# IT Security ist kein Ponyhof

100 von 100 Administratoren antworten auf die Frage nach der verwendeten Methodik für die Absicherung der Endgeräte (Endpoint Protection) mit "Virenscanner".

100 von 100 Administratoren, deren Netzwerke in den letzten 2 Jahren erfolgreich angegriffen wurden, setzten aktuelle Virenscanner ein. 100 von 100 Virenscanner haben versprochen, Weiterentwicklungen und Innovationen implementiert zu haben, die vor neuen Angriffen schützen.

2016 wurden hunderttausende mit Antiviren Produkten vermeintliche geschützte Rechner mit Schadsoftware wie Ransomware befallen. Antivirenhersteller hatten daraufhin versprochen, aus den Fehlern gelernt zu haben und ihre Produkte um Funktionen erweitert zu haben, die auch vor den aktuellsten Bedrohungen schützen sollten. Auf der ceBIT 2017 hielten noch im März 2017 Antivirenhersteller Talks und Präsentationen, um die neue "Anti Ransomware" Erweiterung ihrer Virenscanner Produkte zu erklären und zu vermarkten.

Keine 8 Wochen später, zwischen dem 12.05.2017 und dem 16.05.2017, hat die Ransomware WannaCry innerhalb 4 Tagen über 300.000 Rechner in über 150 Ländern befallen. Praktisch alle diese Rechner waren mit Antivirus Produkten gesichert. Ein Hersteller eines Virenscanners warb bis dahin auf seiner Webseite mit dem Slogan "The NHS is totally protected with [Hersteller]". Dann befiel WannaCry tausende Rechner des Britischen NHS, und der Hersteller änderte seine Werbebotschaft in "[Hersteller] understands the security needs of the NHS".

Nicht zum ersten mal hat die Produktkategorie Antivirus unabhängig vom Hersteller den Nachweis erbracht, nicht als Schutzmechanismus für aktuelle Angriffe geeignet zu sein. Würden Antiviren Produkte tatsächlich das halten, was sie versprechen, dürfte es eigentlich keine Infektionen mit Schadsoftware mehr geben. Denn heute wird so gut wie kein Computer ohne ein Antivirus Produkt in Betrieb genommen. Dies zeigt das Dilemma, in dem Administratoren stecken: Das Netzwerk muss geschützt werden, und Antivirus kann das offensichtlich nicht verlässlich leisten.

Nach einem erfolgreichen Angriff durch eine Schadsoftware ist eine oft zu beobachtende Reaktion der Wechsel von Antivirus Produkt A auf Antivirus Produkt B. Während zeitgleich woanders ein Administrator aus den gleichen Gründen von Antivirus Produkt B auf Antivirus Produkt A wechselt.

Bleibt dem Administrator eine Wahl? Schließlich gilt beinahe ausnahmslos die Binsenweisheit, dass jeder Rechner auf jeden Fall durch einen Virenscanner geschützt sein muss. Wer gegen diese Doktrin verstößt, setzt sich der Gefahr aus, fahrlässig gehandelt zu haben.

Sicherheitsexperten warnen seit Jahren, dass Antivirus Produkte heute keinen ausreichenden Schutz mehr bieten, sogar teilweise die Sicherheit eines Netzwerks kompromittieren. Aber was tun? Welche Möglichkeiten bleiben einem Administrator, sein Netzwerk zu sichern? Die Einschätzung von Fachleuten und Durchschnittsnutzern gehen hier weit auseinander. Laut einer Studie von Google hielten die meisten Laien Antivirenprogramme für die wichtigste Maßnahme, um sich vor Gefahren zu schützen. Doch nicht einmal jeder zehnte Sicherheitsexperte hält Antivirus in diesem Zusammenhang für relevant.

**Doch warum halten sich die Administratoren nicht an die Empfehlungen der Fachleute? Ignorieren sie die Fakten?**

**"Niemand wurde je gefeuert, weil er sich für IBM entschied"**

Im Englischen Sprachraum gibt es die Phrase "Nobody ever got fired for choosing IBM". Sie weist darauf hin, dass die Wahl auf eine etablierte Option nicht wegen einer intrinsischen Qualität fällt, sondern weil es die etablierte Option ist. Anders ausgedrückt: Das haben wir schon immer so gemacht, das machen alle so!

## Wie findet man eine gute Sicherheitslösung?

Der einzige Sinn einer Sicherheitslösung ist, das System gegen Bedrohungen zu schützen. An der Stelle, wo dies scheitert, sind alle anderen Kriterien eines Produktes bedeutungslos. Denn was nützt ein kostenloser Virenscanner, wenn dessen Erkennungsleistung sich auf Schadsoftware von vor 6 Wochen beschränkt?

Kein Produkt bietet 100% Sicherheit. Ein sinnvolles Kriterium sollte kann sein, wie weit man sich dieser unerreichbaren 100% Sicherheit nähern kann. Dass Virenscanner in dieser Frage keine nennenswerten Fortschritte machen, haben sie in den letzten 20 Jahren ausreichend unter Beweis gestellt.

## Schutzniveau von Application Whitelisting

Das exakte Gegenteil der Arbeitsweise eines Virenscanners ist ein Schlüssel zu einem unvergleichlich viel höheren Schutzniveau. Der Virenscanner erlaubt alles und verbietet als Ausnahme davon die Software, die er als unerwünscht definiert bekommt. Software, die dem Virenscanner nicht bekannt ist, wird erlaubt. Dies ist der Grund, warum Virenscanner nicht vor aktueller Schadsoftware schützen können.

Die Application Whitelisting Lösung macht das genaue Gegenteil: "Whitelisting" bedeutet, dass nur erlaubt ist, was auf

der "weißen Liste" steht. Anders formuliert: Die Application Whitelisting Lösung muss lediglich wissen, welche Software im Unternehmensnetzwerk ausgeführt werden darf. Denn auch Schadsoftware ist letztendlich nur Software. Diese wird demnach bereits in der Grundkonfiguration an der Ausführung gehindert, ohne dass diese vorher in irgendeiner Form bekannt sein muss. Einfach aus dem Grund, weil die Schadsoftware nicht bekannt ist. Doch aus diesem Ansatz ergeben sich ganz automatisch Fragen. Bedeutet Application Whitelisting nicht einen erhöhten Aufwand? Wie löst man die sich direkt aufdrängenden Aufgabenstellungen wie die Erstellung der Whitelist mit all ihren vielleicht tausenden Einträgen? Wie werden Änderungen wie Updates und neue Software erfasst? Was ist mit dynamischen Anpassungen im Betrieb? Wie lange dauert es, bis eine Änderung einer Policy aktiv wird? Nachrangig ergeben sich je nach eingesetztem Produkt Detailfragen in Bezug auf das Verhalten auf mobilen Systemen, Reporting, Ausnahmen, individuelle Policies. Welches Schutzniveau wird tatsächlich erreicht? Wie ist die Performance?

Anders als bei Virenscannern, die unabhängig vom Hersteller im Wesentlichen alle das selbe technische Verfahren einsetzen, gehen die Hersteller von Application Whitelisting Lösungen durchaus stark unterschiedliche Wege der technischen Umsetzung. Hersteller wie Ivanti und Microsoft (AppLocker) setzen auf Windows-internen APIs auf, um auf Dateisystem-Ebene Attribute zu prüfen. Der Deutsche Hersteller SecuLution verwendet ein eigenes Ring-Zero Kernel Modul, das die Zuweisung von RAM Speicher für nicht erlaubten Code unterbindet.

## Restrisiko - Verspricht Application Whitelisting 100% Sicherheit?

Application Whitelisting Produkte, die auf Windows internen Berechtigungen basieren, sind sie dem Risiko ausgesetzt, dass Code mit Administrator- oder Systemrechten zur Ausführung kommen und damit die Sicherheit der Application Whitelisting Lösung unterwandern kann. Prominentes Beispiel ist die kürzlich aufgedeckte "Eternalblue" genannte Sicherheitslücke, die auch von der Ransomware "WannaCry" genutzt wurde. "Eternalblue" nutzt einen Fehler im SMB Dienst von Windows. Bei einem Angriff über diese Sicherheitslücke kann ein Angreifer Code mit SYSTEM-Rechten ausführen. Application Whitelisting Lösungen, die sich auf das Windows interne Berechtigungsmodell stützt, kann damit an dieser Stelle prinzipiell keinen Schutz bieten. So wurden auch mit AppLocker geschützte Netzwerke von WannaCry erfolgreich angegriffen. In solchen Szenarien bietet der Ansatz, die Zuweisung von RAM Speicher zu kontrollieren, anstatt auf Windows Berechtigungsebene aufzusetzen, einen nicht sofort offensichtlichen Vorteil mit sich: Auf diese Weise kann auch Code blockiert werden, der unter den Berechtigungen des Administrator- oder Systembenutzers ausgeführt werden soll. Ein Schutzmechanismus entsteht, der vollständig abgekoppelt von Windows internen Berechtigungen ist. Damit sind auch schlecht gepatchte Systeme bereits im Default zum Beispiel gegen WannaCry geschützt.

## Usability und Wartbarkeit

Die Frage des Aufwands für Implementation und Betrieb ist in der Regel entscheidend über den Erfolg einer Application Whitelisting Implementation. Application Whitelisting Lösungen, die auf Basis von Dateisystem Attributen arbeiten, benötigen keine zentrale Datenbank, da das Dateisystem selbst schon die Policies darstellt. Eine der empfohlenen Vorgehensweisen für eine Umsetzung besteht darin, Musterrechner (Golden Images) zu erstellen und diese für Produktivsysteme zu klonen. Im Ergebnis hat der Administrator ein maximal homogenes Netzwerk, was sich sehr positiv auf den Pflegeaufwand im Betrieb auswirken kann. Dieser Ansatz bringt jedoch auch den Nachteil mit sich, dass kurzfristige, dynamische Änderungen von Policies im laufenden Betrieb sehr aufwändig bis unmöglich sind und für jede individuelle Softwareausstattung ein eigenes Golden Image gepflegt werden muss. Darüber hinaus muss der Administrator die gesamte IT Infrastruktur und den Softwarestand auf das Application Whitelisting anpassen. Auch Updates erfordern immer wieder die Erstellung eines jeweils neuen Golden Image.

## Lösungen mit zentraler Policy Datenbank

SecuLutions Application Whitelisting stellt die Whitelist über eine virtuelle Server Appliance im Netzwerk bereit. Agents auf den Endpoints errechnen bei dem Start einer Software den Hash der Anwendung, die gestartet werden soll und fragen dessen Berechtigung in Echtzeit bei der Whitelist an. Durch Lernmodi und Automatisierungen werden die Hashes auf der zentralen Datenbank im Netzwerk automatisch erfasst, klassifiziert und verwaltet, ohne dass der Administrator seine Infrastruktur auf Application Whitelisting anpassen muss. So verspricht der Hersteller SecuLution eine Integration seiner Lösung in ein heterogenes Netzwerk mit z.B. 10.000 Endpoints in insgesamt nur 3 Tagen Arbeit. Der Hersteller verspricht im laufenden Betrieb keinen Mehraufwand in der Administration zu erzeugen.

## Whitelisting von Software ist keine neue Idee

Das deutsche Unternehmen SecuLution konzentriert sich seit 2001 ausschließlich auf die Entwicklung und den Vertrieb der gleichnamigen Application Whitelisting Lösung, die inzwischen in der Version 18 zur Verfügung steht und in mehr als 50 Häusern aus dem Gesundheitswesen in Deutschland zum Einsatz kommt. Die Liste von Anbietern ließe sich problemlos erweitern, allen gemeinsam wäre, dass das angebotene Prinzip des Application Whitelisting eher ein Schattendasein unter den Security Lösungen fristet und das trotz der eindeutig effektiveren Wirkung.

**Ein Vergleich aus dem Alltag: Die LED ist nicht aus der Weiterentwicklung des Streichholzes entstanden.**