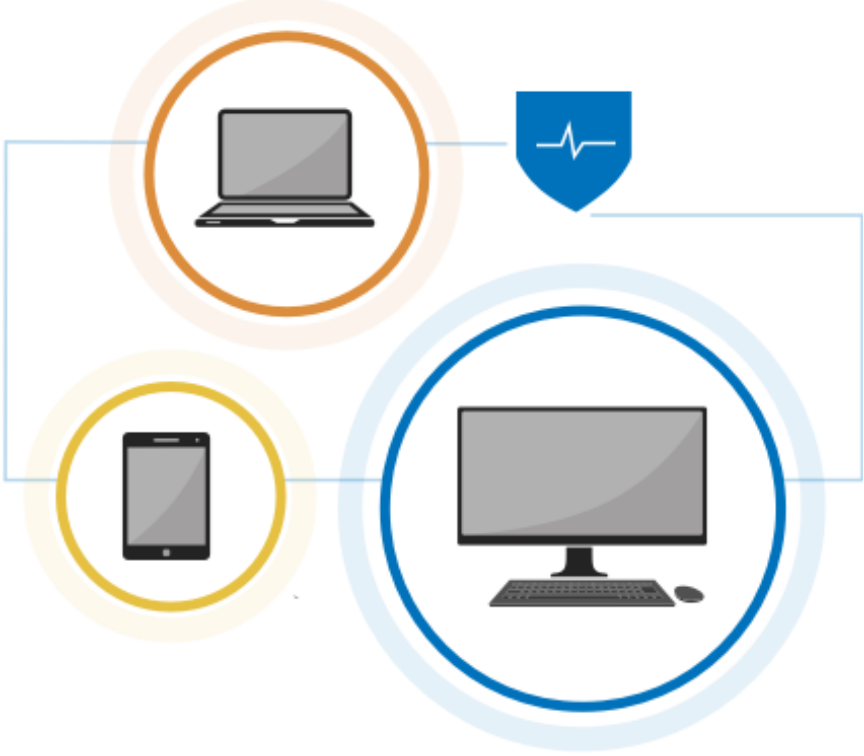
SOPHOS
Security made simple.



Next-Generation Endpoint Protection unter der Lupe

In diesem Whitepaper erfahren Sie, warum Sie Ihre Systeme und Benutzer mit Next-Gen Endpoint Protection schützen sollten. Außerdem erklären wir Ihnen, was eine Endpoint-Lösung können sollte, damit sie Ihrem Unternehmen bestmöglichen Schutz bietet.

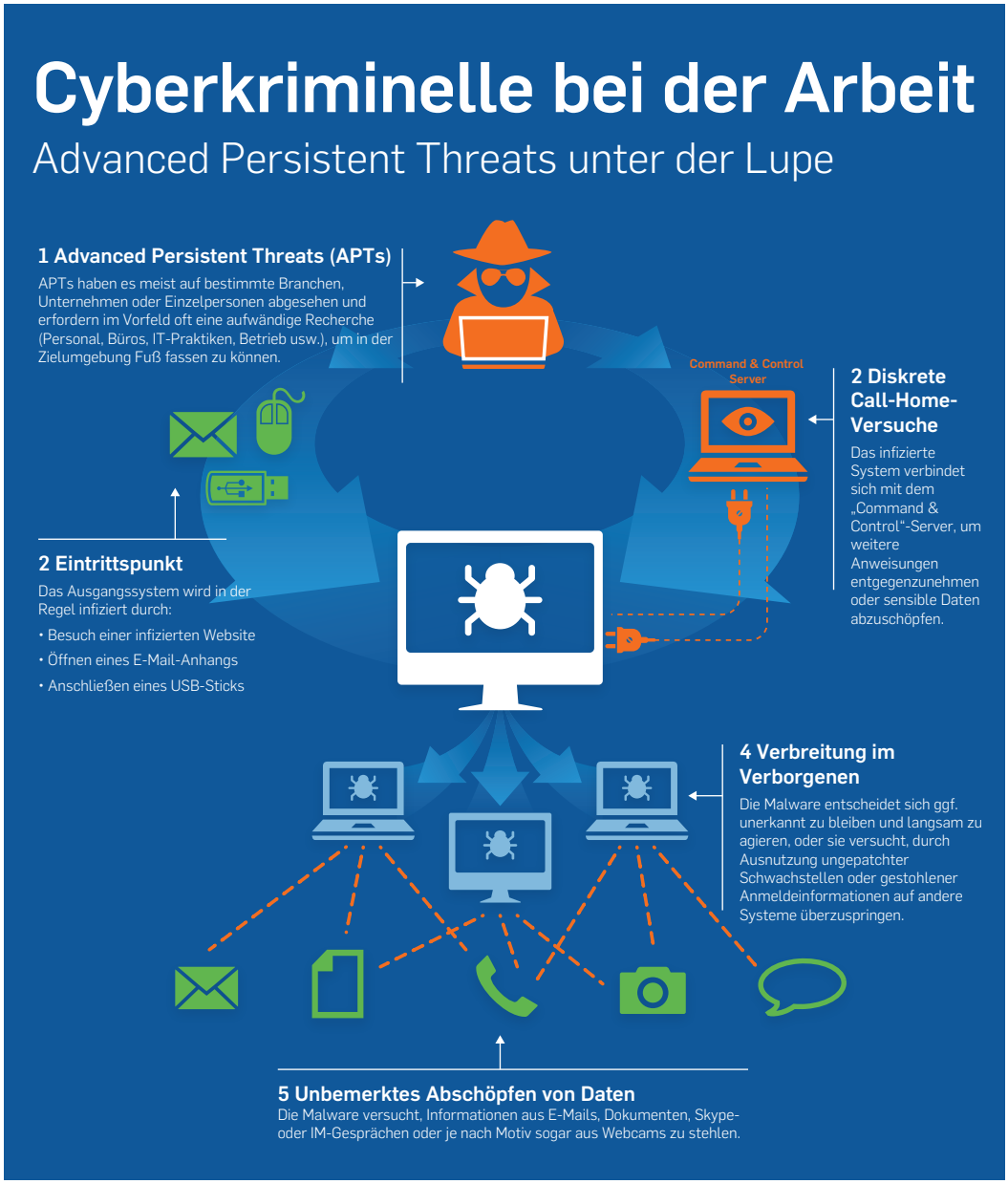
Sophos-Whitepaper April 2016

Bedrohungen auf dem Vormarsch

Advanced Persistent Threats (APTs) und Malware-Angriffe beherrschen mittlerweile tagtäglich die Schlagzeilen. Das Hollywood Presbyterian Medical Center in den USA musste beispielsweise 17.000 USD Bitcoin-Lösegeld zahlen, nachdem seine Daten verschlüsselt worden waren. Auch Krankenhäuser in Deutschland wurden bereits Opfer datenverschlüsselnder Ransomware.

Einer Studie der ISACA zufolge sind 33 % der Unternehmen zudem nicht davon überzeugt, dass sie auf ein durch APTs ausgelöstes Ereignis vorbereitet sind und auf dieses angemessen reagieren könnten[1].

Einer Studie der ISACA zufolge sind 33% der Unternehmen nicht davon überzeugt, dass sie auf ein durch APTs ausgelöstes Ereignis vorbereitet sind und auf dieses angemessen reagieren könnten[1].



Die beste Methode zum Schutz vor APTs ist ein gut abgesicherter Endpoint, auf dem eine Reihe verschiedener Abwehrverfahren dafür sorgen, dass nichts durchs Netz geht. Immer häufiger wird dieses Konzept durch ein koordiniertes Sicherheits-Setup ergänzt, bei dem mehrere Lösungen miteinander kommunizieren und Kontextinformationen austauschen. Auf diese Weise kann die Erkennung beschleunigt und die Reaktion automatisiert werden.

Was dürfen Unternehmen von einer Next-Gen-Endpoint-Lösung erwarten?

Leistungsstarker Schutz ist das Kernelement einer Next-Gen-Endpoint-Lösung und Unternehmen sollten auf leistungsstarke Technologien achten, die in allen Phasen eines Angriffs schützen:

1. **Abwehr:** Malware wird vor der Ausführung gestoppt
2. **Erkennung:** Malware wird erkannt, falls sie die Abwehr durchbrochen hat
3. **Reaktion:** Malware wird nach ihrer Erkennung sofort bekämpft

Leistungsstarke Schutzfunktionen allein sind jedoch nicht ausreichend. Um unter Realbedingungen effektiv zu sein, muss eine Next-Gen-Enpoint-Lösung Benutzer schützen, ohne sie bei der Arbeit zu behindern. Gleichzeitig muss die Lösung aber auch einfach konzipiert sein, sodass Unternehmen den erforderlichen Schutz erfolgreich implementieren können.

Sehen wir uns nun die Schutztechnologien genauer an.

Abwehr – Die erste Verteidigungslinie

Bei der Abwehr geht es darum zu verhindern, dass Malware überhaupt auf ein Gerät gelangt und die Gelegenheit erhält, Fuß zu fassen.

Ihre Endpoint-Lösung sollte Folgendes können:

Exposure Prevention

Web Protection
Sind Webseiten erwiesenermaßen schädlich, enthalten sie verdächtige Elemente?

Device Control
Welche Geräte (z. B. USB-Sticks) dürfen auf den Endpoint zugreifen?

Download-Reputation
Woher stammt die Datei, wer hat sie erstellt, wird sie auf anderen Systemen im Unternehmen verwendet?

Abwehr vor Ausführung

Dateianalysen/HIPS
Überprüfung der Komponenten/ Struktur der Datei, um festzustellen, ob Code enthalten ist, der versucht, die Registry zu manipulieren

Emulator
Ausführung der verdächtigen Datei in einer sicheren Umgebung zu Testzwecken

Signaturen
Schnelle Erkennung bekannter Malware

Erkennung – Malware auf frischer Tat ertappen

Bei der Erkennung kommen verschiedene Verfahren zum Einsatz: um Malware zu identifizieren, die auf ein Gerät gelangt ist, und um zu entscheiden, welche Maßnahmen zu ergreifen sind.

Achten Sie auf die folgenden Funktionen:

Laufzeit-Verhaltensweisen

Malicious Traffic Detection
Kommunizieren Prozesse mit bekannten Schadquellen („Call Home“)?

Speicherüberprüfung
Weist die verdächtige Datei Verhaltensmuster bekannter Malware auf?

Exploit-Erkennung
Katalogisiert der verdächtige Prozess den Speicher eines anderen Prozesses, schleust sich dieser selbst in das System ein?

Reaktion – Bereinigung und weitere Analyse

Bei der Reaktion geht es darum, die Malware rückstandsfrei zu beseitigen, zu gewährleisten, dass der Endpoint sicher ist, und Analysen zur Ermittlung des Eintrittspunkts der Malware durchzuführen.

Malware-Entfernung
Beseitigung der ausführbaren Datei und sonstiger Komponenten der Malware

Ursachenanalyse
Ermittlung der Malware-Ursache, um besser zu verstehen, was kompromittiert worden sein könnte

APTs vs. Endpoint

Das folgende Schaubild zeigt, wie ein typischer APT versucht, ein System zu infizieren, und welche Next-Gen-Endpoint-Funktion in jeder dieser Phasen präsent und aktiv sein sollte.

Exposition

Der APT versucht, sich Zugang zum Gerät zu verschaffen, um weitere Schritte zu unternehmen.

- Gerätekontrollen schränken den Zugriff auf den Endpoint ein (z. B. Blockierung des Zugriffs auf USB-Sticks und externe Festplatten)
- Web Protection prüft, ob Webseiten erwiesenermaßen schädlich sind
- Download-Reputation überprüft, wer die Datei erstellt hat, woher sie stammt und ob andere Systeme im Unternehmen sie nutzen

Exploit

Der APT sucht nach Schwachstellen auf dem Gerät, um sich einzubetten.

- Anwendungs-Lockdown lässt nur die Installation und Ausführung genehmigter Anwendungen auf dem Gerät zu
- Web Protection prüft, ob Webseiten erwiesenermaßen schädlich sind

Übertragung

Der APT versucht, seine Payload auf das Gerät zu übertragen.

- Sandbox-Emulation führt die verdächtige Datei in einer sicheren Umgebung aus, sodass diese getestet werden kann
- Dateianalysen/HIPS überprüfen die Komponenten und Struktur der Datei, um festzustellen, ob Code enthalten ist, der versucht, die Registry zu manipulieren
- Signaturerkennung fängt bereits bekannte Malware schnell und zuverlässig ab

Persistenz

Der APT versucht, auf dem Gerät Aktivitäten auszuführen.

- Exploit-Erkennung prüft, ob der verdächtige Prozess den Speicher anderer Prozesse katalogisiert und ob dieser sich selbst in das Gerät einschleust
- Web Protection prüft, ob Webseiten erwiesenermaßen schädlich sind
- Zu diesem Zeitpunkt sollten die meisten Arten herkömmlicher Malware bereits erkannt und entfernt worden sein

Ziele umsetzen

Der APT hat erfolgreich Fuß gefasst und arbeitet an der Umsetzung seiner Ziele.

- Verhaltensanalysen überprüfen die verdächtige Datei auf Muster bekannter Malware (auch bekannt als Speicherüberprüfung)
- Synchronized Security ermöglicht Austausch von Bedrohungsdaten zwischen Endpoint und Netzwerk. Die Reaktion erfolgt koordiniert und automatisiert. Die Daten von der Firewall ermöglichen dem Endpoint beispielsweise, das kompromittierte Gerät zu identifizieren und zu isolieren. Zu diesem Zeitpunkt wird die automatische Bereinigung aktiviert.

Command & Control

Vollständig etabliert kann der APT nun Call-Home-Aktivitäten starten.

- Malicious Traffic Detection sucht nach Prozessen, die mit bekannten Schadquellen kommunizieren
- Netzwerk-Lockdown isoliert kompromittierte Geräte vom Netzwerk, damit sich die Infektion nicht ausbreiten kann

Koordinierte Sicherheit oder Insel-Lösungen?

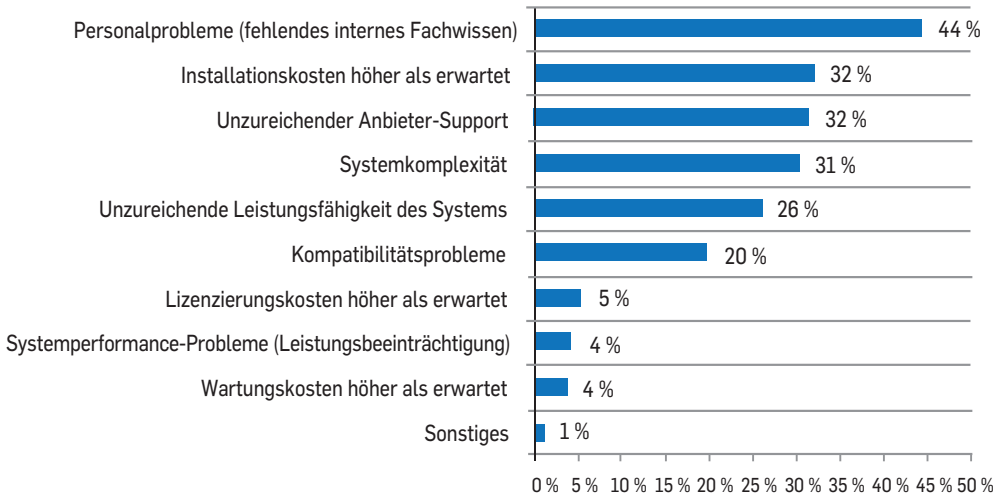
Unternehmen können Next-Gen Endpoint Protection auf zwei Arten bereitstellen: Als integrierte Lösung mit Schutz-, Erkennungs- und Bereinigungsfunktionen oder als komplexes Geflecht von Technologien, die manuell integriert werden müssen und ein manuelles Eingreifen zur Korrelation und Priorisierung von Benachrichtigungen erfordern.

Die größte Herausforderung bei der manuellen Integration besteht darin, dass zur Analyse der Daten von den verschiedenen Lösungen und zur Koordination der Reaktion ein manuelles Eingreifen erforderlich ist.

Ressourcen für die IT-Sicherheit abzustellen oder auch nur geeignete IT-Sicherheitsexperten zu finden, stellt viele mittelständische Unternehmen vor beträchtliche Herausforderungen.

Wie aus der Abbildung unten hervorgeht, ist der wichtigste Grund für die Unzufriedenheit mit Käufen von Sicherheitstechnologien fehlendes internes Sicherheitsfachwissen.

Abbildung 19: Warum Unternehmen einige ihrer Technologie-Investitionen bereuen. Zwei Antworten zulässig.



(Quelle: Ponemon Institute 2015, 2015 Global Study on IT Security Spending & Investments)

Die ISACA sagt weiter:

„IT-Fachkräften fehlen die erforderlichen Kenntnisse, um Technologien effektiv zu nutzen, die Bedrohung zu verstehen und Risikomanagement-Strategien, Tools und Richtlinien für die Cybersicherheit so aufeinander abzustimmen, dass APTs effektiv abgewehrt werden.[2]“

Leider adressieren viele traditionelle, aber sogar auch Next-Gen-Endpoint-Protection-Lösungen diese Problematik nur unzureichend. Diese Lösungen sind für sich genommen zwar durchaus wirksam, bieten Unternehmen jedoch nicht die koordinierten Funktionen zur Abwehr, Erkennung und Reaktion, die sie zur erfolgreichen Bekämpfung immer koordinierterer Angriffe benötigen.

Für ein unterbesetztes IT-Team kann eine solche unzureichend koordinierte Sicherheit den Unterschied zwischen einer effektiven Abwehr oder einem kompromittierten System bedeuten.

Selbst in gut besetzten IT-Teams von Großunternehmen können Sicherheitssysteme, die keine Informationen austauschen, zu doppelten Benachrichtigungen, erhöhtem Zeitaufwand bei der Analyse unbefugter Zugriffe und einer Fülle verschiedener Management-Konsolen führen.

Heute ist es wichtiger denn je, dass Sicherheitslösungen integraler Bestandteil der Unternehmens-IT sind und nicht nur ein Tool von vielen.

Sophos Next-Gen Endpoint Protection

Sophos Next-Gen Endpoint Protection schützt durch Kombination innovativer Sicherheitstechnologien, die über eine zentrale Kontroll-Engine koordiniert werden, in allen Phasen eines Angriffs. Das Ergebnis: optimaler Schutz vor Malware und komplexen Bedrohungen für Ihre Windows-, Mac- und Linux-Systeme.

- Beinhaltet Schutz vor komplexen Bedrohungen, Verhaltensanalysen, Host Intrusion Prevention, Web Security, Malicious Traffic Detection, Anti-Malware usw.
- Wehrt Infektionen ab, erkennt kompromittierte Systeme und beseitigt Bedrohungen mit Echtzeit-Bedrohungsdaten aus den SophosLabs
- Blockiert Schad-URLs und Web-Exploit-Code
- Erkennt und stoppt Kommunikationen von Endpoints mit Servern von Angreifern
- Analysiert Verhaltensweisen vor und nach der Ausführung und kann so bislang unbekannte Malware erkennen
- Liefert Web, Application und Device Control, komplett verwaltet über das intuitive, zentrale Verwaltungstool

Darüber hinaus ermöglicht Sophos Security Heartbeat™ der Sophos Next-Gen Endpoint Protection, Kontextinformationen in Echtzeit mit der Sophos Next-Gen Firewall auszutauschen. Diese synchronisierte Sicherheit („Synchronized Security“) bietet einzigartigen Schutz vor komplexen Bedrohungen und reduziert die Reaktionszeit bei Vorfällen erheblich.

Next-Gen-Endpoint-Security-Technologien sind nur dann ihr Geld wert, wenn Sie die Funktionen auch effektiv nutzen können. Deshalb gewährleistet Sophos Next-Gen Endpoint Protection eine einfache Konfiguration, Bereitstellung und Verwaltung. Die Lösung arbeitet außerdem mit blitzschneller Performance, sodass Kunden bei minimaler Beeinträchtigung – für Benutzer und IT-Manager – von maximalem Schutz profitieren.

Fazit

Eine effektive IT-Sicherheit war nie so wichtig wie heute, aber die verfügbaren Kenntnisse und Ressourcen sind oft sehr begrenzt. Sophos bietet eine effektive Alternative zu komplizierten Insellösungen, die sich einfach implementieren und verwalten lässt. Unternehmen sollten sich die Vorteile eines einzigen Endpoint Agents zur Abwehr, Erkennung und Reaktion vor Augen führen und eine „Synchronized Security"-Strategie erarbeiten, um ihren Schutz und ihre Reaktion bei Sicherheitsvorfällen zu optimieren.

Quellenangaben

[1]*ISACA 2015, 2015 Advanced Persistent Threat Awareness – Third Annual*

[2]*ISACA 2015, 2015 Advanced Persistent Threat Awareness – Third Annual*

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

Oxford, GB | Boston, USA

11.04.2016 WP-DE (MP)

SOPHOS