DATEN SCHÜTZEN

HARDWAREBASIERTE SECURITY MACHT IHR RECHENZENTRUM SICHERER

Moderne Rechenzentren müssen immer mehr leisten, beispielsweise für HCI-Anwendungen, Cloud-Instanzen, Host-basierte VPS oder Edge-Computing.

Dochbeim Schutz Ihres Rechenzentrums geht es um mehr als nur um Software-Patches. Wissen Sie, wie Sie Integritätsbedrohungen und Hypervisor-basierte Angriffe wie Datenwiedergabe oder Speicher-Re-Mapping – verhindern können, um eine isolierte Ausführungsumgebung zu gewährleisten?

DIE ANTWORT:

IT- und Sicherheitsteams sollten mit Servern beginnen, die auf einem Fundament aus Hardware und Silizium mit integrierten Sicherheitsfunktionen aufgebaut sind.

CYBERANGRIFFE NEHMEN ZU – UND DAMIT AUCH INVESTITIONEN IN DIE SICHERHEIT

FORTWÄHRENDE ANGRIFFE

Cybersecurity Ventures prognostiziert, dass im Jahr 2031 alle zwei Sekunden ein Ransomware-Angriff erfolgen wird. Dabei wird die Malware immer effektiver und die damit verbundenen Erpressungsaktivitäten verfeinert.[1]

GESTIEGENE AUSGABEN

Gartner® prognostiziert, dass „die Ausgaben der Enduser für Informationssicherheit und Risikomanagement im Jahr 2021 bei konstanter Währung um 10,14 % steigen werden. Die für den Zeitraum 2020 bis 2025 prognostizierte jährliche Wachstumsrate von 10,1 % (bei kontstanter Währung) wird den Markt bis 2025 auf 221 Milliarden US-Dollar ansteigen lassen.“[2]

DIE FOLGEN VON CYBERANGRIFFEN SIND SEHR REAL

Cybersecurity Ventures schätzt, dass die Kosten, die durch Ransomware entstehen, bis zum

JAHR 2031 265 MILLIARDEN US-DOLLAR BETRAGEN WERDEN[4]

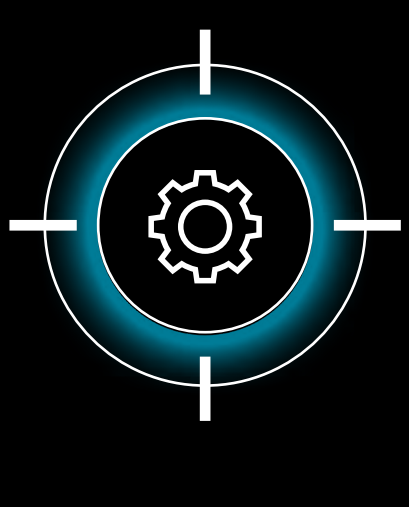
Durchschnittliche Kosten für jeden erfoglreichen Angriff:

4,24 MILLIONEN US-DOLLAR[3]

HYPERVISOR-ANGRIFFE SIND EINE SEHR ERNSTZUNEHMENDE GEFAHR

Kriminelle Hacker haben den Hypervisor im Visier, da er die Kontrolle über alle anderen Systembereiche ermöglicht.

Eine Kompromittierung des Hypervisors kann zur Folge haben, dass der Angreifer vollen Zugriff auf VMs, das physische System und die gehosteten Anwendungen erlangt.



MIT AMD EPYC™ PROZESSOREN KÖNNEN SIE SICH DAVOR SCHÜTZEN

Bei der Sicherheit geht es nicht nur um den Schutz an der Peripherie oder innerhalb der Software – Sicherheitsfunktionen auf dem Silizium können für zusätzliche Sicherheit sorgen.

Die Funktionen der AMD Secure Memory Encryption sind in die CPU integriert, direkt auf dem Chip. Damit kann AMD ein schwieriges Branchenproblem angehen: die Verschlüsselung von Daten, während diese aktiv sind.

Zusätzlich zum AMD Secure Processor enthalten die AMD EPYC™ Prozessoren Verschlüsselungs-Engines in den Speicher-Controllern. Dies trägt dazu bei, schnelle verschlüsselte Speicherlese- und -schreibvorgänge zu gewährleisten, ermöglicht hardware-validiertes Booten und kann mit einer einzigen (ursprünglich installierten) CPU gekoppelt werden.

WEITERE FUNKTIONEN DES AMD EPYC™-PROZESSORS

- ☑ Schutzschichten für aktive Daten
- ☑ Integrierte AES-128-Verschlüsselung
- ☑ Vollständige Speicherverschlüsselung
- ☑ Kryptografische Isolierung für bis zu 509 virtuelle Maschinen
- ☑ Der Code für vorhandene x86 Kundenanwendungen darf nicht geändert werden

Weitere Informationen über den AMD-Ansatz für hardware-basierte Sicherheit

ERFAHREN SIE MEHR

[1] https://cybersecurityventures.com/global-ransomware-damage-costs-predicted-to-reach-250-billion-usd-by-2031/

[2] Gartner, „Forecast Analysis: Information Security and Risk Management, Worldwide”, Shailendra Upadhyay, Mark Driver et al, Aug12, 2021.

[3] https://newsroom.ibm.com/2021-07-28-IBM-Report-Cost-of-a-Data-Breach-Hits-Record-High-During-Pandemic?wpisrc=nl_cybersecurity202#:~:text=CAMBRIDGE%2C%20Mass.%2C%20July%2028%2C%2020

[4] https://cybersecurityventures.com/global-ransomware-damage-costs-predicted-to-reach-250-billion-usd-by-2031/

Gesponsert von AMD. AMD, das AMD Logo, EPYC und Kombinationen davon sind Marken von Advanced Micro Devices, Inc.

GARTNER ist eine eingetragene Marke und Dienstleistungsmarke von Gartner, Inc. und/oder deren Tochtergesellschaften in den USA und international und wird hier mit Genehmigung verwendet. Alle Rechte vorbehalten.

Nachdruck mit freundlicher Genehmigung der IBM Corporation© 2022