DELL Technologies

intel®

Ausfallsicherheit bei Cyberangriffen

Bekämpfen Sie Bedrohungen mit einem umfassenden Sicherheitskonzept, angefangen bei Dell PowerEdge-Servern, gestützt von skalierbaren Intel® Xeon® Prozessoren.

Jetzt loslegen

Inhaltsverzeichnis

Klicken Sie auf die Symbole oder Kapitelüberschriften unten, um zu bestimmten Abschnitten zu navigieren. Verwenden Sie die Pfeilschaltflächen oben, um von Seite zu Seite zu navigieren. Verwenden Sie die Startschaltfläche oben links, um zum Start zurückzukehren.

Teil 1: Die Cybersicherheitslandschaft

Stärker werdende Bedrohungen

Cyberbedrohungen und -angriffe werden immer verheerender und häufiger – ein Trend, der sich voraussichtlich noch verstärken wird. Im Jahr 2020 prognostizierte Cybersecurity Ventures, dass die weltweiten Kosten für Cyberkriminalität in den darauf folgenden fünf Jahren pro Jahr um 15 % steigen und bis 2025 jährlich 10,5 Billionen US-Dollar erreichen würden, während sie sich 2015 noch auf 3 Billionen US-Dollar beliefen.[1] Die Tatsache, dass Daten über viele Geräte, stationär sowie über die Cloud, aufgerufen werden, führt dazu, dass die Anzahl an schweren Datenschutzverletzungen weiter steigt. Um eine sicherere Umgebung zu gewährleisten, müssen Unternehmen einen umfassenderen Ansatz verfolgen.

Die digitale Transformation sorgte ab Beginn des neuen Jahrtausends für große Schlagzeilen, doch die Entwicklung nahm erst ab 2020 an Fahrt auf, da Unternehmen sich an neue und sich schnell verändernde Geschäftsumgebungen anpassen müssen. Während immer mehr Unternehmen mit softwarebasierten Rechenzentren (Software Defined Data Center, SDDC) arbeiten, steigt auch deren Abhängigkeit von Servern als Grundlage für Geschäftsfunktionen. Das bedeutet, dass Serversicherheit der grundlegende Aspekt der allgemeinen Verteidigungsstrategie Ihres Unternehmens sein sollte, die Sie bis zur Ebene der Firmware vor Bedrohungen schützt.

Herausforderungen der Cybersicherheit

Ihr Unternehmen ist von allen Seiten mit Cyberbedrohungen konfrontiert. Zu den herkömmlichen Akteuren gehören Hacktivisten, Terrororganisationen, verfeindete Staaten und Länder, kriminelle Organisationen, allein agierende Hacker und Unternehmensspione. In zunehmendem Maße müssen Sie sich allerdings auch vor Insiderbedrohungen schützen.

Aktuell konzentrieren sich die Nachrichtenmeldungen auf die zunehmende Geschwindigkeit, Ausgereiftheit, Effektivität und finanziellen Auswirkungen von Cyberangriffen. So wurden beispielsweise 2021 50 % mehr Cyberangriffe auf Unternehmensnetzwerke pro Woche verzeichnet als 2020.[2] Und während Ransomware im Jahr 2021 weltweit 20 Milliarden US-Dollar kostete, wird diese Summe bis 2031 voraussichtlich auf 265 Milliarden US-Dollar steigen.[3.]

Laut Prognosen werden sich die Kosten für Ransomware-Angriffe weltweit

bis 2031 auf 265 Milliarden US-Dollar belaufen.[3]

[1] CyberCrime Magazine, „Cybercrime To Cost The World $10.5 Trillion Annually By 2025“, 13. November 2020

[2] DARKReading, „Businesses Suffered 50% More Cyberattack Attempts per Week in 2021“, 11. Januar 2022.

[3] Cloudwards, „Ransomware Statistics, Trends, and Facts for 2022 and Beyond“, 22. März 2022.

Zu den häufigsten Angriffen zählen:

Malware – Dazu gehört bösartige Software wie Spyware, Adware oder Viren, die die Leistung oder Sicherheit Ihres Servers beeinträchtigen können.

Ransomware – Ransomware ist eine Form von bösartiger Software oder Malware, die beim Herunterladen auf einen Server den Zugriff auf Daten und Dateien auf dem Gerät blockieren kann, bis ein Lösegeld gezahlt wird.

Phishingangriffe oder Phishing – Phishing beschreibt die Vorgehensweise, mehrere Personen oder Unternehmen auf betrügerische Weise zu kontaktieren, um unbefugten Zugriff auf vertrauliche und/oder personenbezogene Daten zu erhalten.

Lieferkette – Hierzu gehören Situationen, in denen Hacker zunehmend Schwachstellen in der Lieferkette oder bei Drittanbietern ausnutzen möchten, während Unternehmen wie Ihres versuchen, Ihre Sicherheit zu erhöhen. Der Cyberangriff, der 2020 auf SolarWinds, ein großes IT-Managementunternehmen, ausgeführt wurde, wurde monatelang nicht bemerkt, sodass SolarWinds seine Kunden mit schädlichem Code infizierte. Laut Accenture „zielen 40 % der Cyberangriffe auf die Lieferkette ab“.[4]

40 %
der Cyberangriffe zielen auf die Lieferkette ab.[4]

[4] Accenture, „Securing the Supply Chain“, 2020

Cybersicherheitslandschaft | Branchenübliche Best Practices | NIST-Framework-Support | Zero Trust-Modell | Ihr Unternehmenserfolg

Compliance und behördlicher Druck

Da globale Bedrohungen zunehmen, erhöhen Behörden den Druck, Best-Practice-Richtlinien für die Sicherung nicht nur behördlicher und kritischer Infrastrukturen, sondern auch des privaten Sektors zu definieren. Das ist wichtig, weil sich in den USA fast 90 % der kritischen Infrastruktur wie Gesundheitswesen sowie Energie-, Finanz-, Transport-, Telekommunikations- und Versorgungsbranche in Hand von Privatunternehmen befindet.[5]

Im Mai 2021 und Januar 2022 veröffentlichte das Weiße Haus in den USA Anordnungen, die ein Framework zum Schutz der Infrastruktur des Lands skizzierten und detaillierte Anleitungen zur Zero Trust-Architektur enthielten. Doch nicht nur die USA zeigen großen Tatendrang. Regierungen auf der ganzen Welt entwickeln angesichts von Cyberbedrohungen behördliche Richtlinien, und private Institutionen erstellen Richtlinien und Vorschriften, um wiederkehrende Advanced Threats (hochentwickelte Bedrohungen) abzuschwächen. Diese Anforderungen betreffen nicht nur Bundesbehörden, sondern auch kritische Infrastrukturen und andere vertikale Märkte.

Da Regierungen versuchen, Cyberangriffe einzudämmen oder zu minimieren, sollten Unternehmen sich darauf einstellen, in Zukunft mehr Richtlinien und Vorgaben zu erhalten, beispielsweise:

- **Multifaktor-Authentifizierung (MFA):** MFA, auch bekannt als Zwei-Faktor-Authentifizierung (2FA)[6], schützt Daten vor dem Zugriff durch unbefugte Dritte. Es handelt sich um eine Sicherheitstechnologie, die eine Verifizierung von NutzerInnen erfordert, bevor diese Zugriff erhalten, indem zwei oder mehr voneinander unabhängige Zugangsdaten verwendet werden. In den USA müssen Branchen wie „Finanz-, Gesundheits-, Verteidigungs- und Strafverfolgungswesen sowie Regierungen auf Bundesebene für den Zugang zu Systemen, Netzwerken, Websites und Gebäuden bereits eine Zwei-Faktor-Authentifizierung vorweisen“.[7]
- **Data-at-Rest-Verschlüsselung:** Selbstverschlüsselnde Festplatten mit Key-Management der Enterprise-Klasse.

[5] Das Weiße Haus, Pressekonferenz: „Background Press Call on Improving Cybersecurity of U.S. Critical Infrastructure“, 28. Juli 2021.
[6] NIST, „Back to Basics: What’s multi-factor authentication - and why should I care?“, 16. Juni 2016.
[7] Okta, „Which Industries Require Two-Factor Authentication?“, aufgerufen im Juni 2022.

Was steht auf dem Spiel?

Cyberangriffe können für ein Unternehmen verheerend sein. Je nachdem, in wie viele Schichten der Angriff vordringt und welchen Schaden er verursacht, kann die Recovery-Zeit erheblich ausfallen. Die Wiederherstellung nach einem Ransomware-Angriff nimmt durchschnittlich 22 Tage in Anspruch.[8] Dabei müssen sich Unternehmen möglicherweise mit folgenden Problemen auseinandersetzen:

- Ausfallzeit, um zu ermitteln, was passiert ist, und um dann alle verlorenen Daten wiederherzustellen
- Dauerhafter Verlust von internen Daten und Kundendaten, was langfristige Chancen gefährdet
- Zahlung von Bußgeldern sowie Ausgaben für Nachrüstungen, um sicherzustellen, dass alle Regeln und Vorschriften eingehalten werden
- Schlechte Publicity und Geschäftseinbußen als unmittelbare Folge eines Cyberangriffs
- Langfristiger Reputationsverlust, da Kunden zögern, weiterhin Geschäfte mit Unternehmen zu tätigen, die angegriffen wurden

84%

der VerbraucherInnen bestätigten, dass sie Unternehmen, die ihrer Wahrnehmung nach über starke Sicherheitskontrollen verfügen, loyaler gegenüberstehen.[9]

Im Durchschnitt sind

22 Tage

notwendig, um nach einem Ransomware-Angriff die Wiederherstellung durchzuführen.[8]

Einige Unternehmen sind so sehr auf den Geschäftsausbau konzentriert, dass sie dazu neigen, die entsprechenden Sicherheitsvorkehrungen zu übersehen, die das Unternehmen schützen und bewahren. Wenn eine Sicherheitslücke ausgenutzt wird, kann das jedoch die Leistungsfähigkeit Ihres Unternehmens schnell beeinträchtigen. In Kombination mit der Tatsache, dass Infrastruktur, Workloads und Datennutzung immer komplexer werden, ist die Aufrechterhaltung einer sicheren IT-Infrastruktur und eines sicheren IT-Betriebs deutlich komplizierter geworden.

Die digitale Transformation schafft zwar unbegrenzte Chancen, aber die Herausforderungen beim Aufbau einer flexiblen, modernen IT-Umgebung bei gleichzeitiger Aufrechterhaltung des Vertrauens von Seiten Ihrer Kunden und Stakeholder bleiben bestehen. Wenn Sie den wachsenden Sicherheitsbedrohungen nicht immer einen Schritt voraus bleiben, kann der Schaden katastrophale Formen annehmen. Eine bemerkenswerte Erkenntnis ist, dass 64 % der US-amerikanischen NutzerInnen eher das Unternehmen als die Hacker verantwortlich machen würden, wenn es bei einem Angriff zum Verlust ihrer personenbezogenen Daten kommt.[9] Darüber hinaus bestätigten 84 % der VerbraucherInnen, dass sie Unternehmen, die ihrer Wahrnehmung nach über starke Sicherheitskontrollen verfügen, loyaler gegenüberstehen.[10]

[8] Statista, „Length of impact after a ransomware attack Q1 2020- Q3 2021“, November 2021.

[9] Forbes, „50 Stats Showing Why Companies Need To Prioritize Consumer Privacy“, 22. Juni 2020.

[10] Untersuchungsbericht von SalesForce, „State of the Connected Customer: Third Edition“, Juni 2019.

Ressourcen

Cybersichere Architektur – Infografik

Cybersichere Architektur – Video

Cybersicherheit bei Dell PowerEdge-Servern – Technisches Whitepaper

Teil 2: Branchenübliche Best Practices

Zero Trust

ist ein Architekturansatz, bestehend aus einem Framework aus Sicherheitsprinzipien und Best Practices.

Zero Trust ist eine Antwort auf die Komplexität moderner IT-Umgebungen, einschließlich Cloud und Hybrid Cloud – Cloud-basierte Bestände, die sich nicht innerhalb der Netzwerkgrenzen Ihres Unternehmens befinden. Diese problematische Komplexität wird durch die jüngste Zunahme von RemotenutzerInnen, Millionen BYOD-Geräten (Bring Your Own Devices) und anderen gesetzlichen Vorschriften noch weiter verschärft.

Zero Trust ist keine isolierte Architektur, sondern besteht aus einer Reihe von Leitprinzipien für Workflow, Systemdesign und Betrieb. Effektive Sicherheitsansätze haben sich von einem statischen, groben Perimeteransatz zu einem viel wandelbareren Konzept entwickelt – in dessen Rahmen Ressourcen oder Nutzerkonten, die ausschließlich auf ihrem physischen oder Netzwerkstandort oder ihren Eigentumsrechten an Beständen basieren, kein Vertrauen gewährt wird.

Mit anderen Worten: Ein Zero Trust-Ansatz bewertet und validiert viele Punkte in der IT-Umgebung, bevor Berechtigungen erteilt werden. Das entscheidende Element von Zero Trust ist die Überprüfung von Ressourcen innerhalb des Unternehmens, bevor Zugriff darauf gewährt wird, – sowie die kontinuierliche Überprüfung vor der Prozessausführung oder lateralen Verschiebungen innerhalb des Netzwerks.

In Folge erfolgreicher Ransomware-Angriffe auf Bundesbehörden, kritische Infrastrukturen und den privaten Sektor ist der Druck durch gesetzliche Auflagen erheblich gestiegen. Ein Beispiel hierfür ist die Anordnung des Weißen Hauses, die am 12. Mai 2021 in Kraft trat. Seitdem wurden große Mengen an Dokumentationen erstellt, die Details zur Sicherheitsimplementierung und neue Vorschriften enthalten. Da sich die gesetzlichen Leitlinien immerzu weiterentwickeln, betrachten Unternehmen Sicherheitslösungen nicht mehr als optional, sondern als unabdingbar.
Zero Trust-Anforderungen, die mit der Publikation SP800-207 für das US-Verteidigungsministerium begannen, wurden in Verbindung mit der Anordnung des Weißen Hauses und in Zusammenarbeit mit den US-amerikanischen Behörden CISA und OMB weiter definiert. Wir stellen fest, dass Regierungen auf der ganzen Welt denselben Weg einschlagen und sogar noch strengere Auflagen erlassen.[11]

Ressourcen

Zero Trust-Architektur – Infografik

[11] NIST, „Zero Trust Architecture“, 10. August 2020.

Teil 3: Ein sicheres Fundament als Ausgangspunkt

Die Sicherheitsphilosophie von Dell fußt auf Ausfallsicherheit bei Cyberangriffen.

Der Aufbau einer effektiven Ausfallsicherheit bei Cyberangriffen beginnt mit der Vision, Ihr Unternehmen während des gesamten Gerätelebenszyklus vor böswilligen Akteuren zu schützen. In Übereinstimmung mit dem NIST-Framework zur Cybersicherheit (NIST SP800-160) setzt Dell einen SDL-Ansatz (Security Development Lifecycle) ein, um Produkte und Lösungen zu entwickeln, die Sicherheitsanforderungen von Design, Fertigung, Lieferkette und Management bis hin zur Außerbetriebnahme umfassen.

- Serverfirmware ist darauf ausgerichtet, die Einschleusung von bösartigem Code in allen Phasen des Produktentwicklungslebenszyklus zu blockieren und abzuwehren.
- In jeder Phase der Firmwareentwicklung kommen sichere Programmierverfahren zum Einsatz.
- Wichtige Bestandteile des Designprozesses sind Bedrohungsmodellierung und Penetrationstests.

Der Schutz Ihrer Daten und von geistigem Eigentum erfordert einen mehrschichtigen Ansatz. Bei Dell PowerEdge-Servern sind Sicherheitsfunktionen absichtlich so konzipiert, dass es zur Überlappung von Schichten kommt. Wenn also ein Mechanismus infiziert wird, ist bereits eine andere Schicht vorhanden, um den Angriff abzuwehren. Dieser „Defense-in-Depth“-Ansatz bietet eine verbesserte Ausfallsicherheit und ist das Herzstück unserer cybersicheren Architektur.

PowerEdge-Server sind mit skalierbaren Intel Xeon Prozessoren ausgestattet, die erweiterte Sicherheitsfunktionen bieten, einschließlich Intel SGX, was dazu beiträgt, Daten und Anwendungscode in Echtzeit zu schützen – vom Edge über das Rechenzentrum bis hin zur Multi-Tenant-Public-Cloud. Dies ermöglicht eine verbesserte Zusammenarbeit (z. B. für föderiertes Lernen in KI) mit gemeinsam genutzten Daten – ohne Gefährdung des Datenschutz. Intel Crypto Acceleration steigert die Performance von verschlüsselungsintensiven Workloads, einschließlich SSL-Web-Serving, 5G-Infrastruktur und VPN/Firewalls, und reduziert die Performanceauswirkungen einer umfassenden Verschlüsselung.

Diese Architektur baut auf bestehender PowerEdge-Sicherheit mit erweiterten Funktionen auf, die Ihre Infrastruktur effektiv schützt, indem sie Bedrohungen zuverlässig erkennt und sich nach Cyberangriffen schnell wiederherstellen lässt. Es handelt sich um einen Ansatz, der die wichtigsten Komponenten des NIST-Framework (NIST SP 800-193) erfüllt.

Silicon Root of Trust (chipbasierte Sicherheit)

PowerEdge-Server verwenden eine unveränderliche chipbasierte Root of Trust, um die Integrität des BIOS und der iDRAC-Firmware (Integrated Dell Remote Access Controller) kryptografisch zu attestieren. Diese Root of Trust basiert auf einmal programmierbaren, schreibgeschützten öffentlichen Schlüsseln, die Schutz vor Manipulationen durch Malware bieten.
Als einer der wichtigsten Aspekte der Serversicherheit muss gewährleistet werden, dass der Startvorgang als sicher verifiziert werden kann. Die Root of Trust bietet einen vertrauenswürdigen Anker für Startvorgänge. Ergänzend dazu nutzt der BIOS-Startprozess die Technologie Intel Boot Guard, die überprüft, ob die digitale Signatur des kryptografischen Hash des Start-Image mit der von Dell Technologies werkseitig auf dem Chip gespeicherten Signatur übereinstimmt.

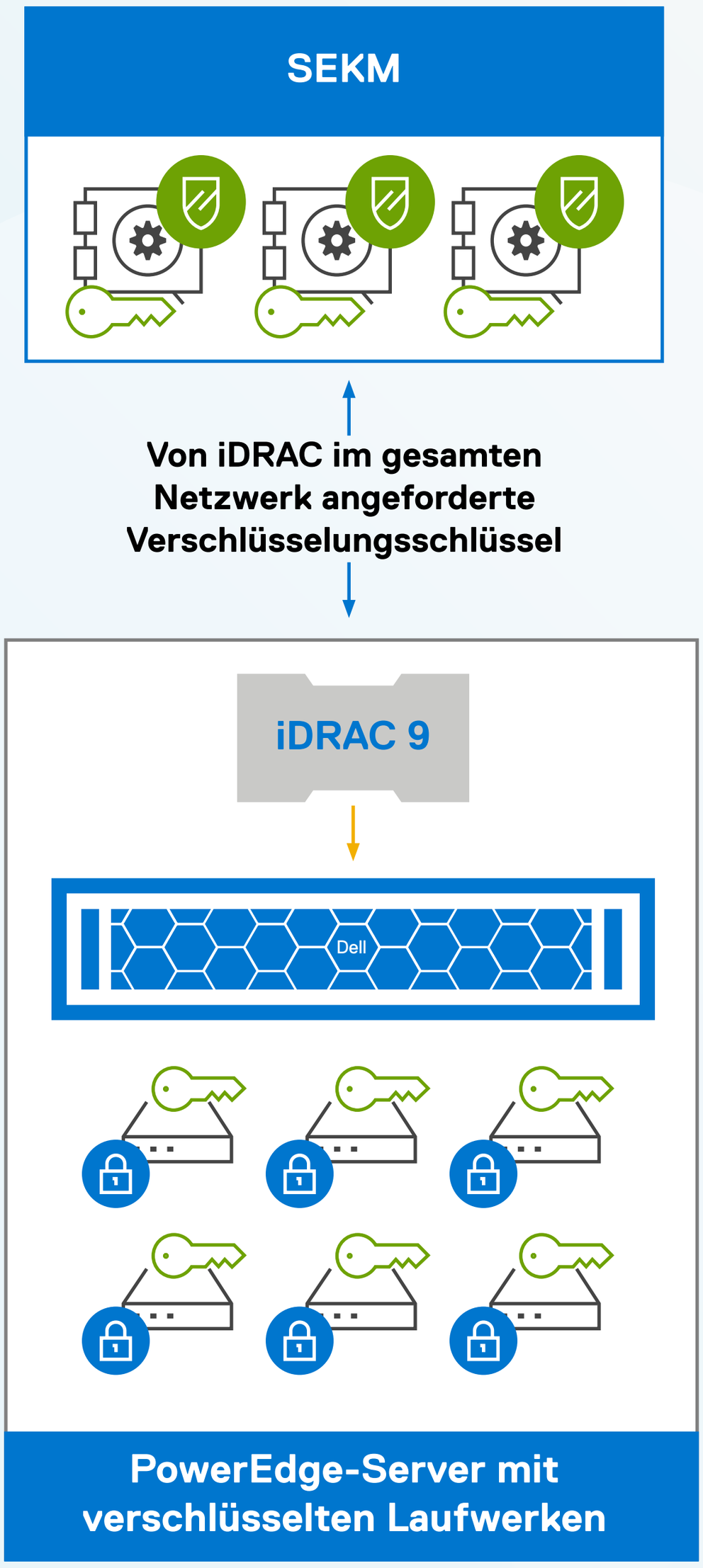
Identitäts- und Zugriffsmanagement

Identitäts- und Zugriffsmanagement (Identity and Access Management, IAM) ist ein kritischer Bereich, insbesondere hinsichtlich des Schutzes vor Ransomware-Angriffen mit Kontrollen wie MFA, um einen Sicherheitsansatz mit geringstmöglichen Berechtigungen und Zero Trust zu ermöglichen. IAM ist darauf ausgelegt, sicherzustellen, dass nur die richtigen Personen auf geeignete IT-Ressourcen und -Daten zugreifen und den Umfang des Zugriffs kontrollieren können.

Erweiterte Data Protection

Data Protection beinhaltet den Schutz Ihrer Geschäftsdaten in der Regel durch Verschlüsselung, egal ob sie im Einsatz sind bzw. ob sie übertragen werden („in transit) oder im Ruhezustand („at rest“) sind. PowerEdge-Server bieten eine breite Palette an sicheren Storage-Optionen für Ihre Daten.

Externes Key-Management ist eine Best Practice, bei der Schlüssel außerhalb von Laufwerken und Hostservern gespeichert werden. Secure Enterprise Key Manager (SEKM) ermöglicht PowerEdge-Kunden die zentrale Verwaltung von Schlüsseln für SEDs in PowerEdge-Servern und eine Skalierung mit Erweiterung der Storage-Kapazität. Das lokale Key-Management (LKM) ist auch für Umgebungen verfügbar, in denen der zentrale Zugriff schwierig sein kann oder die Sicherheitsanforderungen weniger streng sind.



Beispiel für SEKM-Implementierung

Ressourcen

Data Protection – Infografik

SEKM – Website

SEKM – Video

Aktivieren von OpenManage Secure Enterprise Key Manager (SEKM) auf Dell PowerEdge-Servern – Technisches Whitepaper

SEKM – Infografik

Cybersichere Architektur – Video

Dell Security Development Lifecycle

Dell Technologies erzeugt bewusst Code für Sicherheitskontrollen für jede Phase des Serverlebenszyklus, von der Erfassung von Anforderungen bis hin zur Serverwartung. Dazu gehört Code, der entwickelt wurde, um eine Einschleusung zu verhindern, abzuwehren und zu bekämpfen.

Cybersicherheitslandschaft

Branchenübliche Best Practices

NIST-Framework-Support

Zero Trust-Modell

Ihr Unternehmenserfolg

Verifizierte Sicherheit in der Lieferkette

Der umfassende Ansatz von Dell Technologies für Lieferkettensicherheit umfasst grundlegende Maßnahmen wie die Anwesenheit von Mitarbeitern und Cybersicherheitskontrollen. Außerdem verbessert Dell Technologies mit seinem Angebot Secured Component Verification (SCV) die Sicherheit der Komponentenintegrität. Mit SCV können Kunden kryptografisch überprüfen, ob die werkseitig eingestellten Komponenten mit den gelieferten Komponenten übereinstimmen.

Sicherheit bietet die Vertraulichkeit, Integrität und Verfügbarkeit von Informationen, die die IT-Lieferkette beschreiben, oder durchzieht die IT-Lieferkette und bietet Informationen über die Parteien, die an daran beteiligt sind.

Integrität stellt sicher, dass IT-Produkte oder -Services in der IT-Lieferkette original und unverändert sind und gemäß den Spezifikationen der erwerbenden Partei und ohne zusätzliche unerwünschte Funktionen ausgeführt werden.

Qualität reduziert Schwachstellen, die die beabsichtigte Funktion einer Komponente einschränken, zu Komponentenausfällen führen oder Angriffsstellen für böswillige Absichten bieten können.

Resilienz stellt sicher, dass die IT-Lieferkette die erforderlichen IT-Produkte und -Services trotz Unterbrechungen bereitstellt.

Ressourcen

Secured Component Verification – Video

Secured Component Verification – Technischer Hinweis

Secured Component Verification – Tech-Talk

NCC Group: Secured Component Verification Security Assessment – Technisches Whitepaper zur Lieferkette

Vorteile cybersicherer Produkte

- Maximale Verfügbarkeit für Mitarbeiterproduktivität
- Wahrung des Rufs des Unternehmens
- Kundenvertrauen
- Compliance zur Vermeidung kostspieliger Bußgelder und Nachrüstungen
- Freiheit für Innovationen ohne Ablenkung

Teil 4: Mit Ausfallsicherheit bei Cyberangriffen Zero Trust-Anforderungen erfüllen

Der Zero Trust-Ansatz von Dell Technologies wurde optimiert, um die Standards des US-Verteidigungsministeriums zu erfüllen. Wir ermöglichen eine Zero Trust-Architektur durch umfangreiche cybersichere Funktionen und einen auf sieben Säulen basierenden Ansatz, mit dem sich NutzerInnen an jedem Punkt in der IT-Umgebung verifizieren können, bevor Berechtigungen erteilt werden.

Säule 1: Vertrauensstellung bei Geräten

Unsere chipbasierte Hardware-Root of Trust bietet ein Schutzschild über den gesamten Serverlebenszyklus hinweg – vom Design bis zur Außerbetriebnahme. Unsere sichere Lieferkette umfasst mehrere Kontrollebenen, z. B. die Komponentenüberprüfung, um sicherzustellen, dass unsere Server und Software nicht manipuliert oder in böswilliger Absicht verändert wurden. SCV bietet kryptografisch signierte Bestandszertifikate für das gesamte Portfolio von PowerEdge-Servern, einschließlich sicherer Selbstverifizierung, sodass Sie sich bei der Übertragung zu Ihrem Rechenzentrum auf die Integrität Ihrer Hardware verlassen können.

Säule 2: Vertrauensstellung bei NutzerInnen

Mit iDRAC können IT-Administratoren PowerEdge-Server lokal oder remote sicher bereitstellen, aktualisieren und überwachen. Um die Sicherheit zu erhöhen, bietet iDRAC MFA mit RSA SecureID auch mit Integrationen über Active Directory, LDAP-Integration mit Single Sign-On (SSO) und mit rollenbasierter Zugriffskontrolle und -prüfung.

Säule 3: Vertrauensstellung bei Transport und Sitzungen

Der PowerEdge BMC (iDRAC) verfügt über ein dediziertes Netzwerkmodul und Optionen für SSH (Secure Shell)/TLS (Transport Layer Security) zur Verschlüsselung und Authentifizierung der Daten, die zwischen Server(n) und dem Browser übertragen werden, in dem Ihre iDRAC-Webbenutzeroberfläche ausgeführt wird. Der iDRAC ermöglicht Remotemanagement und überwacht das System mit Sensoren auf der Hauptplatine auf kritische Ereignisse. Warnmeldungen und Protokollereignisse werden versendet, wenn Parameter ihre vorhandenen Schwellenwerte überschreiten.

Säule 4: Vertrauensstellung bei Software

Wir führen während des gesamten Softwarelebenszyklus proaktive Verifizierungs-, Validierungs- und Sicherheitstests durch, um unsere Software zu schützen und die Wahrscheinlichkeit zu verringern, dass Malware- oder Codesicherheitslücken darin eingefügt werden. Der umfassend verifizierte Start beinhaltet signierte BIOS- und Firmware-Images, die sicherstellen, dass nicht autorisierter Code nicht auf einem PowerEdge-Server ausgeführt wird. Weitere cybersichere Funktionen umfassen die automatisierte Erkennung von Abweichungen, sichere UEFI-Startfunktionen und Recovery für BIOS und Betriebssysteme.

Säule 5: Vertrauensstellung bei Daten

SEKM arbeitet für die hardwarebasierte Verschlüsselung mit selbstverschlüsselnden Laufwerken sowie mit skalierbarem zentralem Key-Management zusammen, um Sie bei der Bereitstellung und Überwachung von Verschlüsselungsschlüsseln zu unterstützen, einschließlich an Remotestandorten und sogar in der Cloud. Dies bietet Schutz vor unbefugtem Zugriff auf verlorene oder gestohlene Laufwerke oder Systeme. Diese Hardwareverschlüsselung kann mit Softwareverschlüsselung wie VMware® vSAN™ Verschlüsselung auf VxRail kombiniert werden.

Confidential Compute ermöglicht den Schutz von Data-in-Use-Daten auf der CPU und im Arbeitsspeicher und umfasst Technologien von Intel (SGX, TME). Intel SGX bietet Isolierung auf Anwendungs- oder Funktionsebene, um den Vertrauensperimeter zu minimieren.

Die Kombination von Data-at-Rest-Verschlüsselung, skalierbarem Key-Management und Confidential Compute ist dazu in der Lage, das Maß an Schutz zu bieten, das erforderlich ist, um den immer stärker werdenden Bedrohungen von heute entgegenzuwirken.

Säule 6: Transparenz und Analysen

Die Fähigkeit, zu beobachten, was in Ihrer Umgebung vor sich geht, ist von entscheidender Bedeutung. Die Erkennung von Firmwareabweichungen bietet beispielsweise Echtzeiteinblicke in den Integritätsstatus der Firmware, einschließlich unbefugter Änderungen. Wenn Änderungen erkannt werden, kann das System in einen bekannten sicheren Zustand zurückgesetzt werden. Darüber hinaus können Änderungsereignisse über automatisierte Protokollierung und Warnmeldungen nachverfolgt werden, die Audit und Analyse zur Bewertung der umfassenden Systemintegrität unterstützen.

Säule 7: Automatisierung und Orchestrierung

OpenManage Enterprise ist eine Anwendung für Systemmanagement und -monitoring, die einen umfassenden Überblick über PowerEdge-Server, internen Storage und andere Komponenten bietet. Sie umfasst die Erkennung von Abweichungen zum Auffinden von Änderungen an einer nutzerdefinierten Konfigurationsvorlage, die Erstellung von Warnmeldungen und Protokollen zur Nachverfolgung des Systemstatus und die Korrektur von Fehlkonfigurationen basierend auf Richtlinien vor der Konfiguration. OpenManage umfasst Firmware-Rollback, zentralisierte Updates, automatische SSL-Zertifikatsverlängerungen (Secure Sockets Layer) und automatisierte Bereitstellungen für eine konsistente Sicherheitskonfiguration.

Ressourcen

OpenManage Secure Enterprise Key Manager – Lösungsübersicht

Verstehen von Confidential Computing mit vertrauenswürdigen Ausführungsumgebungen und Trusted Computing – Basismodelle

Zero Trust-Architektur – Infografik

Zero Trust – Video

Teil 5: Ihr Unternehmen mit Dell Technologies und Intel auf Erfolg ausrichten

Die zunehmende Ausgereiftheit und die wachsende Angriffsfläche von Bedrohungen erfordern einen modernisierten Ansatz der Ausfallsicherheit bei Cyberangriffen. Unsere Antwort besteht darin, Sie mit einer Reihe von Tools und Technologien beim Aufbau einer Zero Trust-Architektur zu unterstützen. Unser Sicherheitsansatz ermöglicht noch feiner abgestimmte Steuerungen, die von Zugriff und Autorisierung bis hin zur Daten- und Systemstabilität reichen und gleichzeitig ein erstklassiges Nutzererlebnis bieten.

Mit Dell Technologies und Intel als Partner erhalten Sie Folgendes:

- Bewährte Ausfallsicherheit bei Cyberangriffen mit integrierter statt aufgesetzter Sicherheit
- Problemloses Abwägen zwischen Geschäftszielen und Produktivität sowie Sicherheit und Datenschutz
- Eine Hardware- und Software-Suite, die entwickelt wurde, um Ihre IT-Infrastruktur zu schützen und gleichzeitig Vertrauen, Kontrolle und Skalierbarkeit für Ihren Sicherheitsstatus zu bieten
- Kontinuierliche Wachsamkeit zur Aufrechterhaltung eines starken Sicherheitsstatus durch schnelle Reaktion auf gängige Schwachstellen und deren Ausnutzung

Ressourcen

Sicherheitslösungen – Webseite

Business Resiliency Services

Managed Detection and Response

Weitere Informationen zu cybersicheren PowerEdge-Servern finden Sie unter Dell.com/Servers.

Abonnieren Sie unseren beliebten Dell Technologies Power2Protect-Podcast und hören Sie sich die neuesten Folgen zu den Themen Sicherheit und Ausfallsicherheit bei Cyberangriffen an.

Cybersicherheitslandschaft

Branchenübliche Best Practices

NIST-Framework-Support

Zero Trust-Modell

Ihr Unternehmenserfolg