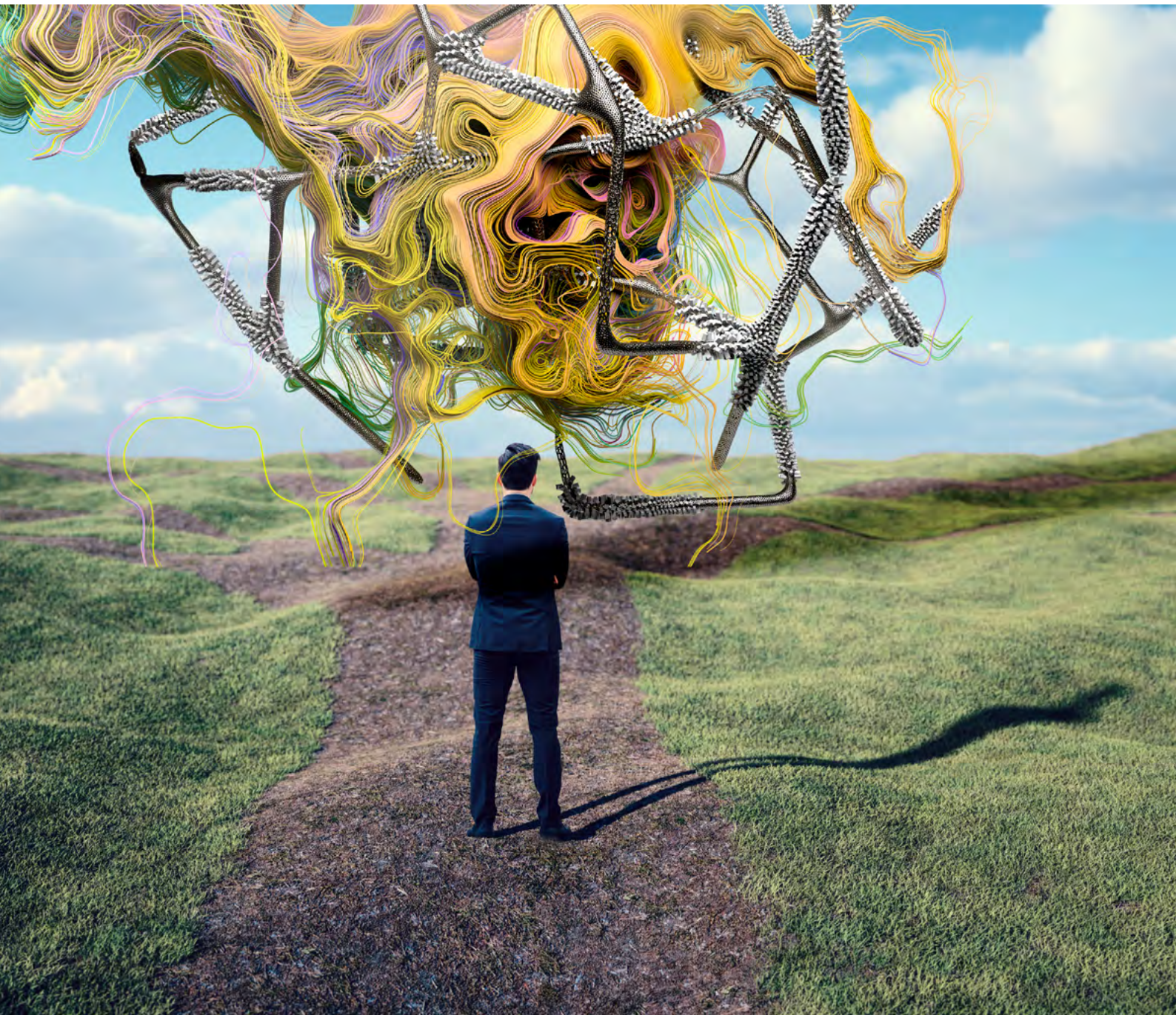
| Finanzdienstleister & Versicherungen

Effizientes Patch-Management in der Hybrid-Cloud

Virtual Patching



PATCH-MANAGEMENT IST COMPLIANCE-VORGABE

Sie brauchen die Cloud, um wettbewerbsfähig zu bleiben und Ihren Kunden attraktive, digitale Services bieten zu können. Bestimmt haben Sie schon Systeme migriert oder planen dies gerade. Damit sind Sie in bester Gesellschaft: Laut einer aktuellen PWC-Studie setzen 78 Prozent der deutschen Banken bereits auf Cloud-Services. Eine der größten Herausforderungen in der Cloud bleibt jedoch die Sicherheit von Unternehmensdaten und die Einhaltung von Compliance-Vorgaben.

Sie müssen unter anderem die BaFin-Anforderungen gemäß BAIT, MaRisk und MaComp erfüllen, PCI-DSS-konform sein und sich mit der PSD 2 und Basel IV herumschlagen. Eine wichtige Compliance-Vorgabe ist stets das Patch-Management – gerade auch für Systeme, die Sie in die Cloud auslagern und außerhalb Ihres geschützten Rechenzentrums betreiben. Doch in komplexen, hybriden Infrastrukturen gestaltet sich das Patching noch aufwändiger als zuvor, weil Sie verschiedene Umgebungen betrachten müssen und oft Transparenz fehlt.

WIE SCHNELL KÖNNEN SIE KRITISCHE PATCHES AUSROLLEN?

Klar ist: Offene Schwachstellen können Sie sich nicht erlauben. Denn in der Finanzbranche stehen hochsensible Zahlungs- und Kundendaten auf dem Spiel, ganz zu schweigen vom Reputationsverlust, den ein Datenschutzvorfall oder ein Service-Ausfall verursachen würde. Das Problem ist nur:

Ihre IT-Infrastruktur ist historisch gewachsen. In einer hybriden Landschaft betreiben Sie möglicherweise auf On-Premise-Ebene noch zahlreiche Legacy-Systeme für die es gar keine Patches mehr gibt. Diese sind besonders leicht angreifbar.

Bevor Sie einen Patch einspielen, müssen Sie ihn erst einmal gründlich testen. Das ist aufwändig und kostet viel Zeit.

Wenn neue Schwachstellen bekannt werden, zählt jede Minute. Sie müssen die Sicherheitslücken schließen und das System patchen, bevor Cyberkriminelle eindringen. Aber was passiert, wenn Sie keine Ressourcen zum Test haben oder der Test Probleme verursacht und länger braucht, als erwartet?

WAS TUN?

Sie brauchen eine Security-Lösung, die Virtual Patching einsetzt. Diese Technik schließt Schwachstellen automatisiert auf Netzwerkebene, sodass Cyberkriminelle sie nicht mehr ausnutzen können. Virtual Patching ist performanter und sicherer als Exploit-Filter, wie sie in herkömmlichen IDS/IPS-Lösungen (Intrusion Detection System/Intrusion Prevention System) und Next-Generation-Firewalls zum Einsatz kommen. Letztere wirken nur gegen Angriffe, die sie kennen. Für jeden neuen Exploit muss ein neuer Filter entwickelt werden. Das bremst das Security-System aus und führt zu einer hohen Zahl an False Positives. Virtual Patching betrachtet dagegen die Schwachstelle an sich und deckt sie komplett ab. So ist sie auch vor künftigen Exploits geschützt.

Je schneller ein virtueller Patch zur Verfügung steht, umso höher die Sicherheit. Bei Trend Micro sorgt die Zero Day Initiative (ZDI) für einen entscheidenden Vorsprung. In ihr haben sich Sicherheitsforscher auf der ganzen Welt zusammengeschlossen. Sie sind für die Erstaufdeckung von rund 50 Prozent aller bekannten Schwachstellen verantwortlich. Daher kann Virtual Patching, das auf Daten der ZDI basiert, bereits Schwachstellen schließen, die noch gar nicht veröffentlicht sind. Im Durchschnitt erhalten Nutzer einen solchen virtuellen Patch bereits 96 Tage früher als einen Hersteller-Patch. Erfahren Sie mehr über die aktuelle Schwachstellenforschung im Omdia Research Whitepaper.

DIE OPTIMALE ERGÄNZUNG: XDR

Da IPS mit Virtual Patching einen Großteil der Angriffe bereits auf Netzwerkebene abwehrt, reduziert sich die Zahl der Events in den nachfolgenden Security-Systemen. Damit Sie noch schneller reagieren können, lohnt sich eine zuverlässige Lösung für Extended Detection and Response (XDR). Sie sammelt Meldungen aller angeschlossenen Security-Systeme, filtert die relevanten heraus und korreliert sie zu verwertbaren Warnungen. Lesen Sie zu XDR auch die Einschätzung von ESG Research.

DIESE VORTEILE BRINGT VIRTUAL PATCHING

- Virtual Patching ermöglicht ein automatisiertes Patch Management in komplexen, hybriden Infrastrukturen.
- Mit Virtual Patching können Sie auch ungepatchte Legacy-Systeme schützen.
- Kritische Schwachstellen werden sofort geschlossen. Dadurch gewinnen Sie Zeit. Sobald ein Hersteller-Patch verfügbar ist, können Sie diesen dann in aller Ruhe testen und einspielen.
- Ihre Systeme sind in der Regel innerhalb von 24 Stunden geschützt, sobald eine Schwachstelle bekannt wird. Für Schwachstellen, die die Trend Micro Zero Day Initiative zuerst entdeckt, kann Trend Micro Tipping Point bereits vor Veröffentlichung virtuelle Patches bieten. Im Schnitt ist dies 96 Tage früher als ein vergleichbares Schutzniveau anderweitig erreicht wird.
- 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 Produkten Deep Security, Cloud One, Apex One und TippingPoint von Trend Micro enthalten. Trend Micro liegt im IDPS Market Share von Gartner für Netzwerksicherheitsausrüstung (1. Quartal 2020) 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."

TREND MICRO
Securing Your Connected World