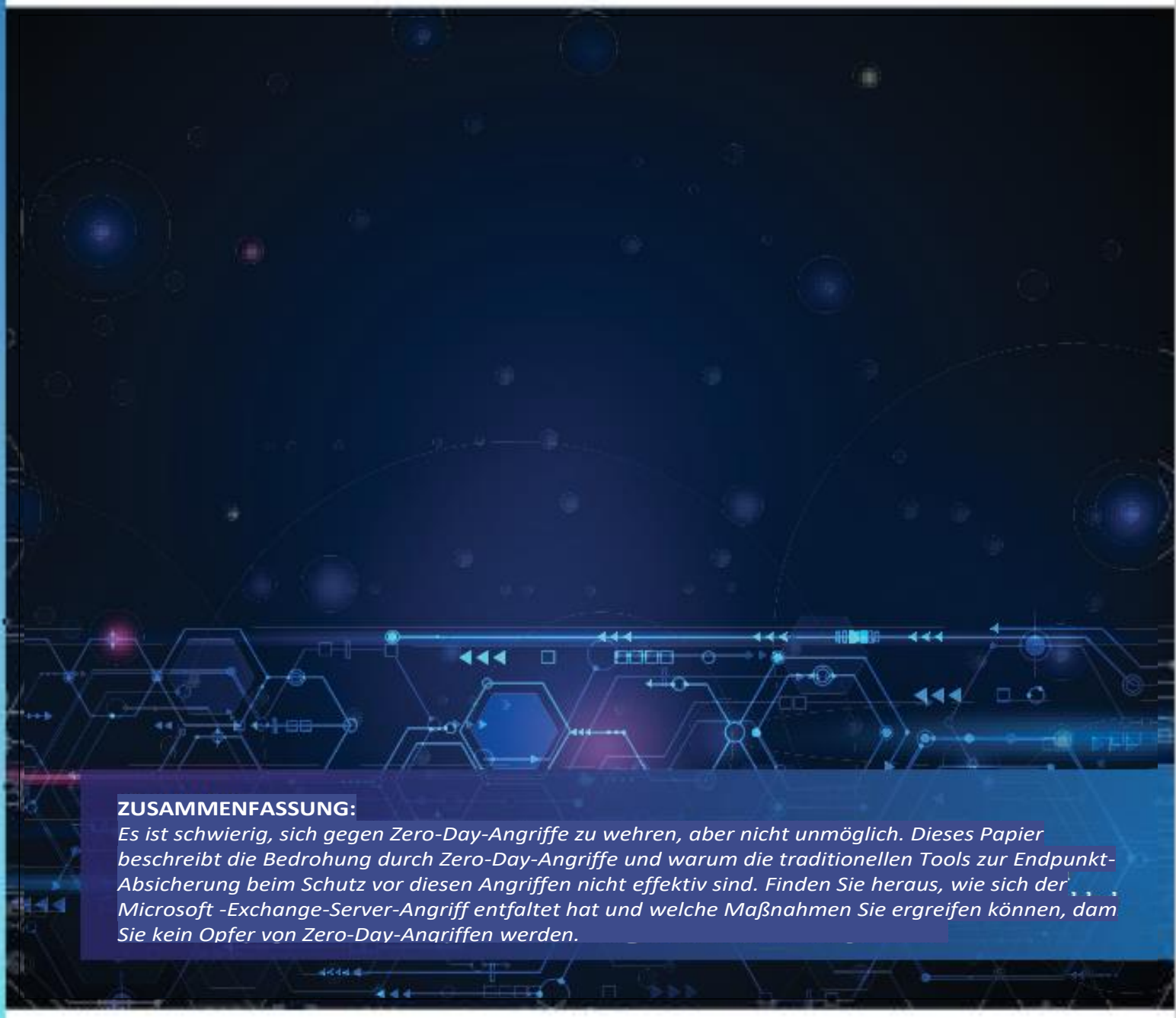
APPGUARD

Die Malware-Defensive

Zero-Day-Attacken mit der richtigen Abwehr verhindern:

Bereiten Sie sich auf den nächsten MS-Exchange-Angriff vor

WHITEPAPER



ZUSAMMENFASSUNG:

Es ist schwierig, sich gegen Zero-Day-Angriffe zu wehren, aber nicht unmöglich. Dieses Papier beschreibt die Bedrohung durch Zero-Day-Angriffe und warum die traditionellen Tools zur Endpunkt-Absicherung beim Schutz vor diesen Angriffen nicht effektiv sind. Finden Sie heraus, wie sich der Microsoft -Exchange-Server-Angriff entfaltet hat und welche Maßnahmen Sie ergreifen können, dam Sie kein Opfer von Zero-Day-Angriffen werden.

Die Bedrohung durch Zero-Day-Angriffe

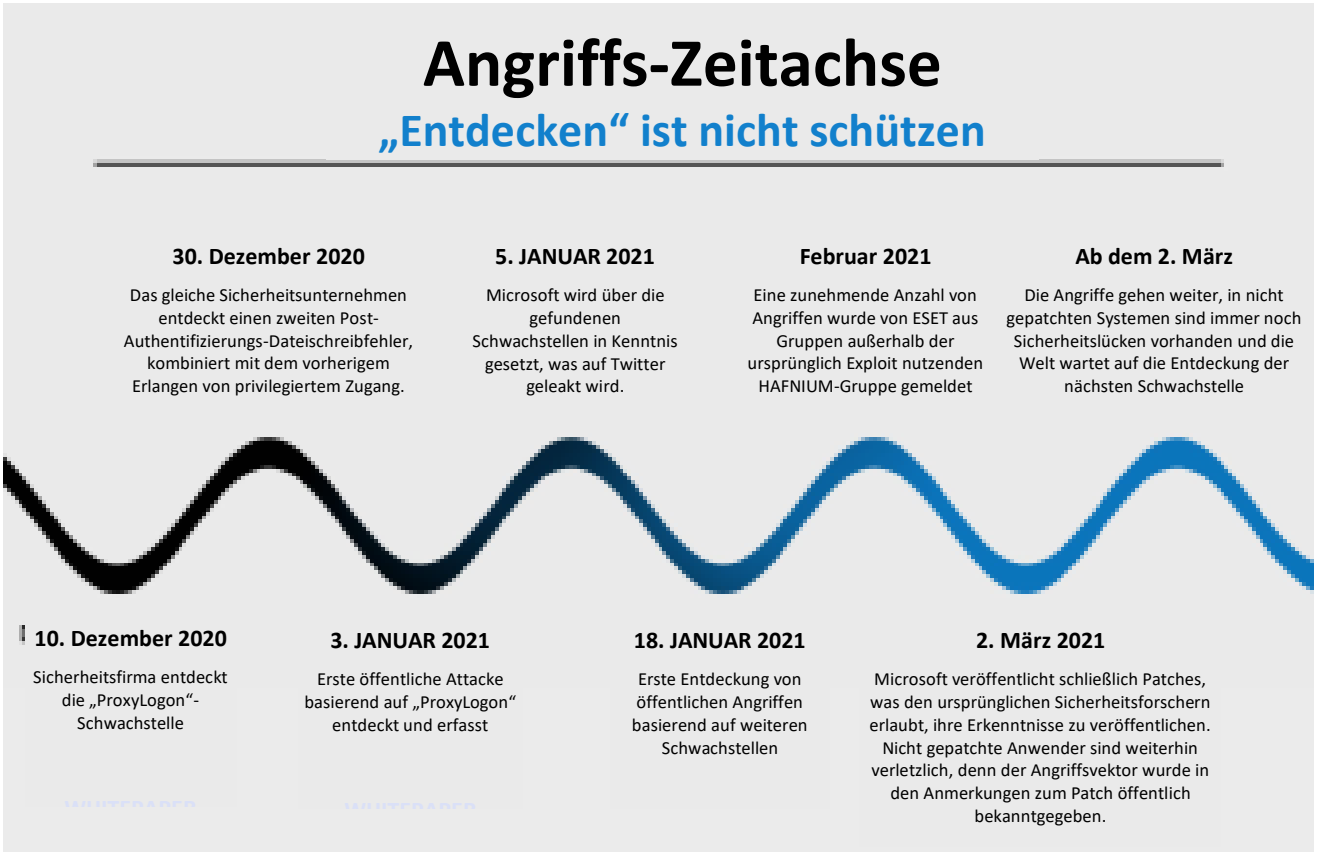
Zero-Day-Angriffe sind nichts Neues. Schon seit einiger Zeit wissen Hacker, dass Software-Programme verletzlich sind und dass unbeabsichtigte Schwachstellen in der Software ausgenutzt werden können, um Malware zu verbergen, mit der auf ansonsten sichere Daten zugegriffen werden kann. Böswilliger Code kann über Tage, Monate oder Jahre unbemerkt in einer Umgebung verweilen und sensible Daten sammeln, ohne entdeckt zu werden. Zero-Day Schwachstellen gehören zu den am meisten verbreiteten Angriffen, aber auch zu jenen, die am schwierigsten abzuwehren sind.

Software-Programmierer halten stets Ausschau nach Sicherheitslücken in ihrer Software und wenn eine Schwäche erkannt wird, geben sie Patches heraus, um die Sicherheitslücke zu schließen. Jedoch verkündet der Programmierer durch das Versenden des Patches der ganzen Welt, wo Schwachstellen zu finden sind. Häufig erkennen Hacker das als Möglichkeit, Schaden anzurichten, bevor die Anwender Zeit haben, den Patch zu implementieren. Hacker versuchen auch, proaktiv Sicherheitslücken in Programmen zu finden – sie entdecken sie häufig früher, als die Software-Programmierer. Im Grunde haben Software-Entwickler und Anwender nicht einen Tag Zeit („Zero Days“), um eine Schwachstelle zu beseitigen, bevor sie zu einer Gelegenheit zum Missbrauch durch Hacker wird.

Der jüngste Microsoft-Exchange-Server-Angriff erinnert erneut daran, wie verletzlich Software ist. Wie viele andere Zero-Day-Attacken war die Microsoft-Exchange- Server-Attacke, die einem chinesischen Betreiber namens HAFNIUM zugeschrieben wird, ein Multi-Vektor-Angriff. Während der Angriff Anfang Januar 2021 erkannt und gemeldet wurde, konnte Microsoft erst am 2. März einen Patch veröffentlichen und gab dem Angreifer so Monate Zeit, um Schwachstellen auszunutzen und wahllos Server zu infizieren. Zum Zeitpunkt der Veröffentlichung des Patches waren bereits viele Systeme kompromittiert. Tatsächlich wird geschätzt, das zehntausende Einheiten weltweit infiziert wurden.

Die Microsoft-Exchange-Server-Attacke verstehen

Die Microsoft-Exchange-Server-Attacke war ein mehrgliedriger Angriff, der verschiedene Angriffsvektoren verwendete. Zuerst verschaffte er sich Zugang zu einem Exchange Server, indem er gestohlene Passwörter verwendete oder zuvor unerkannte Sicherheitslücken nutzte, um einen Anwender mit Zugangsrechten zu imitieren. Der Angreifer erstellte dann eine Web-Shell, um die Kontrolle über den kompromittierten Server zu übernehmen. Durch den Zugang zum Server war der Hacker in der Lage, Daten aus dem Netzwerk der Organisation zu stehlen. Im Wesentlichen zielte der Angreifer auf die Unified-Messaging-Funktion des Codes von Microsoft Exchange ab, um aus der Ferne Code zu starten, der Web-Shells installiert, die dauerhaften Zugang zum System ermöglichen. Durch das Installieren von Web-Shells erhielten die Hacker Administratorenrechte, was mehrere Wege zur Kompromittierung eröffnete, darunter das Abgreifen von Zugangsdaten und seitliche Bewegung in andere Systeme. Diese mehrgliedrigen Angriffe werden häufig als Malware-Cocktails bezeichnet.



„AppGuard setzt die normalen Verhaltensweisen des Host-Systems durch und verwendet dazu eine Kombination aus Kontrollmechanismen, die Barrieren errichten und den Pfad der Malware in verschiedenen Phasen ihrer potentiellen Attacke unterbrechen. Die Abwehr erfolgt, ohne dass die Malware oder ihre Auswirkungen erkannt werden müssen.“

Warum traditionelle Tools nicht vor Zero-Day-Exploits schützen können

Die Auswirkungen des Microsoft-Exchange-Server-Angriffs haben auf jeden Fall bewiesen, dass herkömmliche Maßnahmen bei Zero-Day-Attacken wirkungslos sind. Der Angriff verwendete eine Code-Ausführung aus der Ferne, die keinerlei Authentifizierung erforderte und es den Angreifern erlaubte, in Software einzudringen, ohne von den herkömmlichen Sicherheitsvorrichtungen erkannt zu werden. Dazu gehören Anti-Virus, Endpoint Protection Platforms (EPP) sowie Endpoint-Detection- und Response-Lösungen (EDR). Angesichts der Tatsache, dass herkömmliche Anti-Virus- und Anti-Virus-Tools der nächsten Generation Einbrüche feststellen, indem sie bekannten böswilligen Code erkennen oder Code, der sich nicht auf ihrer Liste vertrauenswürdiger Codes befindet, ist böswilliger Code, der in diese Software eingebettet ist, unmöglich zu erkennen.

Das trifft auch für Endpoint-Detection- und Response-Systeme (EDR) sowie Endpoint-Protection-Platform-Lösungen zu (EPP), denn diese Tools konzentrieren sich auf das Erkennen von Angriffen auf Endpunkte, basierend auf dem Extrapolieren von vorherigem Bedrohungsverhalten, um aktuelle oder zukünftige Bedrohungen vorherzusagen.
Diese Methode erfasst einige der Bedrohungen, ihr entgehen jedoch andere, wenn deren Art ausreichend einzigartig ist. Darüber hinaus erscheint eine Bedrohung, selbst wenn ein EDR-System diese erkennt, in einem Protokollsystem, das in einer Unmenge falscher positiver Alarmmeldungen begraben ist. Das erfordert einen großen Aufwand für die forensische Analyse, um zu erkennen, welche Alarme Maßnahmen erfordern und welche nicht. Die verzögerte Reaktionszeit kann entscheiden, ob eine Kompromittierung erfolgt oder nicht, je nachdem, wie schnell der Angreifer zuschlägt.

Abwehr von Zero-Day-Attacken mit AppGuard

AppGuard ist anders. Statt zu versuchen, den Missbrauch von Anwendungen zu stoppen, werden gekaperte Anwendungen unschädlich gemacht und die Malware kann so ihr gewünschtes Ziel nicht erreichen. Das geschieht, indem Echtzeit-Sicherheitsprotokolle durchgesetzt werden, die sich nicht auf das Erkennen des Verhaltens von Malware verlassen, Gut und Böse unterscheiden oder Alarme generieren, die menschliches Eingreifen erfordern. Stattdessen erzwingt AppGuard die normalen Verhaltensweisen des Host-Systems und verwendet dazu eine Kombination aus Kontrollmechanismen, die Barrieren errichten und den Pfad der Malware in verschiedenen Phasen ihrer potentiellen Attacke unterbrechen. Die Verteidigung erfolgt, ohne dass die Malware oder ihre Auswirkungen erkannt werden müssen. Aus diesem Ansatz folgt, dass die Effektivität von AppGuard bei Malware, die neue Muster verwendet, genauso stark ist und der Entwicklung nicht immer hinterherhinkt. Daher ist AppGuard in einzigartiger Weise geeignet, Zero-Day- und ausgereifte vielgestaltige Angriffe abzuwehren.

Die Zero-Trust-Endpunkt-Absicherung von AppGuard verwendet patentierte Startrestriktions-, Eingrenzungs- und Isolationstechniken, um das Verhalten von Anwendungen und Dienstprogrammen dynamisch zu kontrollieren. Statt zu versuchen, mit der konstanten Entwicklung von Malware Schritt zu halten, greift AppGuard ein, indem es die begrenzte Anzahl hochriskanter Aktionen einschränkt, die Malware zum Erledigen ihrer Aufgabe benötigt. Das sind zum Beispiel Registry-Modifikationen, Lese-/Schreibzugriff auf Speicher und unbefugter Zugang zu Informationen. Durch die Anwendung dieser Kontrollen, die adaptiv auf Kontext basieren, bietet AppGuard maximale Sicherheit, während die normalen Vorgänge ungehindert zugelassen sind, so dass die Arbeit erledigt werden kann.

Diese Abwehr auf mehreren Ebenen unterbricht die ersten Phasen von häufig nicht erkennbaren Cyber-Angriffen, darunter Zero-Day-Malware, Phishing, als Waffe missbrauchte Dokumente, „Malvertising“, Watering-Hole-Taktik, dateilose Malware, Drive-by-Downloads, Ransomware, Memory-Scraper und andere eskalierende Angriffe, die konventionelle Sicherheitsansätze nicht stoppen können und werden. Jedoch liegt die Stärke von AppGuard darin, dass es seine Kontrollen über jene böswilligen Aktivitäten anwendet, die in den frühen und späten Phasen der Angriffe notwendig sind, so dass es mehrere Gelegenheiten gibt, den Erfolg von Angriffen zu verhindern.

Der patentierte Ansatz von AppGuard vereint auf einzigartige Weise einfache und leicht zu steuernde Regelkontrollen, die nicht akzeptable, jedoch deterministische Aktionen dynamisch blockieren. Während Widersacher das Aussehen und Verhalten von böswilligem Code einfach ändern können, werden die erforderlichen Aktionen nur sehr selten geändert. Angreifer von Endpunkten können ihre Ziele nicht erreichen, ohne eine bestimmte begrenzte Anzahl von Aktionen durchzuführen. AppGuard unterbricht diese.

Wie AppGuard die Microsoft-Exchange-Server-Attacke vereitelt hat: Ein Beispiel aus dem echten Leben

Die adaptiven Regelkontrollen von AppGuard schützten die Kunden von AppGuard und neutralisierten die Microsoft-Exchange-Server-Attacke, indem sie Barrieren für die Aktion errichteten, die der Exchange-Server nach der Kaperung auszuführen versuchte. Technisch passt sich AppGuard automatisch an Änderungen der Anwendung sowie an unterwartete Angriffsvarianten an. Im Falle der Exchange-Server-Attacke wäre ein Kunde mit AppGuard - egal, ob es gerade eben oder vor fünf Jahren installiert wurde - durch die Standardregeln von AppGuard vor diesem Angriff geschützt gewesen. Wie bereits vorher angemerkt, handelte es sich bei der Microsoft-Exchange-Server-Attacke um einen mehrgliedrigen „Malware-Cocktail“ und verschiedene kombinierte Komponenten der Kontrollen von AppGuard verhinderten ihren Erfolg.

Eingrenzungsregel über den Exchange Server

Die Eingrenzungsregel von AppGuard verhindert, dass eingegrenzte Anwendungen und Dienstprogramme Änderungen vornehmen oder auf Speicher von Systemressourcen lesen/schreiben können, wobei für besondere Bedürfnisse Ausnahmen möglich sind. Hier die Standard-Konfiguration von AppGuard:

- Blockierte die versuchte Exploit-Schreiboperation in
  - “C:\inetpub\wwwroot\”
  - %PROGRAMFILES%
- Blockierte das Lesen des Local Security Authority Subsystem Service (“LSASS” - ein wesentlicher Windows-Sicherheitsprozess) bei dem Versuch, Zugangsdaten zu stehlen.
  - Wenn dies aufgrund einer Konfigurationsausnahme durch den Administrator nicht geschehen wäre, würde der Angriff in einem späteren Stadium des Angriffs
  - blockiert, wenn der Zwischenspeicher für Zugangsdaten in folgendes Verzeichnis schreibt:
    - C:\windows\temp\
    - C:\root\

Isolationsregel über LSASS

Die Isolationsregel blockiert den Zugang zu Speicher und Steuerung von wertvollen Systemressourcen, wobei nur wenige spezifische Ausnahmen als betriebliche Notwendigkeiten erlaubt sind, die durch einen Administrator konfiguriert werden. Exchange benötigte solche Ausnahmen nicht, daher traf diese Regel nicht zu.

- Da es sich bei LSASS um eine wertvolle Ressource handelt, würde die Isolationsrichtlinie standardmäßig angewandt. Wenn daher eine Ausnahme von der Eingrenzungsregel angewandt ist d.h. um die vorherige Regel zu umgehen), würde die Isolation greifen und den Zugang sowie die Fähigkeit blockieren, Zugang zu Sicherheits-Anmeldedaten zu erlangen.

Zero-Trust-Bereich - Start-/Ladekontrollen

Diese Regel teilt das Host-System in wertvolle und nicht vertrauenswürdige Bereiche auf (d.h. Bereiche mit (a) wenigen, wenn nicht keinen Restriktionen für die Art von Dateien oder deren Änderungen und (b) mit viel Zugang zur Außenwelt wie Benutzerprofil, Desktop, Downloads etc.). Scripte und Dienstprogramme, die aus nicht vertrauenswürdigen Bereichen gestartet werden, werden blockiert. Es stehen zusätzliche Start- und Ladekontrollen zur Verfügung, um die Angriffsfläche zu verkleinern und die Anwendung von bestimmten hochriskanten Dienstprogrammen zu verbieten, außer unter sehr speziellen Umständen, da diese Dienstprogramme häufig bei Living-off-the-Land-Angriffstechniken verwendet werden. Hier blockierte AppGuard

- den Versuch, Benutzerkonten hinzuzufügen, da das entsprechende Dienstprogramm eingegrenzt ist.

- Als der Exchange Server versuchte, böswillige ausführbare Dateien, Scripte oder DLLs in Verzeichnisse zu schreiben, in denen AppGuard normalerweise das Schreiben erlaubt (d.h. in diesem Bereich wird keine Isolationsregel angewandt), wurden diese dennoch von der Ausführung abgehalten, weil sie versuchten, aus einem nicht vertrauenswürdigen Bereich zu starten. Zum Beispiel wurde PowerCat über eine böswillige DLL geladen und von AppGuard blockiert, weil sie von einem nicht vertrauenswürdigen Ort agierte und einen wertvollen Standort anvisierte.

Nicht-standardmäßige Isolationsergänzungen

Einige Kunden verwenden zusätzliche Regeln und wenden AppGuard-Isolationsregeln an, um das Installieren von Snap-ins zu verhindern, indem im Wesentlichen ausgewählte Registry-Keys abgeriegelt werden, die nur von ausgewählten Konfigurationsanwendungen oder in Wartungsfenstern geändert werden dürfen. Die zusätzlichen Regeln hätten auch jene Aktivitäten blockiert, die bei dem Angriff verwendet wurden, um sich einzunisten und Informationen zu stehlen.

„Aus diesem Ansatz folgt, dass die Sicherheitseffektivität von AppGuard bei Malware, die neue Muster verwendet oder brandneue Schwachstellen ausnutzt, genauso stark ist und nicht ständig hinterherhinkt. Daher ist AppGuard in einzigartiger Weise geeignet, Zero-Day-und ausgereifte vielgestaltige Angriffe abzuwehren.“

AppGuard sollte in einem Umfeld mit zunehmend gefährlichen Cyber- und menschlichen Bedrohungen die erste und hauptsächliche Verteidigungslinie sein.

Mark Kelton

Ehemaliger stellvertretender Direktor für Spionageabwehr, CIA

Diese Beispiele verdeutlichen die Vorteile der wahren präventiven Techniken von AppGuard, die Redundanzen und Barrieren auf die gefährlichen Aktivitäten anwenden, die Malware versucht, im Verlauf eines Angriffs auszuführen.

Durch das Ergreifen eines agnostischen Ansatzes für das „Wie“ und einen Schwerpunkt auf das „Was“ schließt AppGuard die inhärenten Löcher in jeder Konfiguration einer Anwendung, die Angreifer stets für Ihre Zwecke zu nutzen versuchen. Ein weiterer Vorteil dieses Ansatzes ist, dass in den wenigen Lücken, die im Interesse der betrieblichen Effektivität verbleiben, die Belastung der Erkennungstools erheblich reduziert ist. Dadurch können sie böswillige Aktionen genauer und effizienter abfangen und so die Anzahl der Alarme und Kosten für menschliche Ressourcen senken.

Schutz vor Zero-Day-Exploits

Zero-Day-Angriffe laufen ins Leere. Cyber-Angriffe, die auf vertrauenswürdige Anwendungen abzielen, sind hochgradig skalierbar mit weitreichenden Auswirkungen. Die Angriffe auf Microsoft Exchange Server hatten Auswirkungen auf Unternehmen, Regierungen und Cybersecurity-Teams auf der ganzen Welt. Angreifer verfeinern ihr Handwerk ständig und von Nationalstaaten unterstützte Angreifer sind entschlossener denn je, Schaden anzurichten. Organisationen müssen ihre fundamentalen Cybersecurity-Fähigkeiten verbessern und Hilfsmittel bereitstellen, die vor einer großen Bandbreite von Angriffen schützen, einschließlich Zero-Day. AppGuard mit seiner patentierten Endpunkt-Absicherungstechnologie wurde so entwickelt, dass es die fortschrittlichsten Angriffstechniken verhindert, einschließlich jener, die in den jüngsten hochkarätigen Angriffen eingesetzt wurden.

Über AppGuard

AppGuard ist ein Cybersecurity-Unternehmen, das es sich zur Aufgabe gemacht hat, einen neuen Standard zu setzen: echter Cyber-Schutz für alle.
Die patentierte Technologie von AppGuard verhindert Kompromittierungen, bevor sie geschehen, indem sie Malware-Aktivitäten daran hindert, Schaden anzurichten, ohne sie wiederkennen zu müssen.

Im Gegensatz zu erkennungsbasierten Lösungen überlistet AppGuard böswillige Akteure, damit Unternehmen ihren Aufgaben nachgehen können und die Schadsoftware nicht machen kann, was sie will.

APPGUARD

Die Malware-Defensive

www.appguard.us | software@ingrammicro.ch