KASPERSKY lab

Ein Leitfaden zur aktuellen Bedrohungslage

www.kaspersky.de/business-security
#truecybersecurity

Kaspersky®
Endpoint Security
for Business

Ein Leitfaden zur aktuellen Bedrohungslage

Je weiter die digitale Transformation von Unternehmen auf der ganzen Welt voranschreitet, desto stärker sind sie auf ihre IT-Systeme angewiesen. Gleichzeitig versuchen Cyberkriminelle global, neue und innovative Tools und Ansätze zu entwickeln oder alte Tools umzufunktionieren, damit ihre Cyberangriffe die Erkennung umgehen. Durch die steigende Komplexität fortschrittlicher Bedrohungen verfolgen immer mehr IT-Abteilungen einen vorfallsbasierten Sicherheitsansatz – eine Tatsache, die die großen Herausforderungen verdeutlicht, mit denen Unternehmen und Sicherheitsanbieter zu kämpfen haben.

Für Großunternehmen auf der ganzen Welt liegen die durchschnittlichen Kosten einer Datenschutzverletzung bei knapp über 1,2 Mio. US-Dollar, was einem Anstieg von 24 Prozent seit 2017 und 38 Prozent seit 2016 entspricht. Jedes Unternehmen kann Opfer eines Angriffs werden, denn so etwas wie 100-prozentige Sicherheit gibt es nicht. Organisationen können jedoch verschiedene Schritte unternehmen, um sich vor Bedrohungen zu schützen. In diesem Dokument gehen wir davon aus, dass Sie bereits standardmäßigen Schutz in Ihrem Unternehmen implementiert haben, und stellen Ihnen einige der am weitesten verbreiteten Bedrohungen vor. Hierbei erfahren Sie, welche Schäden die einzelnen Bedrohungen anrichten und mit welchen fortschrittlichen Technologien Sie sich davor schützen können.

Für Großunternehmen auf der ganzen Welt liegen die durchschnittlichen Kosten einer Datenschutzverletzung bei knapp über 1,2 Mio. US-Dollar, was einem Anstieg von 24 Prozent seit 2017 und 38 Prozent seit 2016 entspricht.

Dateilose Bedrohungen: Erfolg durch Tarnung

Im Gegensatz zu Bedrohungen, die heruntergeladen und ausgeführt werden, werden dateilose Bedrohungen im Systemspeicher ausgeführt. Da sie statt auf der Festplatte im Code des Arbeitsspeichers enthalten sind und sich auch in der Windows-Registrierung bzw. der Windows-Verwaltungsinstrumentation verstecken können, sind sie nur schwer zu erkennen und entgehen oftmals klassischen Virenschutztools und Intrusion Prevention Systems. Ein Benutzer besucht eine schädliche Webseite, klickt auf eine Fake-Werbung, die Malware enthält, und schon beginnt die Ausführung ...

Dateilose Angriffe sind 10 Mal häufiger erfolgreich als dateibasierte: 77 Prozent der erfolgreichen Infektionen im Jahr 2017 beinhalteten dateilose Methoden. Und als ob das nicht reicht, erlebten 2017 42 Prozent der Unternehmen mindestens eine dateilose Attacke, die erfolgreich ihre Daten stehlen und/oder ihre IT-Infrastruktur infizieren konnte.* Eines der bekanntesten Beispiele für dateilose Angriffe erfolgte 2017 auf das amerikanische Kreditunternehmen Equifax. Hierbei nutzten die Angreifer eine ungepatchte Schwachstelle, um schädliche Befehle auszuführen und so 146,6 Millionen persönliche Datensätze zu entwenden.

So helfen wir

Die **Verhaltenserkennung** von Kaspersky Lab überwacht Aktivitäten innerhalb eines Systems, um verdächtiges Programmverhalten zu finden. Hierbei ist es egal, ob sich hinter dem untersuchten Prozess eine Datei verbirgt – sämtliche schädliche Aktivitäten werden blockiert. Die Prinzipien der Verhaltenserkennung basieren auf dauerhaft ausgeführten Machine-Learning-Prozessen sowie den umfangreichen Bedrohungsinformationen, die das Kaspersky Security Network über Data-Science-Verarbeitung und Analyse globaler Echtzeitstatistiken gewinnt. Unser **Exploit-Schutz** blockiert Malware, die versucht, Software-Schwachstellen auszunutzen. Gleichzeitig kann **Adaptive Anomaly Control** Aktionen blockieren, die vom aufgezeichneten Muster abweichen (z. B. um den Start von PowerShell zu verhindern).

* The 2017 State of Endpoint Security Risk Report, Ponemon Institute.

CMD-/PowerShell-Bedrohungen: leistungsstark und opportunistisch

Shell-Skriptdateien hielt man früher für verhältnismäßig harmlos – auch wenn sie das nicht sind. PowerShell-Skripte unterscheiden sich hier jedoch deutlich: Sie sind äußerst leistungsstark, stellen eine vollständige Scripting-Umgebung dar und bieten Cyberkriminellen vielfältige Angriffsmöglichkeiten. So können sie zusätzliche Module aus dem Internet herunterladen, körperlose Malware starten oder remote beliebigen Code auf anderen Geräten im Netzwerk ausführen – und all das über ein eigentlich legitimes Programm, den PowerShell-Interpreter, der seit Windows 7 standardmäßig zu dem Betriebssystem zählt.

PowerShell-Angriffe nehmen exponentiell zu. Ein beachtlicher Teil der Malware verwendet hierbei auf die ein oder andere Weise CMD/PowerShell. Im April 2018 veröffentlichte Kaspersky Lab Informationen zur „Operation Parliament", einer Cyberspionage-Kampagne, die auf hochrangige legislative, exekutive und judikative Organisationen auf der ganzen Welt, vor allem aber im Nahen Osten und in Nordafrika abzielte. Die Angreifer hatten verschiedenste politische Einrichtungen zum Ziel: von Parlamenten und höchsten Behörden bis hin zu Militär, Nachrichtendiensten und Wahlkommissionen. Die Malware bietet Cyberkriminellen ein CMD-/PowerShell-Terminal, über das sie beliebige Skripte oder Befehle ausführen und die Antwort per HTTP-Anfrage senden können.

So helfen wir

Kaspersky Lab verfügt über die nötigen Technologien, um der Welle an PowerShell-Malware Herr zu werden. Die an unsere Engines übertragenen Strings werden sorgfältig mittels Verhaltenserkennung analysiert und ihre Ausführung wird blockiert, wenn etwas Verdächtiges gefunden wird. Dies ist zum Beispiel der Fall, wenn PowerShell von einem ungewöhnlichen Standort aus gestartet wird (z. B. Word oder der Ordner „Temp"), wenn die PowerShell-Befehlszeile seltsame Parameter enthält oder das Skript selbst verschlüsselt ist. Unsere Komponente „Adaptive Anomaly Control" erkennt anhand erlernter Muster ungewöhnliches Verhalten – auch bei PowerShell.

Ransomware: immer weniger, dafür aber immer raffinierter

Dieser Malware-Typ basiert auf Cryptors, also Trojanern, die Systeme über Schwachstellen, wie z. B. E-Mail-Anhänge oder Phishing-Links zu speziellen Malware-Webseiten, infizieren. Das Angriffsmodul verschlüsselt daraufhin im Hintergrund alle Daten, die für das Opfer von Wert sein könnten. Hierzu zählen Finanzinformationen, rechtliche Dokumente, Kundendatenbanken, Diagramme usw. Im Anschluss fordern die Cryptolocker ein Lösegeld, um die entsprechenden Dateien wieder zu entschlüsseln. In der Regel ist es nicht möglich, Dateien, die mit aktueller Cryptomalware verschlüsselt wurden, wieder zu entschlüsseln.

Ransomware hat 2017 stark zugenommen. In diesem Jahr fand mit WannaCry auch der bisher größte Ransomware-Angriff statt, der sich rasend schnell verbreitete und weltweit über 700 000 Opfer erreichte. Reckitt Benckiser, Anbieter von Verbrauchergütern, verlor bei einem Angriff mit der NotPetya-Ransomware in nur 45 Minuten den Zugriff auf 15 000 Laptops, 2000 Server und 500 Computersysteme. So verursachte die Attacke Schäden von ca. 130 Millionen US-Dollar.

Logistikanbieter Maersk meldete einen Umsatzverlust von ca. 300 Millionen US-Dollar aufgrund eines NotPetya-Angriffs. Zwar hat das Volumen von Ransomware 2018 abgenommen, die gesteigerte Raffinesse sorgt jedoch in Großunternehmen weiterhin für große finanzielle Schäden. Ransomware ist unter den Top 5 der teuersten Sicherheitsvorfälle für Unternehmen.

Unterschiedliche Ransomware-Varianten nutzen auch verschiedene Angriffstechnologien und Infektionsmethoden. Deshalb sind mehrstufige Lösungen unerlässlich, die spezielle Anti-Ransomware-Technologien zum Schutz Ihres gesamten Systems beinhalten.

So helfen wir

Kaspersky Endpoint Security for Business umfasst **Verhaltenserkennung** und eine **Remediation Engine**, die Malware blockiert und bereits verschlüsselte Dateien wiederherstellt. Und in Szenarien, in denen Verschlüsselungsprozesse über einen anderen Host im Netzwerk gestartet werden, blockiert unsere Anti-Cryptor-Engine entsprechende Aktivitäten und verweigert die Netzwerkverbindung zum schädlichen Host. Selbst für Unternehmen, die Lösungen anderer Anbieter verwenden, bietet das kostenlose Standalone-Tool **Kaspersky Anti-Ransomware** grundlegenden Ransomware-Schutz.

Cryptominer: angetrieben von der Gier

Kryptowährungen sind in den letzten Jahren zu einem wichtigen Thema geworden und zogen weltweit immer mehr Interessenten an. Die Chance, Geld mit Kryptowährungen zu verdienen, hat jedoch auch viele Cyberkriminelle angezogen. So werden im Zeitalter der Ransomware die meisten Lösegelder in Kryptowährungen gefordert, wie z. B. anonyme und nicht regulierte Bitcoins. Es war also nur eine Frage der Zeit, dass Miner in dieser Bedrohungsszene mitmischen.

Cryptominer, oder kurz „Miner", sind eine Art von Malware, die rasant zunimmt. Die anhaltende Entwicklung des Kryptowährungsmarktes hat zu einem rasanten Anstieg von Miner-Installationen geführt – und das ohne Wissen der Benutzer. Denn wenn eine neue Kryptowährung aufkommt, ist es deutlich leichter, sie zu minen und daraus einen Gewinn zu generieren, als bei etablierten Währungen.

Das Mining von Kryptowährungen ist an sich vollkommen legal – zum Problem wird es erst, wenn Kriminelle arglose Benutzer ohne ihr Wissen zur Installation von Mining-Software bewegen oder die Installation über Software-Schwachstellen selbst durchführen. So erhalten die Cyberkriminellen Kryptowährungen, während ihre Opfer eine beträchtliche Verlangsamung ihrer Systeme erleben. Oder wie es im MIT Technology Review heißt: „Cyberkriminelle nutzen alte Tricks und neue Kryptowährungen, um gestohlene Rechenleistung in digitales Geld zu verwandeln."

Zwischen 2017 und 2018 stieg die Anzahl der Benutzer, die Opfer von Minern wurden, um nahezu 44,5 Prozent. Auch der Anteil erkannter Miner an den insgesamt entdeckten Bedrohungen stieg zwischen 2016 und 2017 um über fünf und zwischen 2017 und 2018 sogar um fast acht Prozent. Die Anzahl der Benutzer, die mit mobilen Minern zu tun hatten, steigt ebenfalls stetig, wenn auch nicht so rasant: So waren es hier zwischen 2016 und 2018 „nur" 9,5 Prozent. Kaspersky Lab hat eine Zunahme der versuchten Miner-Installation auf Unternehmensservern festgestellt. Wenn diese Versuche erfolgreich sind, können die Geschwindigkeiten bei der Datenverarbeitung drastisch abfallen und Geschäftsprozesse plötzlich unterbrochen werden.

So helfen wir

Die **Verhaltenserkennung** von Kaspersky Lab erkennt getarnte Bedrohungen, die normale Virenschutztechnologien nicht finden. Sie identifiziert alle Programme (schädlich wie auch legitim), die versuchen, mit einer Mining-Adresse zu kommunizieren. Auch Versuche, Befehlszeilen-Parameter (einschließlich Wallet-Nummern, Pooladressen usw.) auszuführen, Aktionen von ungewöhnlichen Standorten aus zu starten (z. B. aus dem Ordner „Temp") oder eine Verbindung zu Mining-Pooladressen herzustellen, werden blockiert. Unsere Komponente **Adaptive Anomaly Control** erkennt anhand erlernter Muster versteckte Versuche, Prozesse und Programme zu starten.

Es gibt zahlreiche Berichte zu Mitarbeitern, die die Ressourcen ihres Unternehmens – also Computer, Server und sogar ganze Rechenzentren – ausnutzen, um nach Geschäftsschluss Kryptowährungen zu minen. Die **Webkontrolle** kann die Kommunikation mit Mining-Pooladressen identifizieren und blockieren und so verhindern, dass Miner Ihr System belasten.

Mobile Bedrohungen: das endlose Fressen

Die umfassende Nutzung mobiler Plattformen ist für Cyberkriminelle nach wie vor ein wahrer Segen. 2018 blieb die Bedrohungslage bei Mobilgeräten jedoch verhältnismäßig stabil. Im dritten Quartal erkannte Kaspersky Lab über 1,3 Millionen schädlicher Installationspakete für mobile Geräte. Unsere Statistiken zeigen, dass die Anzahl finanzieller Bedrohungen für Mobilgeräte mit jedem Quartal ansteigt. Und schon eine einzige Malware-Infektion auf einem Unternehmensgerät kann Schäden von 713 000 US-Dollar – bzw. 664 000 USD bei BYOD-Geräten – anrichten.

Die vielleicht wichtigste Entwicklung ist jedoch die Veröffentlichung des Banking-Trojaners „Asacub". Asacub wurde 2015 zum ersten Mal entdeckt und hat sich seither zur führenden Bedrohung im Bereich Banking-Trojaner entwickelt. Ihre Skalierung und Performance ließ selbst die leistungsstärksten Mobile-Kampagnen hinter sich.

So helfen wir

Kaspersky Security for Mobile ist eine MTD- (Mobile Threat Defense) und MTM-Lösung (Mobile Threat Management), mit der Unternehmen sicherstellen können, dass mobile Mitarbeiter ihre Mobilgeräte für Arbeitsaufgaben nutzen, ohne zum Unternehmensrisiko zu werden. Die Kombination aus leistungsstarkem **Malware-Schutz**, Cloud-basierten Bedrohungsinformationen und maschinellem Lernen bietet Schutz vor bekannten, unbekannten und fortschrittlichen Bedrohungen für Daten auf Mobilgeräten sowie aus Online-Aktivitäten. **Webkontrolle** und **Phishing-Schutz** gewährleisten zuverlässige und sichere Webfilter, um den Zugriff auf schädliche und andere unerwünschte Webseiten zu blockieren.

Geldautomat-/PoS-Bedrohungen: kein Rückgang in Sicht

Durch die Kombination verschiedener Faktoren, darunter der Einsatz veralteter und nicht mehr unterstützter Betriebssysteme sowie die Verfügbarkeit intuitiver Entwicklungsplattformen, kann fast jeder schädlichen Code erstellen.

Geldautomaten und Points of Sale (PoS) sind weiterhin ein beliebtes Ziel für Cyberkriminelle. Geldautomaten werden bereits seit 2008 angegriffen. Mit „Backdoor.Win32.Skimer" wurde damals das erste schädliche Programm entdeckt, das auf Geldautomaten abzielte. 2017 trat dann der erste Fall von Malware-as-a-Service speziell für Geldautomaten auf: Cyberkriminelle fügten alle nötigen Schadprogramme mit Videoanweisungen zu einem Paket zusammen und boten dieses Paket jedem Interessenten an, der selbst Geldautomaten hacken wollte. Im selben Jahr entdeckten Kaspersky-Forscher bis dato unerkannte Angriffe auf Geldautomaten, bei denen neue Malware sowie Remote- und dateilose Vorgänge zum Einsatz kamen.

In den ersten sieben Monaten 2018 war die Anzahl der Malware-Infektionen bei Geldautomaten/PoS-Systemen bereits um 57 Prozent höher als im gesamten Jahr 2017. Experten gehen davon aus, dass Angriffe über Software, die speziell auf Finanzunternehmen zugeschnitten ist, darunter auch Software für Geldautomaten und PoS-Terminals, weiterhin zunehmen werden. PoS-Attacken zählen zu den drei beliebtesten Angriffsmustern.

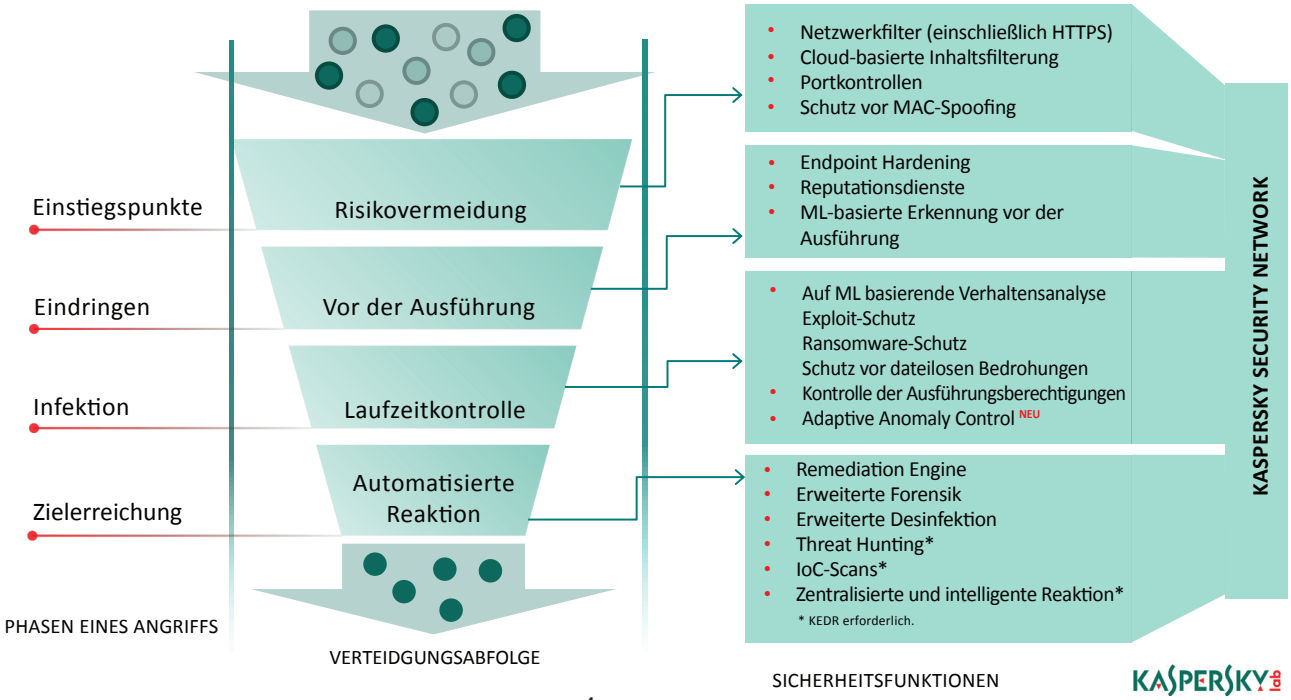
So helfen wir

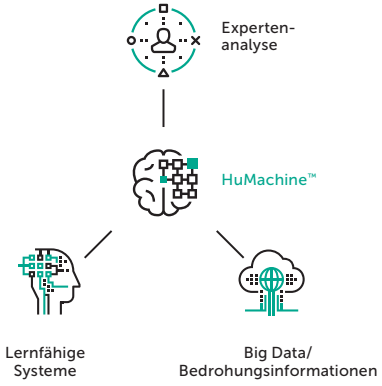
Kaspersky Embedded Systems Security wurde speziell für Unternehmen mit Geldautomaten und PoS-Systemen entwickelt, um in diesem speziellen Bereich die Sicherheit zu gewährleisten. Mit **Malware-Schutz**, **Programm-** und **Gerätekontrollen** sowie **Arbeitsspeicherschutz** und **Firewall-Verwaltung** schützt die Lösung die individuellen Schwachstellen entsprechender Architekturen, berücksichtigt hierbei die einzigartigen Funktionen sowie die Betriebssystem-, Channel- und Hardware-Anforderungen und unterstützt auch weiterhin Windows XP. All diese Komponenten sorgen gemeinsam mit der **Überwachung der Dateiintegrität** und der **Protokolluntersuchung** dafür, dass Kaspersky Embedded Systems Security alle relevanten PCI-DSS-Anforderungen optimal einhält.

Fortschrittliche Bedrohungen erfordern umfassenden Schutz

Je weiter sich die moderne Bedrohungslandschaft entwickelt, desto seltener reichen klassische Schutzlösungen aus – auch wenn entsprechende Technologien unverzichtbar sind. Um den Schutz zu steigern und so auch die hier erwähnten fortschrittlichen Bedrohungen abzuwehren, müssen Unternehmen ihre Sicherheit auf die nächste Stufe anheben. Hierzu benötigen sie Next Generation-Lösungen, die mehrere Technologie-Ebenen mit maschinellem Lernen, Bedrohungsinformationen und Expertenanalysen kombinieren, um heute und in Zukunft relevanten und effektiven Schutz zu gewährleisten.

Kaspersky Lab: Umfassende Schutztechnologien wehren bekannte, unbekannte und hochentwickelte Bedrohungen ab





Kaspersky Lab
Finden Sie einen Partner in Ihrer Nähe: **www.kaspersky.de/partners**
Kaspersky for Business: **www.kaspersky.de/business-security**
True Cybersecurity: **www.kaspersky.de/true-cybersecurity**
IT Security News: **www.kaspersky.de/blog/b2b/**

#truecybersecurity
#HuMachine

www.kaspersky.de