Use Case Gesundheitswesen

TREND MICRO™ | Global Leader in Cybersecurity

Der Schutzschild für ungepatchte Systeme

Virtual Patching

BESTIMMT KENNEN SIE DAS PROBLEM

Server zu patchen ist aufwändig. Denn bevor Sie einen Patch einspielen, müssen Sie ihn erst einmal gründlich testen. Das kostet Zeit, die Sie nicht haben, weil Ihre IT-Abteilung ohnehin schon überlastet ist. Zudem empfiehlt der Branchenstandard B3S für Healthcare-Einrichtungen dringend, dass Sie einen Rollback-Prozess brauchen, falls ein Patch Probleme verursacht. Aber was tun, wenn dieser Fall eintritt?

Im schlimmsten Fall bleiben Sicherheitslücken also über einen längeren Zeitraum hinweg offen, bis man Zeit findet sich darum zu kümmern. Für einige Legacy-Systemen gibt es ohnehin keine Updates mehr, weil das Support-Ende längst überschritten ist. Und manche medizintechnischen Geräte lassen sich nicht patchen, weil sie anschließend nicht mehr richtig funktionieren würden.

Also stecken Sie in einem Dilemma: Sie müssen mit ungepatchten Systemen leben, obwohl Sie sich offene Schwachstellen eigentlich nicht leisten können. Schließlich ist die Gesundheitsbranche besonders stark von Cyberangriffen betroffen.

WARUM HERKÖMMLICHE IDS/IPS-LÖSUNGEN NUR BEDINGT WEITERHELFEN

Mit einer Next Generation Firewall (NGFW) oder einem Intrusion Detection/Intrusion Prevention System versuchen Sie, Angriffe so gut es geht auf Netzwerkebene abzuwehren, bevor diese die verwundbaren Systeme erreichen. Das Problem ist nur:

In der Regel nutzen NGFW und IDS/IPS-Lösungen Exploit-Filter, um Attacken zu blockieren. Ein Filter gilt jeweils für einen speziellen Exploit. Doch Cyberkriminelle entwickeln immer wieder neue Methoden, um eine Schwachstelle auszunutzen. Das Security-System braucht also immer mehr Filter und wird dadurch immer langsamer.

Häufig wird ein neuer Exploit-Filter unter großem Zeitdruck entwickelt, passt dadurch nicht exakt und blockiert lieber etwas großzügiger. So steigt mit jedem neuen Filter die Zahl der False Positives, die dem Security-Team das Leben schwer machen.

Da Exploit-Filter eine Schwachstelle nie komplett abdecken, gibt es immer noch Teile, die verwundbar sind. Es bleibt also ein Restrisiko, dass das Sicherheitssystem Attacken übersieht und die Schwachstelle ausgenutzt wird.

WAS TUN?

Sie brauchen eine IPS-Lösung, die Virtual Patching einsetzt. Diese Technik betrachtet nicht die einzelnen Exploits, sondern die Schwachstelle an sich. Ein virtueller Patch deckt eine Schwachstelle vollständig ab und schützt sie auch gegen künftige Exploits. Der Clou: Die Security-Lösung sieht von außen so aus wie vorher, nur die Schwachstelle ist nicht mehr ausnutzbar. Cyberkriminelle können die Schwachstelle zwar erkennen und versuchen auszunutzen – allerdings ohne Erfolg. So schützt Virtual Patching auch ungepatchte Systeme.

Entscheidend ist, dass ein virtueller Patch möglichst schnell zur Verfügung steht, sobald eine Schwachstelle bekannt wird. Bei Trend Micro garantiert das die Zero Day Initiative (ZDI). In ihr haben sich unabhängige Sicherheitsforscher auf der ganzen Welt zusammengeschlossen, um Schwachstellen aufzudecken. Rund die Hälfte aller weltweit bekannten Vulnerabilities wurden von der ZDI entdeckt.

Daher kann Virtual Patching, das auf Daten der ZDI basiert, bereits Schwachstellen schließen, die noch gar nicht veröffentlicht sind. Im Durchschnitt gewinnen Nutzer so einen Sicherheits-Vorsprung von 96 Tagen, bis ein Hersteller-Patch verfügbar ist.

ZUSAMMEN STARK: IPS UND XDR

IPS mit Virtual Patching kann einen Großteil der Angriffe bereits auf Netzwerkebene abwehren und so die Last für die nachfolgenden Security-Systeme reduzieren. Diese fangen dann die Bedrohungen ab, die noch durchkommen. Es lohnt sich, in eine zuverlässige Lösung für Extended Detection and Response (XDR) zu investieren. Sie sammelt Meldungen aller angeschlossenen Security-Systeme, filtert die relevanten heraus und korreliert sie zu verwertbaren Warnungen.

DARUM LOHNT SICH VIRTUAL PATCHING

- Mit Virtual Patching können Sie auch ungepatchte Legacy-Systeme und Medizintechnik schützen, ohne dass Sie deren Software anfassen müssen.
- Ihre Systeme sind automatisch innerhalb von 24 Stunden nach Bekanntwerden einer Schwachstelle geschützt. Für Schwachstellen, die zuerst von der Trend Micro Zero Day Initiative gefunden werden, kann der Schutz über Trend Micro Tipping Point bereits vor Veröffentlichung der Schwachstelle verfügbar gemacht werden. Im Schnitt ist dies 96 Tage früher als ein vergleichbares Schutzniveau anderweitig erreicht wird.
- Sie gewinnen Zeit. Kritische Schwachstellen sind sofort geschlossen. Sobald ein Hersteller-Patch verfügbar ist, können Sie diesen dann in aller Ruhe testen und einspielen.
- Im Vergleich zu NGF- und IDS/IPS-Systemen mit Exploit-Filtern reduziert IPS mit Virtual Patching die Zahl der False Positives erheblich und ist performanter.

DER PARTNER AN IHRER SEITE

Virtual Patching ist unter anderem in den Trend Micro-Produkten Deep Security, Vision One Endpoint Security, TippingPoint enthalten. Trend Micro liegt im IDPS Market Share von Gartner für Netzwerksicherheitsausrüstung auf Platz 1. Die Zero Day Initiative von Trend Micro ist laut Omdia seit 2007 führender Anbieter in Global Vulnerability Research and Discovery.

Trend Micro (börsennotiert in Tokyo) hat über 30 Jahre Erfahrung als Spezialist für Sicherheitslösungen. Das Unternehmen wird seit 15 Jahren erfolgreich von seiner Mitgründerin Eva Chen geleitet, die als Leading Woman in IT international anerkannt ist. Seit der Gründung im Jahr 1988 achtet sie mit ihrem Managementteam darauf, dass das Unternehmen gesund wächst und reinvestiert auch in Krisenzeiten umfangreich in Forschung und Entwicklung.

Ihr Credo: „Unsere einzige Konkurrenz sind Cyberkriminelle, denen man Einhalt gebieten muss."

Copyright © 2023 Trend Micro Incorporated. Alle Rechte vorbehalten. Trend Micro, das Trend Micro Logo und das T-Ball-Logo sind Marken oder eingetragene Marken von Trend Micro Incorporated. Alle anderen Firmen- bzw. Produktnamen sind Unternehmenskennzeichen oder eingetragene Marken ihrer jeweiligen Eigentümer. Die in diesem Dokument enthaltenen Informationen können sich ohne vorherige Ankündigung ändern. Trend Micro, das Trend Micro Logo und das T-Ball-Logo tragen das Registered-Trade-Mark-Symbol der USA. Einzelheiten darüber, welche personenbezogenen Daten wir erfassen und warum, finden Sie in unserer Datenschutzerklärung auf unserer Website unter: https://www.trendmicro.com/de_de/about/legal/privacy.html.