ENDPOINT PROTECTION SOLUTIONS REPORT 10/17

Autoren: Kevin Börner, Markus Reiniger, Daniel Vollmer

Endpoint-Security-Lösungen müssen sich ständig neuen Bedrohungslagen anpassen um Benutzer, Systeme, Daten und letztlich Unternehmen zu schützen. Der Schutz des Endpunktes stellt meist die letzte Verteidigungslinie dar. Im vorliegenden Report werden die Hersteller aktueller und schon länger am Markt bestehenden Antiviruslösungen mit relativ neuen sogenannten Next-Generation Lösungen verglichen. Hierbei stellt sich die Frage: Ist die Erkennungsrate traditioneller AV-Produkte weiterhin ausreichend oder bieten neue Lösungen mit neuartigen Ansätzen und Technologien einen nennenswerten Vorteil im Schutz vor bekannter, unbekannter und neuer Malware?

EPSR, Oktober 2017

Bei diesem Report handelt es sich um die dritte Ausgabe. Gegenüber den vorherigen Reports wurden noch mehr Malware-Samples gesammelt, um den Ergebnissen eine noch höhere Aussagekraft zu verleihen. Ebenfalls sind die getesteten AV-Produkte auf die letztverfügbaren Versionen aktualisiert worden.

Das Ergebnis der Untersuchung ist eindeutig: Next-Gen-Lösungen bieten gegenüber den klassischen AV-Lösungen eine signifikant höhere Erkennungsrate bei deutlich niedrigerer Belastung der Systemressourcen.

Next-Gen-Lösungen sind meist von Grund auf neu entwickelte Produkte die mithilfe von Künstlicher Intelligenz (KI), Verhaltensanalyse und intelligenter Prozessüberwachung den Schutz sicherstellen. Hierbei ist irrelevant ob es sich um bekannte oder unbekannte Malware handelt. Die Produkte arbeiten signaturlos und bieten eine Unterstützung für die gängigsten Betriebssysteme und Plattformen (Windows, Linux, Mac).

Alle Produkte sind als AV-Hersteller bei Microsoft registriert. Die Testszenarien beziehen sich alleine auf den Schutz vor Schadcode. Die Samples befinden sich zu Testbeginn bereits auf den Testsystemen. Weitere relevante Schutzkomponenten zur Abwehr von Cyberangriffen wie unter anderem Browserschutz, Schutz vor maliziösen E-Mails und Perimeterschutz werden in diesem Test nicht betrachtet. Des Weiteren ist auch der Test zum Schutz vor Exploits kein Bestandteil dieses Reports.

UNTERSUCHTE LÖSUNGEN

Next-Generation-Lösungen

CylancePROTECT in der Version 1450 (2.0.1450.8)
Cylance setzt bei der Erkennung von Malware und Exploits hauptsächlich auf KI mit maschinellem Lernen. Die KI erkennt durch statische Analyse von Executables und DLLs ob eine Datei gut- oder bösartig ist und das ohne die Datei ausführen zu müssen (pre-execution und predictive). Zusätzlich zur KI nutzt Cylance weitere Schutzmodule und Funktionen um den Endpunkt zu schützen, wie z.B Script Control zum Schutz vor Scripten oder Macros, wie sie häufig bei Ransomware-Angriffen genutzt werden oder Memory Protection um vor Exploits in Software zu schützen.

Palo Alto Networks Traps Advanced Endpoint Protection 4.1 (v4.1.0.28239, 21-1729)
Traps ist Teil der Security Plattform von Palo Alto Networks und schützt vor bekannten und unbekannten maliziösen Executables, DLLs und Office-Dateien mit einem einzigartigen Multi-Method-Präventionsansatz. Dieser Ansatz maximiert den Schutz gegen unbekannte Malware und Exploits und reduziert gleichzeitig die Angriffsfläche.

Durch das Kombinieren von verschiedensten Präventionsmethoden wird ermöglicht, Malware vor der Kompromittierung eines Systems zu blockieren. Skriptbasierte Angriffe werden out-of-the-box verhindert.

Das Herzstück des Clients zur Malware-Prävention ist die Local Analysis welche ohne klassische Signaturen, Scan Funktion oder Verhaltensanalysen das System schützt. Hierfür werden Hunderte von Datei-Eigenschaften in Echtzeit durchsucht. Auf Basis dieser Eigenschaften wird mittels Machine-Learning ein Verdict ermittelt, ob eine Datei gut- oder bösartig ist. Ransomware wird von Traps bei Erkennung eines Angriffs sofort gestoppt und das Verschlüsseln der Daten unterbunden. Die Multi-Method-Exploit-Prevention soll das Ausführen von Exploits mit den Modulen Pre-Exploit-Protection, Technique-Based-Exploit-Prevention und Kernel-Exploit-Prevention verhindern.

Sophos Endpoint Protection 2017 (11.5.6) mit Intercept X (3.7.0)
Intercept X erweitert den Sophos Anti-Viren-Schutz um Threat- und Exploit-Erkennung. Unerlaubte Verschlüsselungsaktivitäten (wie z.B bei Ransomware) werden durch ein Modul, genannt CryptoGuard, verhindert. Intercept X soll durch diese Technologien Zero-Day-Malware erkennen, im Vorfeld verhindern und damit den signaturbasierten AV-Schutz ergänzen.

Etablierte Lösungen

Kaspersky Endpoint Security 10 (10.3.0.6294)
Kaspersky Endpoint Security bietet Schutz für den PC, Mac und für mobile Endgeräte. Die Schutzmodule sind ähnlich wie bei Symantec EP 14. Es ist ein AV-Scanner mit Signaturdatenbank integriert und zusätzlich besteht die Möglichkeit einer heuristischen Analyse von Dateien. Des Weiteren sind Module wie Password Manager, Schutz für mobile Geräte, Firewall und eine Programmkontrolle integriert.

McAfee Endpoint Security 10.5 (10.5.2.2041)
McAfee bietet zusätzlich zu seinem AV-Scanner nun auch Machine-Learning-Techniken an. Diese teilen sich in Statische- und Verhaltensanalysen auf. Außerdem werden Firewall-Module und eine Webkontrolle mit dem Schutz verknüpft. Das Threat-Prevention-Modul soll außerdem Schutz vor Exploits bieten.

Symantec Endpoint Protection Cloud 22 (22.10.1.10)
Symantec bietet viele neue und verbesserte Erkennungsfunktionen zusätzlich zur klassischen Signaturdatenbank. Es werden Module wie beispielsweise Verhaltensanalysen, maschinelles Lernen und statische Analysen genutzt, um Malware zu erkennen.

Trend Micro Office Scan 12 (12.0.1556)
Office Scan nutzt wie alle herkömmlichen Lösungen einen AV-Scanner auf Basis von Signaturen. Seit der neuesten Version werden zusätzlich maschinelle Lernverfahren genutzt, die vor der Ausführung Dateien analysieren sollen. Ebenso werden Verhaltensanalysen von Skripten und Browser-Angriffen durchgeführt.

Windows Defender von Microsoft (1.251.959.0)
Windows Defender bietet einen herkömmlichen AV-Scanner mit zusätzlich weiteren Features wie einer integrierten Firewall. Das Programm stellt eine schlanke und vor allem integrierte und kostenfreie Alternative dar.

Alle getesteten Lösungen bieten eine zentrale Management-Konsole (in der Cloud und / oder On-Premise). Eine Ausnahme hierbei ist lediglich der Windows Defender, der als integriertes Produkt von Microsoft Windows keine zentrale Managementkonsole bietet.

TESTKRITERIEN UND METHODIK

Testaufbau

Die Anzahl der getesteten Malware Samples wurde im Vergleich zum vorherigen Report stark erhöht. Insgesamt wurden in einem ersten Durchgang Basis Test und im zweiten Testszenario Holiday Test jeweils 8000 Malware Samples genutzt. Beim Basis Test sind die 8000 Samples alle zunächst offline getestet und anschließend online getestet worden. Die Maschinen wurden zwischen den Tests zurückgesetzt.

Ein Viertel der Samples sind hierbei im Original aus den unten genannten Quellen heruntergeladen worden. Diese Samples wurden nach Analyse anschließend mehrfach verändert (Obfuscation) und damit auf drei verschiedene Arten mutiert. Dies soll unbekannte bzw. Zero-Day-Malware simulieren.

Diese Dateien werden dann meist nicht mehr von signaturbasierten Methoden erkannt. Für eine einfache Mutation wurde der Hashwert der Dateien geändert. Für die beiden erweiterten Mutationen wurden Packtechniken für ausführbare Dateien, mithilfe von Softwarepackern wie UPX und mPress, genutzt. Der Basis Test nutzte demnach 2000 Originale Dateien, 2000 Hash veränderte Dateien, 2000 UPX gepackte Dateien und 2000 mPress gepackte Dateien.

Testmethodik

Basis Test
Das Schlüsselkriterium für den Basis Test der Endpoint-Security-Lösungen war die Erkennungsrate (Wirksamkeit). Alle Endpoint-Security-Lösungen wurden unter gleichen Bedingungen im iT-CUBE Testlabor in einem Zeitraum von 14 Tagen wie folgt getestet:

- Sofern vorhanden, wurden mittels Update-Funktion die Signaturdatenbanken der Lösungen und alle anderen Module auf den aktuellsten Stand gebracht.
- Um die AV-Lösungen auch auf Reputationsdatenbanken, Intelligenz in der Cloud und Sandboxen zugreifen zu lassen, wurde ein Internetzugriff ermöglicht.
- Mittels Scanfunktion wurden die Malware Samples vor der Ausführung gescannt und die Erkennungsrate ermittelt.
- Im Anschluss wurden die verbleibenden Samples ausgeführt (Execution Test).
- Damit die ausgeführte Malware z.B C2-Kommunikation ausführen und weiteren Schadcode nachladen konnte wurde ein Internetzugriff ermöglicht (Erkennungsrate Online).
- Zusätzlich wurde ein Test mit allen Samples ohne Internetzugriff durchgeführt (Erkennungsrate Offline).
- Die getesteten Malware-Samples bestanden aus einem Mix von ca. 50% Ransomware, 20% Trojaner, 10% Zero Day und 20% sonstiger Malware. Die Samples wurden in einem Zeitraum von 14 Tagen gesammelt.
- Die genutzten Samples stammen aus verschiedenen öffentlichen Quellen: *http://malwr.com, http://dasmalwerk.com, http://malc0de.com/database, http://testmyav.com, http://virustotal.com*

Holiday Test
Das zweite Testszenario stellt den Holiday Test dar. Dabei wurden die Testgeräte 14 Tage vor Start des Tests vom Internet getrennt und nicht mehr aktualisiert. Anschließend wurden die 8000 Malware Samples auf die Systeme kopiert und gescannt. Dieser Test stellt ein realitätsnahes Szenario dar, bei dem der Mitarbeiter bspw. aus dem Urlaub zurückkehrt und sich, bevor die Signaturdatenbanken aktualisiert werden konnten, mit Malware infiziert. Der Test soll die Erkennungsraten in Abhängigkeit zu Signaturdatenbanken darstellen. Internetzugriff war hierbei prinzipbedingt nicht eingerichtet.

ERGEBNISSE UND INTERPRETATION

Next Generation Lösungen

Die Next-Gen-Lösungen von Palo Alto Networks mit Traps und Cylance mit CylancePROTECT erreichten durchweg sehr hohe Erkennungsraten (Traps 99,8% und Cylance 99,7%). Sophos mit Intercept X erreichte dabei 87,3%.

Der Holiday Test bestätigt die Effektivität der signaturlosen Ansätze von Palo Alto Networks und Cylance. Andere Lösungen bieten keinen ausreichenden Schutz ohne beständiges Updaten ihrer Signaturdatenbanken oder Internetzugriff.

Wie die Ergebnisse zeigen, konnte durch den erweiterten Multi-Methoden Präventionsansatz, neue Content Updates und den neuen Anti-Ransomware Schutz der Version 4.1 Palo Alto Networks Traps seine Erkennungsleistung weiter verbessern.

Der Reifegrad des KI-Modells von CylancePROTECT zeigt erneut hohe Verlässlichkeit und durchweg sehr gute Erkennungsraten und das, ohne die Ausführung einer Datei.

Konventionelle AV-Lösungen

Bei den konventionellen AV-Lösungen wäre die alleinige Nutzung der Signaturdatenbank nicht ausreichend gewesen und hätte beispielsweise bei Trend Micro eine Erkennungsrate von lediglich 25% erzeugt. Durch die zusätzlichen Module und Technologien wie statische Analyse, Verhaltensanalyse und Vertrauchlichkeitsabfragen werden teilweise signifikant höhere Raten von 70% bis 90% (Symantec und Kaspersky) erreicht. Diese liegen jedoch noch immer weit hinter den Endpoint-Lösungen von Palo Alto Networks und Cylance zurück.

Enttäuschend waren die Testkandidaten McAfee und Trend Micro. Trotz neuartiger Technologien und Module konnten beide keine zufriedenstellenden Erkennungsraten erreichen. Die Produkte konnten daher nicht überzeugen.

Der Windows Defender, als kostenloser Schutz integriert in Microsoft Windows, wurde als Referenz mit in den Test aufgenommen. Erstaunlicherweise konnte der Windows Defender teilweise andere Hersteller überbieten.

LÖSUNGEN IM VERGLEICH – BASIS TEST

Lösung	Szenario			
	Erkennungsrate vor Ausführung offline	**Erkennungsrate** vor Ausführung online	**Erkennungsrate** nach Ausführung offline	**Erkennungsrate** nach Ausführung online
Palo Alto Networks Traps 4.1.0	*Siehe **	*Siehe **	**99,81%**	**99,79%**
CylanceProtect 1450	**98,66%**	**99,73%**	**98,66%**	**99,73%**
Kaspersky Endpoint Security 10	**75,84%**	**76,30%**	**93,88%**	**94,24%**
Sophos Endpoint Protection 2017 (11.5.6) mit Intercept X (3.7.0)	**53,38 %**	**72,06 %**	**65,73 %**	**87,34 %**
Symantec Endpoint Protection Cloud	**51,06 %**	**56,31 %**	**60,13 %**	**68,48 %**
McAfee ENS 10.5	**45,40 %**	**47,05 %**	**60,25 %**	**63,81 %**
TrendMicro OfficeScan	**25,13 %**	**28,19 %**	**55,41 %**	**59,39 %**
Windows Defender	**37,90 %**	**38,16 %**	**48,05 %**	**48,38 %**

** Eine Scanning Funktion existiert zurzeit für Standard und Golden-Images. Roadmap Sessions werden auf Anfrage mit Palo Alto Networks organisiert.*

LÖSUNGEN IM VERGLEICH – HOLIDAY TEST

Lösung	Szenario
	Erkennungsrate Offline im Holiday Test-Szenario
Palo Alto Networks Traps 4.1.0	**99,81 %**
CylancePROTECT 1450	**98,66 %**
Kaspersky Endpoint Security 10	**75,59 %**
Sophos Endpoint Protection 2017 (11.5.6) mit Intercept X (3.7.0)	**47,30 %**
McAfee ENS 10.5	**45,21 %**
Trend Micro OfficeScan	**25,26 %**
Symantec Endpoint Protection Cloud	**17,04 %**
Windows Defender	**11,81 %**

Alle Werte wurden erhoben unter den genannten Testbedingungen. Abweichungen von 1% können nicht ausgeschlossen werden.

iT-CUBE SYSTEMS AG • Paul-Gerhardt-Allee 24 • 81245 München • info@it-cube.net • +49(0) 89 2000148 00

SYSTEMRESSOURCENVERBRAUCH

Zur Bewertung der verbrauchten Systemressourcen wurden CPU- und Arbeitsspeicherauslastung der zu der jeweiligen Lösung gehörenden Prozesse überwacht und gemessen. Die Systemauslastung ist naturgemäß bei einem laufenden Angriffsversuch höher. Hierbei zeigten sich allerdings erhebliche Unterschiede, wie stark die Belastung zunimmt. Bei einigen Produkten waren mehr als 20 Prozesse für den Betrieb der Endpoint Lösung aktiv. Dies wirkte sich auch negativ auf die Gesamtauslastung des Systems aus.

CylancePROTECT und Palo Alto Networks Traps verbrauchen sehr wenige Systemressourcen – im normalen Betrieb ca. 1% CPU-Last und bei einem laufenden Angriff maximal 10% CPU-Last. Gleiches gilt für die Arbeitsspeichernutzung, die im Bereich von 20-50 MB maximal liegt.

Alle anderen getesteten Lösungen verbrauchen weit mehr Systemressourcen.

Sind die Lösungen im normalen Betrieb mit 2-4 % noch recht genügsam, erhöht sich bei einem Angriffsversuch die CPU-Last auf bis zu 100% und mehrere hundert Megabyte bis teilweise einige Gigabyte Arbeitsspeicher werden benötigt. Dies macht den Rechner zumindest für die Zeit des Angriffs praktisch unbrauchbar.

ZUSAMMENFASSUNG

Die Ergebnisse des Tests zeigen besonders bei den neuen Versionen eine teils signifikante Steigerung der Erkennungsraten. Dabei konnten sich die Next-Generation-Lösungen der Hundertprozent-Marke noch ein Stück weiter nähern, als in den beiden vorangegangenen Tests. Allerdings gab es auch im übrigen Testfeld Fortschritte.

Weiterhin konkurrenzlos sind die neuen Lösungen in Hinsicht auf den Resourcenverbrauch. Hier schneidet die neue Generation erheblich besser ab als jede etablierte Lösung im Testfeld.

Zusammenfassend zeigt das folgende Diagramm die Ergebnisse in Bezug auf die Gesamtperformance.