INFORMATION TECHNOLOGY
INTELLIGENCE CONSULTING

ITIC 2021 Globaler Server-Hardware, Serverbetriebssystem-Sicherheitsbericht

Juni 2021

Inhaltsverzeichnis

Kurzübersicht

Das dritte Jahr in Folge bewerteten Kapitalgesellschaften geschäftskritische Server von IBM, Lenovo, Huawei und Hewlett-Packard Enterprise (in dieser Reihenfolge) als die sichersten Plattformen, die die geringste Anzahl erfolgreicher Datenschutzverletzungen erlebten und sich als am schwersten zu hacken erwiesen.

Das sind die Ergebnisse der aktuellen ITIC-Befragung über Globale Server Hardwaresicherheit, bei der die Sicherheitsmerkmale und -funktionen von 15 verschiedenen Server-Plattformen verglichen wurden. Die unabhängige webbasierte Befragung von ITIC befragte von Januar 2021 bis Mitte Juni 2021 über 1.100 Unternehmen weltweit in 28 verschiedenen Branchen.

IBM, Lenovo, Huawei, HPE und Cisco behaupteten ihre Positionen als die zuverlässigsten und sichersten Serverplattformen trotz eines signifikanten Anstiegs von Sicherheitshacks um 42 % und von Datenschutzverletzungen während der weltweiten COVID-19 Pandemie in den letzten 18 Monaten.

Die Top-Server, angeführt vom IBM Z, IBM POWER, Lenovo ThinkSystem und Huawei KunLun (in dieser Reihenfolge), erzielten bei der aktuellen ITIC-Befragung alle ihre jeweils besten Sicherheits- und Zuverlässigkeits-/Uptime-Leistungen während COVID-19 und erzielten insbesondere die besten Sicherheitsergebnisse unter allen 15 Mainstream-Server-Hardware-Plattformen in jeder Sicherheitskategorie, einschließlich:

- Die geringste Zahl erfolgreicher Sicherheitshacks/Datenverletzungen.
- Die insgesamt geringste ungeplante Serverausfallzeit aufgrund ***beliebiger*** Gründe und die geringste ungeplante Serverausfallzeit aufgrund eines Sicherheitsvorfalls.
- Die schnellste Mean Time to Detection (MTTD)vom Beginn der Attacke bis zur Isolierung und Deaktivierung seitens des Unternehmens.
- Die schnellste Mean Time to Remediation (MTTR), um Server, Anwendungen und Netzwerke zum vollständigen Betrieb zurückzubringen.
- Die geringste Anzahl an verlorenen, gestohlenen, gelöschten, beschädigten oder veränderten Daten als direkte Folge einer Sicherheitsdatenverletzung (z. B. Ransomware, Phishing-Betrug oder CEO-Betrug).
- Die geringsten Geldverluste aufgrund eines erfolgreichen Sicherheitsangriffs.
- Das höchste Vertrauen in die eingebettete Sicherheit der Server-Hardware bezüglich der Bereitstellung von Alarmen/Warnungen und der Abwehr von Sicherheitsangriffen und Datenverletzungen.

Unternehmenskritische Systeme von Hewlett-Packard Enterprise (HPE) und Cisco lieferten ebenfalls eine hohe Sicherheitsstufe und rundeten die Top-Five der sichersten Server ab. Auf der anderen Seite des Spektrums erwiesen sich die markenfreien White-Box-Server erneut als die durchlässigsten Server und verzeichneten die höchste Anzahl an erfolgreichen Sicherheitsdurchdringungen.

Die aktuelle ITIC-Befragung zur globalen Sicherheit ergab ebenfalls, dass die geschäftskritischen Server von IBM, Lenovo, Huawei und HPE die niedrigsten Prozentsätze von Ausfallzeiten aufgrund erfolgreicher Sicherheitsangriffe und Datenschutzverletzungen erfahren haben (**Siehe Anhang 1).**

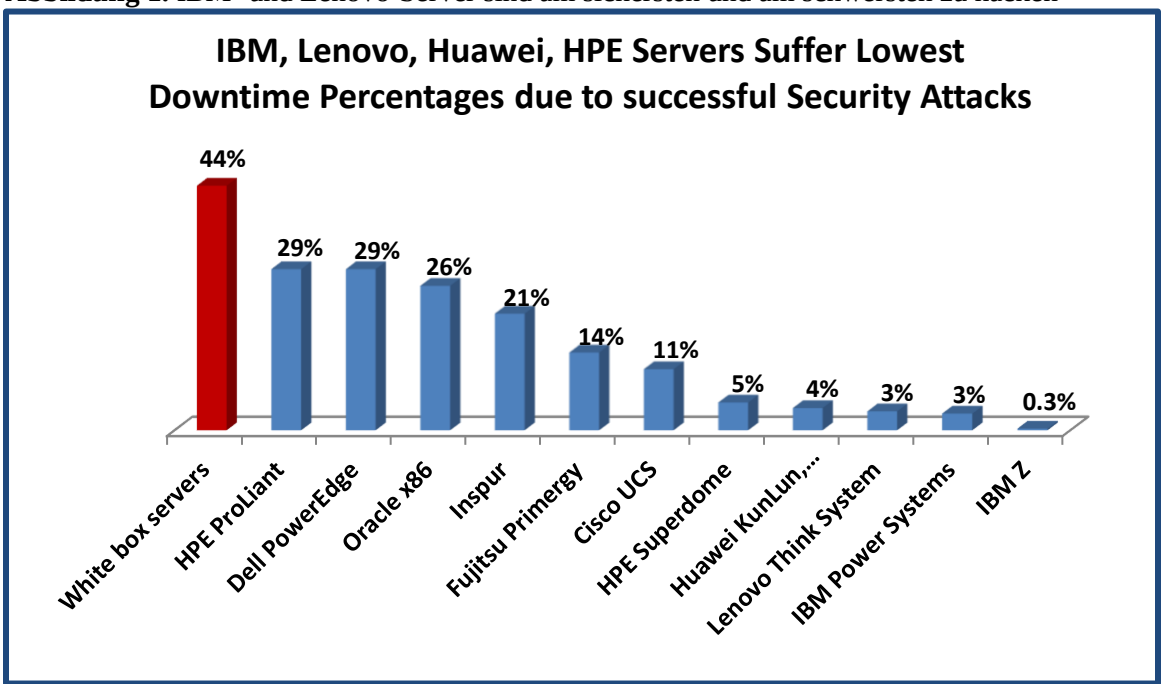
Der IBM Z Mainframe übertrifft alle anderen Server und ist eine Klasse für sich, da er in der neuesten ITIC-Studie die bisher höchsten Sicherheitsniveau- und Zuverlässigkeitsbewertungen erreicht hat.

Nur ein verschwindend geringer Anteil (0,3 %) der IBM Z High-End-Server erlitt eine erfolgreiche Datenschutzverletzung. Von anderen Mainstream-Hardware-Plattformen meldeten nur drei Prozent (3 %) der IBM Power Systems- und Lenovo ThinkSystem-Anwender, dass ihre Systeme erfolgreich gehackt wurden, während weniger als vier Prozent (4 %) der Huawei KunLun- und fünf Prozent (5 %) der HPE Integrity Superdome Server-Kunden eine erfolgreiche Sicherheitsverletzung von Januar 2021 bis Mitte Juni 2021 meldeten.

Etwas mehr als jeder zehnte oder 11 % der Cisco UCS-Server wurden erfolgreich gehackt. Ciscos Hardware schnitt extrem gut ab, vor allem wenn man bedenkt, dass viele der UCS-Server an entfernten Standorten und an der Netzperipherie implementiert sind, die häufig die erste Verteidigungslinie sind und

die Hauptlast an Hackerangriffen tragen. Markenfreie White-Box-Server waren am anfälligsten für Sicherheitsverletzungen; 44 % der Befragten der ITIC-Umfrage gaben an, dass diese Systeme erfolgreich gehackt wurden.

Abbildung 1. IBM- und Lenovo-Server sind am sichersten und am schwersten zu hacken



Quelle: ITIC 2021 Global Server Hardware, Server OS Security Survey

Insgesamt geben die Ergebnisse der ITIC-Umfrage an, dass es einen deutlichen und erweiterten Abstand bei der Server-Hardwaresicherheit und -Zuverlässigkeit zwischen den leistungsfähigsten Plattformen und den unsichersten Angeboten gibt. Die weltweite Pandemie löste im Zusammenhang mit COVID-19 eine Welle von Datenschutzverletzungen, Ransomware, Phishing, Business Email Compromise (BEC), CEO-Betrug und Angriffen aus, die unvermindert weitergehen.

Die jüngsten Umfrageergebnisse des ITIC geben an, dass Zuverlässigkeit und Sicherheit untrennbar miteinander verwoben und sogar symbiotisch sind. Sicherheits- und Datenverletzungen untergraben unmittelbar die Verfügbarkeit der betroffenen Server, Anwendungen und Netzwerke. Sicherheitshacks und Datenschutzverletzungen sind kostenintensiv und gefährlich. Sie gefährden das geistige Eigentum (IP) von Unternehmen sowie das von Geschäftspartnern, Kunden und Lieferanten. Ein erfolgreicher Sicherheitshack kann auch die persönlichen Daten der Mitarbeiter offenlegen.

Es ist kein Zufall, dass die Top-Five der zuverlässigsten Serverplattformen (IBM Z, IBM Power Systems, Lenovo ThinkSystem, Huawei KunLun und Fusion Server, HPE Superdome Integrity und Cisco UCS, in dieser Reihenfolge) auch die beachtlichste Sicherheit aufweisen.

Einführung

Die weltweite Pandemie löste im Zusammenhang mit COVID-19 eine Welle von Datenschutzverletzungen, Ransomware, Phishing, Business Email Compromise (BEC), CEO-Betrug und Angriffen aus, die unvermindert weitergehen, und zwar in jeder Branche, der auf unzählige Unternehmens- und Konsumenten-Geräte und Software abzielt.

Niemand und nichts ist immun. Dies macht eine inhärente, stabile Infrastruktursicherheit unabdingbar.

Die aktuelle ITIC-Befragung ergab, dass insgesamt 73 % der Umfrageteilnehmer befürchten, dass ihre Organisationen in den weiteren 12 bis 18 Monaten einem gezielten Angriff durch professionelle Hacker zum Opfer fallen werden. Dieser Zeitplan deckt sich mit dem weit verbreiteten Trend von Schulen, Colleges und Universitäten, Studenten und Lehrern, die Fernunterricht hatten und sich nun auf regulären Präsenzunterricht vorbereiten. Ebenso wechseln derzeit viele Unternehmen und Behörden als Sicherheitsmaßnahme zu einem hybriden Homeoffice-Modell.

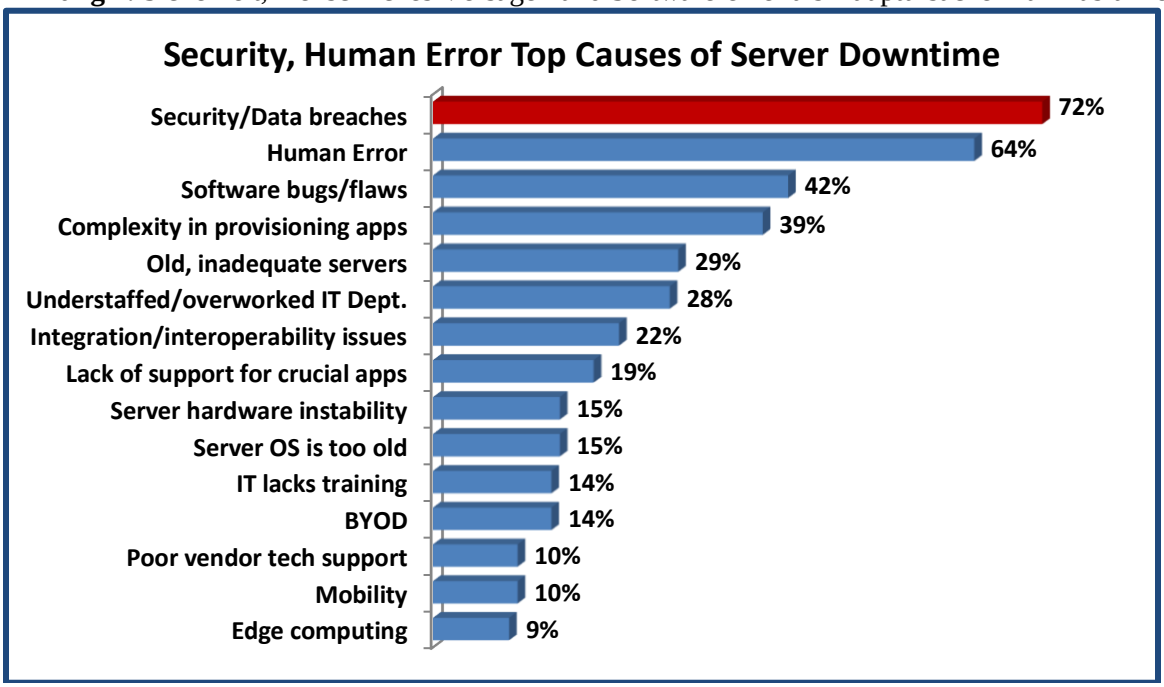
Die jüngsten Ergebnisse der ITIC-Sicherheitsstudie werden durch verschiedene US-Bundesbehörden gestützt, die seit Anfang 2020 mehrere Warnungen vor Cybersicherheitsrisiken herausgegeben haben. Das Federal Bureau of Investigation (FBI), die Cybersecurity and Infrastructure Security Agency (CISA) des Department of Homeland Security und das Office of Compliance Inspections and Examinations (OCIE) der Securities and Exchange Commission (SEC).

Laut FBI-Warnungen, die im Mai und Juni veröffentlicht wurden, umfassen die Cybersicherheitsbedrohungen im Zusammenhang mit COVID-19: Betrügereien, die auf Versicherungsleistungen für Arbeitslose und staatliche Bonuszahlungen (Federal Stimulus Checks) abzielen; Gesundheitswesen; Banken; ältere Menschen; Kryptowährung und Regierungsbetrug. Das FBI stellt fest, dass es auch Fälle von „...Kriminellen gibt, die sich auf betrügerisches Verhalten online gegenüber Kindern konzentrieren, die während der Pandemie ihren Unterricht von zu Hause fortsetzen."

Die starken Sicherheitsergebnisse von IBM, Lenovo, Huawei, HPE und Cisco (in dieser Reihenfolge) sind besonders bemerkenswert, da sie während der weltweiten COVID-19-Pandemie erzielt wurden. Etwa 40 % der von ITIC Befragten berichteten, dass ihre Server, Betriebssysteme und kritische Geschäftsanwendungen seit Beginn von COVID-19 Anfang 2020 von erfolgreichen Sicherheitshacks betroffen waren. Dies ist ein Zuwachs von neun Prozentpunkten gegenüber 31 % in den letzten sechs Monaten und ein Anstieg von 21 Prozentpunkten gegenüber den 19 % der Unternehmen, die in der ITIC-Befragung 2020 (Global Server Hardware, Server OS Reliability) angaben, dass ihre Server erfolgreich gehackt wurden.

Sicherheit ist ein Technologie- und Geschäftsproblem, das sich auf alle Unternehmen auswirkt. Rund 72 % der Befragten nannten Sicherheit und Datenschutzverletzungen als größte Bedrohung für die Zuverlässigkeit von Servern, Anwendungen, Rechenzentren, Netzperipherien und Cloud-Ökosystemen **(siehe Anhang 2)**. Die Hacks sind gezielter, orts- und zeitunabhängig und schädlich. Sie sind so konzipiert, dass sie ihren Opfern, den Unternehmen und Konsumenten, maximale Schäden und Verluste zufügen.

Anhang 2. Sicherheit, menschliches Versagen und Softwarefehler als Hauptursachen für Ausfallzeiten



Quelle: ITIC 2021 Global Server Hardware, Server OS Security Survey

Die Bedrohungslandschaft: Sicherheitslücken und Datenschutzverletzungen sind hinsichtlich der Zuverlässigkeit die größte und teuerste Bedrohung

Datenschutzverletzungen sind ein großes Geschäft und ein primäres Geschäft für die aufkeimende professionelle Hacker-Community. Ein erfolgreicher Hack ist auf vielen Ebenen kostenintensiv. Laut der gemeinsam von IBM und dem Ponemon Institute 2020 durchgeführten Studie Cost of a Data Breach[1] belaufen sich die Kosten für eine Datenschutzverletzung auf durchschnittlich 3,86 Millionen Dollar. Dies entspricht einem Zuwachs von 10 % seit 2015. Die tatsächlichen Kosten variieren je nach Dauer und Schwere der Hacker-Angriffe. Ransomware-Angriffe sind weiterhin präsent.

[1] „2020 Cost of a Data Breach Study", IBM und Ponemon Institute. URL: https://www.ibm.com/security/data-breach

Und sie sind sehr kostenintensiv. Der Ransomware-Angriff vom 07. Mai 2021 durch die DarkSide-Hacker legt die Colonial Pipeline Co. für sechs Tage still[2]. Die Colonial Pipeline liefert 45 % der Gas- und Dieselbrennstoffe an die US-Ostküste von New Jersey nach Florida. Der Angriff legte Lieferungen still und verursachte Gasmangel in mehreren Staaten, darunter Florida, North Carolina und Virginia. Er endete erst, als der Generaldirektor von Colonial Pipeline, Joseph Blount, zustimmte, den Hackern ein Lösegeld von 4,4 Millionen Dollar zu zahlen. Blount sagte gegenüber The Wall Street Journal, dass er die Lösegeldzahlung in Höhe von 4,4 Millionen Dollar genehmigte, da die Führungskräfte nicht wussten, wie sehr die Cyberattacke in die Systeme eingedrungen war und wie lange es folglich dauern würde, den Betrieb der Pipeline wiederherzustellen.

Der Colonial Pipeline Ransomware-Angriff ist nur einer von vielen. Er hebt die Schwachstellen, Risiken und hohen Kosten im Zusammenhang mit erfolgreichen Sicherheitsangriffen hervor. Der Colonial Pipeline Ransomware-Angriff verstärkt ebenfalls die Notwendigkeit, über eine einwandfreie Sicherheitsinfrastruktur zu verfügen. Server-Hardware ist das grundlegende Element eines jeden Unternehmensnetzes und Geschäftsumfeldes.

Ein DTEX Systems-Bericht fand heraus, dass „nur 30 % der Organisationen darauf vorbereitet waren, einen vollständigen Wechsel auf Remote-Arbeit zu schützen." Die Studie von DTEX Systems hat auch herausgefunden, dass fast 75 % der Organisationen hinsichtlich der Sicherheitsrisiken, die durch Home-Office-Nutzer eingeführt werden, besorgt sind und 73 % der Unternehmen haben zugegeben, dass sie nur teilweise oder keine Einsicht in die Nutzeraktivität haben, wenn ihr VPN durch Remote-Arbeiter inaktiviert wird. Ein weiteres alarmierendes Ergebnis ist, dass Telearbeiter ihre Firmenlaptops für die persönliche Nutzung verwenden; 25 % der Befragten geben an, dass dies das Risiko von Drive-by-Downloads erhöht, und 15 % sagen, dass ihre Unternehmen anfälliger für Phishing-Angriffe geworden sind.

Die jüngste Studie des ITIC zeigt, dass die stündlichen Kosten aufgrund von Ausfallzeiten weiter steigen. Bei 89 % der Unternehmen übersteigen sie inzwischen 300.000 $. Insgesamt gaben 42 % der befragten mittelgroßen und großen Unternehmen an, dass eine Stunde Ausfallzeit ihre Firmen mehr als eine Million (1 Million Dollar) kostet. In einem Worst-Case-Szenario kann eine Datenschutzverletzung, die während hoher Auslastungsstunden auftritt und entscheidende Geschäftsoperationen unterbricht, Unternehmen Millionen pro Minute kosten. Jede Organisation, die eine langwierige Betriebsunterbrechung von Stunden

[2] „Colonial Pipeline CEO Tells Why He Paid Hackers a $4.4 Million Ransom," The Wall Street Journal, 19. Mai 2021. URL: https://www.wsj.com/articles/colonial-pipeline-ceo-tells-why-he-paid-hackers-a-4-4-million-ransom-11621435636

oder Tagen als Ergebnis einer gezielten Ransomware-Attacke erleidet, wird mit ziemlicher Sicherheit viele Millionen an Schäden erleiden.

Neben den offensichtlichen monetären Einbußen aufgrund von Produktivitätsverlusten und gestörten Unternehmensaktivitäten müssen Unternehmen Personalressourcen und die Anzahl der IT- und Sicherheitsadministratoren, die in Abwehrmaßnahmen und vollständige Wiederaufnahme des Betriebs involviert sind, berücksichtigen. Die Unternehmen müssen auch bestimmen, ob Daten oder geistiges Eigentum (IP) verloren gegangen, gestohlen, beschädigt, gelöscht oder verändert wurden oder nicht. Organisationen müssen bei Sicherheitsvorfällen und Datenschutzverletzungen auch in die Kosten eines etwaigen Rechtsstreits sowie mögliche zivil- oder strafrechtliche Geldstrafen berücksichtigen. Einige Kosten, z. B. Beschädigung des Ansehens einer Organisation, sind unkalkulierbar und können zu entgangenen Geschäften führen.

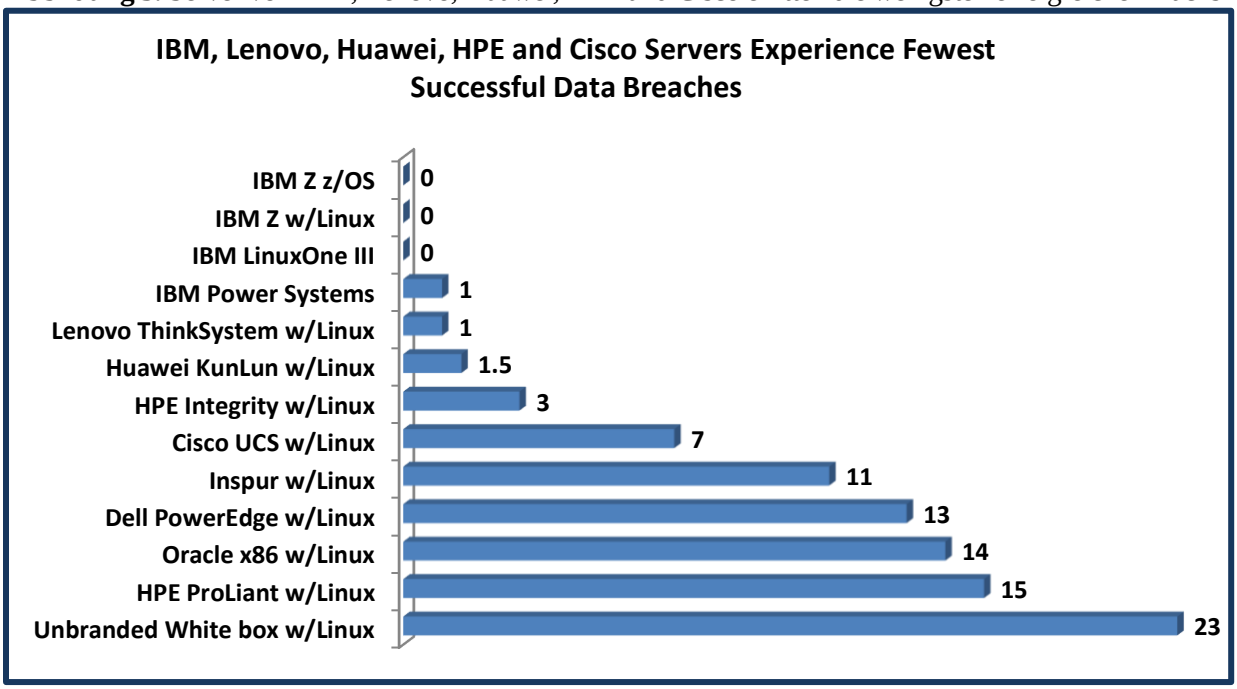
Hacker wählen ihre Ziele sehr präzise aus und nutzen sehr schnell jede Gelegenheit aus. Die COVID-19-Pandemie ist das beste Beispiel hierfür. Hacker visierten unverzüglich Telearbeiter und an Online- und Zoom-Klassen teilnehmende Schüler an. Sie konzentrierten sich auf so genannte „leicht verwundbare Ziele“. Kommunen und Gemeinden, kleine und mittelgroße Schulbezirke, Krankenhäuser, Gesundheitseinrichtungen, Arztpraxen und Bankfilialen, denen es vor Ort an in Vollzeit beschäftigtem Sicherheitspersonal und IT-Administratoren mangelt und die möglicherweise nicht die neueste Sicherheitsvorrichtungen installiert haben.

Server-Anbieter: IBM, Lenovo, Huawei und HPE erhöhen die Sicherheit

Es überrascht nicht, dass Anbieter wie IBM, Lenovo, Huawei und HPE, die immer wieder erstklassige Bewertungen bezüglich der Server-Zuverlässigkeit erreichen, auch zu den am meisten geschützten Hardware-Plattformen gehören. Diese Anbieter und in jüngerer Zeit auch Cisco haben die Serversicherheit – und im Fall von Lenovo Server-, PC- und Laptop-Sicherheit – zu einer Top-Priorität gemacht und in den letzten Jahren stark in die Stärkung der inhärenten Sicherheit ihrer Produktangebote investiert. Als die COVD-19 Pandemie einschlug, verfügten sie also bereits über eine starke, eingebettete Sicherheit und das kam ihnen zugute.

Wie **Anhang 3** zeigt, gab es bei den am meisten geschützten Server-Hardware-Plattformen die wenigsten erfolgreichen Sicherheitsverletzungen. Die Befragten von IBM Z mit z/OS, Red Hat Enterprise Linux (RHEL) und IBM LinuxONE III gaben alle an, dass diese Plattformen in den 16 Monaten keine erfolgreichen Sicherheitsangriffe erlitten. Es folgten IBM Power Systems- und Linux ThinkSystem-Server mit je einem, Huawei KunLun mit durchschnittlich zwei Hacker-Angriffen, HPE Integrity mit drei erfolgreichen Sicherheitsverletzungen und Ciscos UCS Server mit sieben Datenverletzungen. Die markenfreien White-Box-Server waren mit durchschnittlich 20 erfolgreichen Datenschutzverletzungen in den letzten 16 Monaten am anfälligsten.

Abbildung 3. Server von IBM, Lenovo, Huawei, HPE und Cisco erlitten die wenigsten erfolgreichen Hacks



Quelle: ITIC 2021 Global Server Hardware, Server OS Security Survey

Daten & Analysen: Anbieterergebnisse in Bezug auf Sicherheit

Die ITIC-Umfrage 2021 zur Sicherheit von Server-Hardware ergab, dass die Server IBM Z, IBM Power Systems, Lenovo ThinkSystem und Huawei KunLun und Fusion (in dieser Reihenfolge) in jeder Sicherheitskategorie die besten Ergebnisse erzielten:

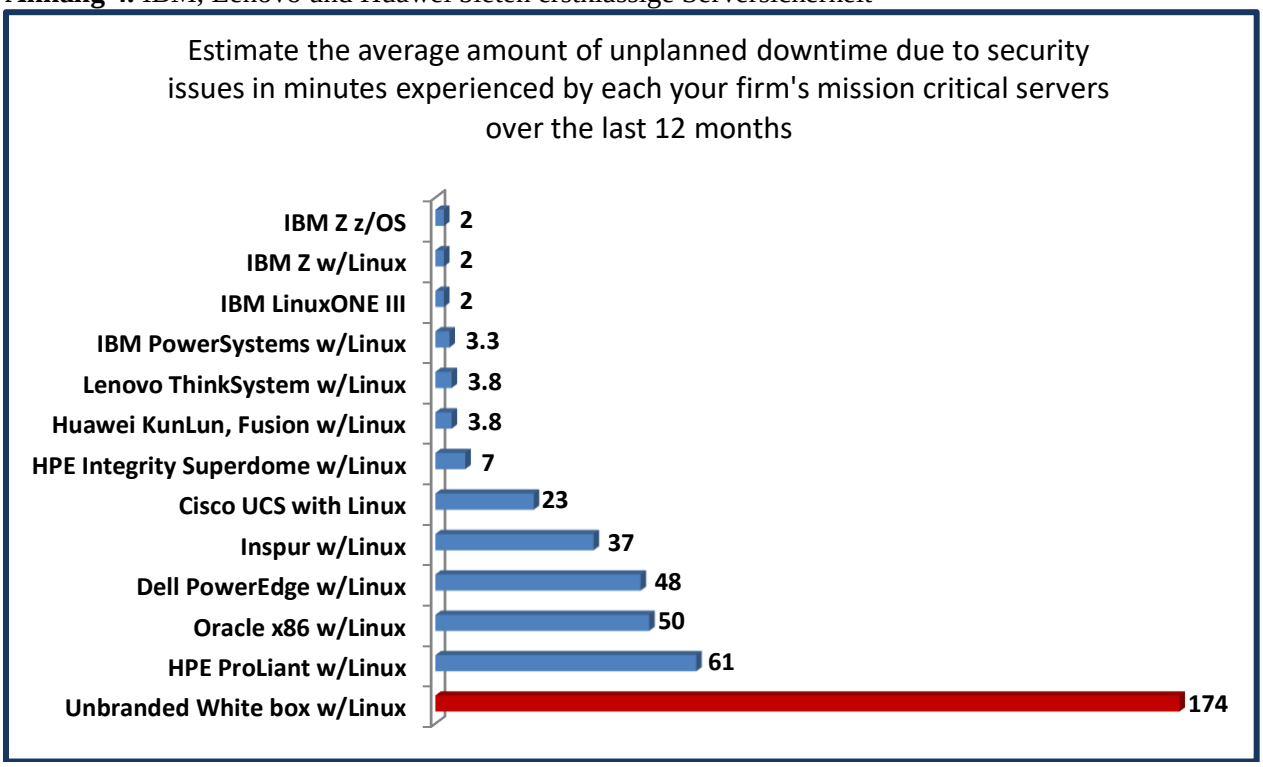
- Die geringste Anzahl **erfolgreicher** Sicherheitsangriffe/Datenschutzverletzungen.
- Die insgesamt geringste ungeplante Serverausfallzeit aufgrund ***beliebiger*** Gründe und die geringste ungeplante Serverausfallzeit aufgrund eines Sicherheitsvorfalls.
- Die schnellste Mean Time to Detection (MTTD)vom Beginn der Attacke bis zur Isolierung und Deaktivierung seitens des Unternehmens.
- Die schnellste Mean Time to Remediation (MTTR), um Server, Anwendungen und Netzwerke zum vollständigen Betrieb zurückzubringen.
- Die geringste Anzahl an verlorenen, gestohlenen, gelöschten, beschädigten oder veränderten Daten als direkte Folge einer Sicherheitsdatenverletzung (z. B. Ransomware, Phishing-Betrug oder CEO-Betrug).
- Die geringsten Geldverluste aufgrund eines erfolgreichen Sicherheitsangriffs.

- Das höchste Vertrauen in die eingebettete Sicherheit der Server-Hardware bezüglich der Bereitstellung von Alarmen/Warnungen und der Abwehr von Sicherheitsangriffen und Datenverletzungen.

Wie **Anhang 4** veranschaulicht, erlitten die geschäftskritischen Server IBM Z, IBM Power Systems, Lenovo ThinkSystem und Huawei KunLun die geringste Anzahl an ungeplanter Ausfallzeit als direktes Ergebnis von erfolgreichen Sicherheits- und Datenverletzungen.

IBM Z und IBM LinuxONE III kamen im Durchschnitt jeweils auf nur 2 Minuten ungeplanter Ausfallzeit pro Server aufgrund von Sicherheitsproblemen. Sie wurden dicht gefolgt von IBMs POWER8- und POWER9-Servern, die aufgrund eines Sicherheitsproblems auf knapp über 3 Minuten ungeplante Ausfallzeit kamen; die Lenovo ThinkSystem-Hardware und die Huawei KunLun- und Fusion-Server erlebten jeweils einen Durchschnitt von 3,8 Minuten ungeplanter Ausfallzeit pro Server aufgrund von Sicherheitsvorfällen. Wieder einmal haben markenfreie White-Box-Server, von denen viele unlizenzierte Versionen von Server-Betriebssystemen und Software-Anwendungen ausführen, 174 Minuten oder knapp drei Stunden Ausfallzeit, direkt zurechenbar zu sicherheitsrelevanten Probleme, erlitten. Das macht die am meisten geschützten IBM Z Server bis zu 87x sicherer und zuverlässiger als die unsichere White-Box-Hardware, während die Angebote von IBM POWER8 und POWER9 bis zu 58x sicherer sind als markenfreie White-Box-Server.

Anhang 4. IBM, Lenovo und Huawei bieten erstklassige Serversicherheit



Quelle: ITIC 2021 Global Server Hardware, Server OS Security Survey

Die durchschnittliche Zeit bis zur Erkennung ist ein kritisches Barometer

Sicherheitshacks und Datenschutzverletzungen sind im digitalen Zeitalter ein Teil des Geschäfts. Irgendwann wird jede Organisation und deren Server, Server-Betriebssysteme und Anwendungen ihrer kritischen Hauptgeschäftszweige Opfer einer versuchten oder erfolgreichen Datenschutzverletzung werden.

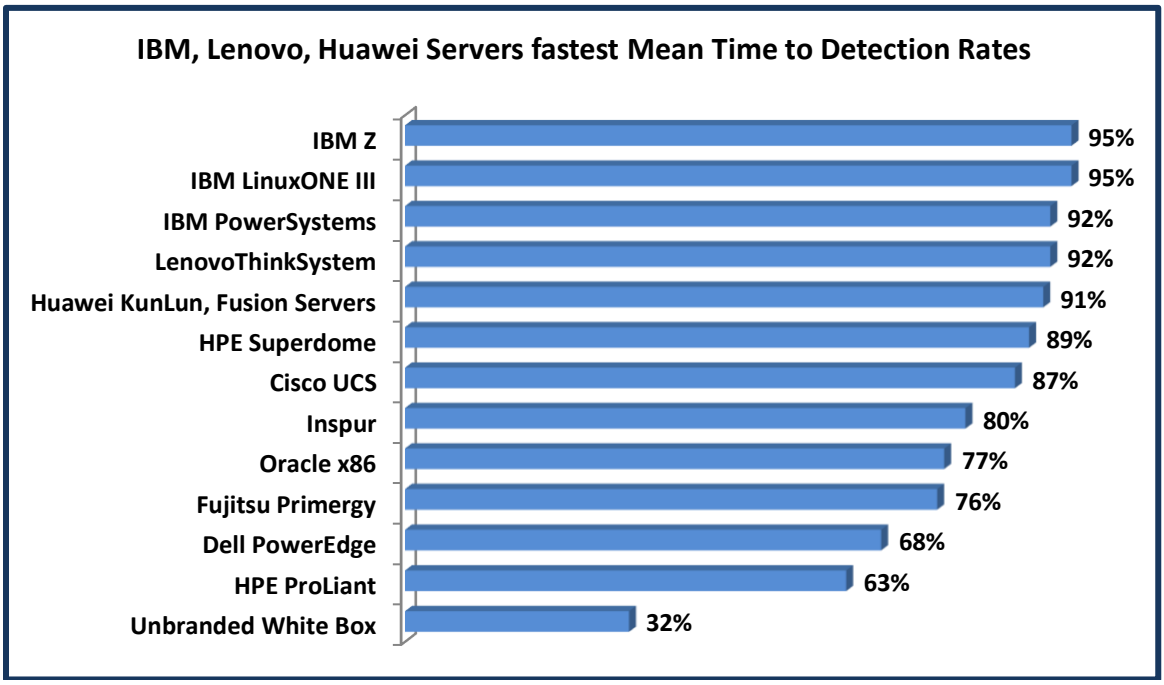
Organisationen müssen sich auf eine stark eingebettete Server- und Infrastruktur-Sicherheit verlassen, die Gefahren erkennt, Warnungen und Alarme ausgibt und Bedrohungen isolieren kann. Eine starke Vorbereitung auf Seiten des Unternehmens und ein gut ausgebildetes Personal von Sicherheitsexperten und IT-Administratoren sind von größter Bedeutung.

Je schneller die Server und Software des Unternehmens ein Sicherheitsproblem finden und darauf reagieren können, desto größer sind die Chancen, Angriffe zu isolieren und zu vereiteln, ***bevor*** sie das direkte Geschäftsumfeld des Netzwerks infiltrieren, Datentransaktionen und tägliche Unternehmensaktivitäten unterbrechen und vertrauliche Daten und gesitiges Eigentum abrufen können.

Abbildung 5 zeigt, dass die IBM Z-, IBM Power Systems-, Lenovo ThinkSystem-, Huawei KunLun- und Fusion-Server, HPE Superdome- und Cisco UCS-Server (in dieser Reihenfolge) einmal mehr bei der Abwehr von Hackerangriffen herausragten. Diese Server hatten die besten MTTD (Mean Time to Detection)-Werte aller Server-Plattformen.

Überwältigende 95% der IBM Z, IBM LinuxOne III Umfrageteilnehmer gaben an, dass ihre Server in der Lage waren, einen versuchten Sicherheitsverstoß "sofort oder innerhalb der ersten 10 Minuten" des Hacks zu finden und ihn auszuschalten. Ihnen folgten IBM Power Systems, Lenovo ThinkSystem und Huawei KunLun; jeweils 92 % dieser Plattform-Nutzer gaben an, einen Sicherheitsverstoß „sofort oder innerhalb der ersten 10 Minuten“ erkennen und abwehren zu können. Je schneller die infrastrukturkritischen Server, Betriebssysteme und geschäftskritischen Anwendungen einen Hacker-Angriff abwehren können, desto besser stehen die Chancen, dass der Betrieb wenig bis keine Ausfallzeit erleidet oder Opfer von gestohlenen, veränderten, beschädigten oder gefährdeten Daten und IP-Diebstahl wird.

Abbildung 5. Über 90 % der Server von IBM, Lenovo und Huawei erkennen Sicherheitsangriffe sofort oder innerhalb der ersten 10 Minuten



Quelle: ITIC 2021 Global Server Hardware, Server OS Security Survey

Sicherheitsergebnisse von Serveranbietern

Highlights der IBM-Sicherheitsumfrage

- **IBM Z**-Server erzielen weiterhin erstklassige Ergebnisse unter allen Serverplattformen in Bezug auf Zuverlässigkeit, Erreichbarkeit, Leistung und Sicherheit. Die IBM Z-Produktfamilie („Z“ steht für „Zero“-Ausfallzeit) übertrifft konsistent **alle** Mitbewerber in jeder Kategorie bezüglich Zuverlässigkeit und liefert die niedrigsten Gesamtbetriebskosten (total cost of ownership, TCO) und schnellsten Investitionserträge (return on investment, ROI). Die Server der Systeme z13, z14 und z15 erzielten die besten Ergebnisse in Bezug auf Zuverlässigkeit/Verfügbarkeitszeit, Anwendungsverfügbarkeit und durchgängige Sicherheit hinsichtlich der tatsächlichen Minuten ungeplanter Ausfallzeit pro Server/pro Jahr. Der IBM z Mainframe und die IBM LinuxONE zeigen wahre Fehlertoleranz mit nur 0,60, weniger als eine Minute ***ungeplanter*** Ausfallzeit pro Server, pro Jahr aufgrund von Serverfehlern, verglichen mit den 0,74 Sekunden, die die Z- und LinuxONE-Plattformen in der Global Server Reliability-Umfrage von ITIC im Jahr 2019 durchschnittlich erreichten. Während die Reduktion von 0,14 Sekunden YoY pro Server-Ausfallzeit unbedeutend klingt, senkt sie die Ausfallzeit um fast 19 % und die TCO der IBM Z und LinuxONE um 230 $, von 1.232 $ pro Server/pro Minute im Jahr 2019 auf 1.002 $ pro Server/pro Minute in der aktuellen ITIC 2021 Global Server Hardware Security-Studie. Insgesamt verzeichnet die IBM Z nur 4,32 Sekunden nahezu unmerklicher monatlicher Ausfallzeit. Ebenso wichtig ist angesichts des anhaltenden Anstiegs von Sicherheitsangriffen und

Datenschutzverletzungen die überragende Sicherheit des IBM Z-Servers. Z registriert weiterhin den niedrigsten Prozentsatz (weniger als ein Prozent) erfolgreicher Datenschutzverletzungen von Januar bis Mitte Juni 2021. Darüber hinaus meldeten die Teilnehmer der IBM Z- und LinuxONE III-Umfrage auch die schnellste Mean Time to Detection (MTTD). 95 % der befragten ITIC-Unternehmen gaben an, dass ihre Sicherheits- und IT-Administratoren Hacker-Angriffe auf diesen Plattformen finden und abwenden konnten. Einzeln und zusammengenommen untermauern diese Ergebnisse den Erfolg der Z- und LinuxONE III-Angebote. Die Plattformen wurden auch durch die Übernahme von Red Hat durch IBM im Jahr 2019 gestärkt, was zu einem erheblichen Anstieg der Linux-Workloads auf den Z- und LinuxONE-Plattformen geführt hat. IBM-Führungskräfte erklärten öffentlich, die Firma habe einen 55 % igen Zuwachs an Linux-MIPS gesehen. Sie stellten auch fest, dass 92 von IBMs Top-100 Z-Kunden Linux-Workloads ausführen. Insgesamt kommt die Z-Plattform laut IBM durchschnittlich auf 100 bis 200 neue Implementierungen pro Jahr.

- **IBMs LinuxONE III** basiert auf der IBM Z-Plattform. Es richtet sich speziell an Hybrid-Cloud-Umgebungen und nutzt die Pervasive Encryption von Z. Die LinuxONE III Plattform und IBM z15 enthalten ebenfalls IBM Hyper Protect Data Controller, der transparenten, durchgängigen Zugriffsschutz und Geheimhaltung auf Datenebene bietet. Der IBM Hyper Protect Data Controller ermöglicht es Unternehmen, Daten zu verschlüsseln, Zugriff zu gewähren und zu entziehen und die Kontrolle zu bewahren – selbst wenn sie das System **verlassen.** Das Ergebnis: IBM LinuxONE III teilen sich die höchsten Sicherheits- und Zuverlässigkeits-Rankings im der ITIC-Befragung 2021; 95 % der LinuxONE III-Unternehmen erkennen Datenverletzungen „sofort oder innerhalb der ersten 10 Minuten“ des Angriffs und wehren diese ab.

- **IBM Power Systems** 92 % der IBM Power Systems-Kunden gaben an, dass ihre IT- und Sicherheitsadministratoren in der Lage waren, Angriffe „sofort oder innerhalb der ersten 10 Minuten“ einer Verletzung zu erkennen und zu verhindern. IBMs POWER9 Scale-out-Systeme sind seit drei Jahren auf dem Markt und die nächste Generation Power10-Server soll im Herbst 2021 verfügbar sein. IBM frischt die Produktlinie kontinuierlich auf und aktualisiert sie, mit besonderem Augenmerk auf Leistung, Unterstützung geschäftskritischer Workloads, Unterstützung intelligenter Analysen, speicherinterne Datenbanken und eingebettete Sicherheit. Alle Power Systems-Modelle sind cloudfähig. IBM Power Systems verfügen über integrierte Sicherheit auf allen Ebenen des Stacks – Prozessor, Systeme, Firmware, Betriebssystem und Hypervisor. Durch eine beschleunigte, im Chip integrierte Verschlüsselung werden Daten während der Übertragung und vor Ort geschützt. IBM gibt an, dass sein PowerVM Hypervisor keine bekannten Sicherheitsschwachstellen aufweist. POWER9-Server sind ebenfalls cloudfähig und schließen das integrierte PowerVM Virtualisierungs-Leistungsspektrum ein. Die POWER9 Scale-out-Server sind für die Integration in die Cloud und KI-Strategien von Unternehmen konzipiert. Dies bietet das hohe Leistungs- und RAS-Leistungsspektrum, das erforderlich ist, um geschäftskritische Workloads zu unterstützen, z. B. IBMs Db2- und Oracle-Datenbanken sowie SAP HANA. Power10 ist auf Energieeinsparungen und Erfolg in 7nm-Design ausgelegt. IBM schätzt, dass dies Verbesserungen von bis zu 3x größeren Prozessor-Energieeinsparungen, Arbeitslast-Kapazität, und Container-Dichte im Vergleich zu POWER9 darstellt. Darüber hinaus werden die kommenden Power10-Server eine Reihe fortschrittlicher Funktionen bieten, darunter die Unterstützung von Multi-Petabyte-Speicher-Clustern, die die Cloud-Kapazität zur Unterstützung speicherintensiver Arbeitslasten erweitern werden. Power10 wird auch über hardwareaktivierte Sicherheitsfunktionen verfügen, z. B. eine transparente Speicherverschlüsselung, für durchgängige Sicherheit. Der IBM Power10-Prozessor ist darauf ausgelegt, mit der vierfachen Anzahl von AES Verschlüsselungs-Engines pro Kern im Vergleich

zum IBM POWER9 einen deutlich schnelleren Verschlüsselungserfolg für die anspruchsvollsten heutigen und zukünftig zu erwartenden Standards zu erzielen, u. a. quantensichere Kryptografie und vollständig homomorphe Verschlüsselung. Neue funktionale Erweiterungen der Containersicherheit sind ebenfalls enthalten.

Highlights der Lenovo-Sicherheitsumfrage

- **Lenovo ThinkSystem**-Server erzielten die besten MTTD-Raten unter allen Intel x86-basierten Servern. 92 % der Umfrageteilnehmer gaben an, dass ihre IT- und Sicherheitsadministratoren versuchte Hacker-Angriffe und Datenschutzverletzungen unverzüglich oder innerhalb der ersten 10 Minuten des unbefugten Zugriffs erkannten und abschalteten. Dies ist kein Zufall. In den sieben Jahren seit der Übernahme von IBMs x86-basiertem Servergeschäft und den zehn Jahren seit der Übernahme von IBMs PC- und Notebook-Linie hat Lenovo die Sicherheit zu einer ersten Priorität gemacht. Infolgedessen sind Lenovo-Server und Desktops nach und nach immer stärker geworden, da die Firma kontinuierlich die Leistung, Zuverlässigkeit und Sicherheit der Server und ihrer Desktop-PCs und Laptops verbessert und verstärkt. Der technische Service und Support von Lenovo ist ebenfalls erstklassig. Lenovos ThinkSystem-Server zeigten kontinuierliche Verbesserungen in Bezug auf Zuverlässigkeit, mit einer bisher besten durchschnittlichen Verfügbarkeitszeit: 1,51 Minuten pro Server Ausfallzeit aufgrund von Hardware-Problemen. Wie IBM hat auch Lenovo eine ausgezeichnete und effektive taktische und strategische Sicherheitsstrategie aufgebaut und umgesetzt. 2018 stellte Lenovo die durchgängige Sicherheitstechnologie ThinkShield für seine PCs und Laptops vor. Die intelligente ThinkShield-Technologie hat Lenovo-PCs und -Servern in den letzten drei Jahren bei der Zunahme von Sicherheitsangriffen einen guten Dienst erwiesen. Während der weltweiten COVID-19-Pandemie, als viele Unternehmen auf ein Remote-Modell für Arbeitnehmer und Studenten gleichermaßen umstellten, hatten IT- und Sicherheitsadministratoren große Mühe, mit den Datenverletzungen Schritt zu halten. Lenovos ThinkShield-Sicherheitslösung bietet unerlässliche Unterstützung. ThinkShield ist zum Beispiel im ThinkSystem SE350 prominent vertreten. Dieses Modell ist Lenovos erster spezialisierter Edge-Server, der auf die Netzperipherie abzielt, um optimale Bandbreite zu liefern, Sicherheit zu stärken und Ausfallzeit zu reduzieren. ThinkSystem SE350 ist ein Server mit geringem Platzbedarf. Er ist 1,75 Zoll hoch, 8,1 Zoll breit und 14,9 Zoll tief und kann an einer Wand montiert, in einem Regal platziert oder in einem Rack installiert werden. ThinkSystem SE350 ist auch für leistungsfähige Server konzipiert. Er basiert auf Intels Xeon-D-Prozessor und ist mit 256GB RAM und 16TB internem Halbleiter-Speicher ausgestattet. ThinkSystem SE350 hat die physischen Sicherheitsmerkmale erweitert, z. B. eine Sperrung der Frontblende, Erkennung von Angriffen von außen, Manipulationserkennung und verschlüsselte Speicher. Er verfügt über eine Zero-Touch-Bereitstellungssoftware. Lenovos umfassende Strategie kombiniert Innovation mit zuverlässigen, flexiblen, und sicheren Rechenzentrensystemen. Dies ist ein geschickter Schachzug, der auch weitreichende Auswirkungen auf Lenovos Server, Netzwerke und letztlich seine unternehmensweiten Kunden hat. Menschliche Fehler sind der mit Abstand größte Verursacher von Serverausfallzeit. Endbenutzer gehören traditionell zu den schwächsten Gliedern in der umfassenden Sicherheitskette, insbesondere während der weltweiten COVID-19 Pandemie, bei der ein signifikanter Prozentsatz von Endbenutzern Telearbeit leistete und Schüler Fernunterricht absolvierten. Es macht für Lenovo Sinn, sowohl den Desktop als auch die Server zu sperren. Lenovo setzt strenge Sicherheitsstandards, Richtlinien und Verfahren in seinen

Fertigungsfunktionen und der weltweiten Logistikkette durch. Die Qualitätsingenieure von Lenovo halten das Prüfungsrecht der vertrauenswürdigen Lieferanten der Firma zu jeder Zeit aufrecht, wodurch die Firma noch mehr Kontrolle und Einsicht in die Sicherheit ihrer Gerätekomponenten erhält. ThinkShield bietet auch Sicherheit auf Gestaltungsebene. Dazu gehört das Schützen von BIOS und Firmware, sowie der Sichtschutz von Bildschirmen und Laptop-Kameraverschlüsse in seinen Geräten, um „visuelles Hacking" zu minimieren, wenn sich mobile Nutzer an öffentlich zugänglichen Orten aufhalten. ThinkShield wurde entwickelt, um die Identitäten und Berechtigungsnachweise der Benutzer zu schützen und bietet FIDO-zertifizierte Authentifikatoren und Integration mit Intel Authenticate (mit bis zu 7 Authentifizierungsfaktoren). ThinkShield verfügt außerdem über einen BIOS-basierten Smart-USB-Schutz, der die USB-Ports so konfiguriert, dass sie nur auf Tastaturen und Zeigegeräte reagieren. Lenovo betont auch, dass sich seine offenen Server-, Speicher-, Netzbetriebs- und Systemmanagement-Plattformen nahtlos in vorhandene und ältere Umgebungen integrieren. In persönlichen Interviews mit ITIC-Analysten nannten Lenovo-Kunden die einfache Durchführbarkeit der Bereitstellung und die einfache Durchführbarkeit der Integration sowie Abwärtskompatibilität als Plus für die zugrundeliegende Zuverlässigkeit und Stabilität der ThinkSystem-Plattform. Lenovo-Nutzer lobten auch die Kundendienstleistungen und den Support des Anbieters. Lenovos Systemdesign unterstützt unternehmenskritische Datenbanken, Unternehmensanwendungen, Big-Data-Analysen, sowie Cloud- und virtuelle Umgebungen. Beide Systeme vereinen zahlreiche fehlertolerante und hochverfügbare Funktionen in einem High-Density-, Rack-optimierten Paket, das den Platzbedarf minimiert und „massive Netzwerk-Computingaktivitäten" minimiert und die Wartung vereinfacht, da das System nie aus dem Rack entfernt werden muss. Im August 2020 stellte Lenovo mehrere neue Modelle seiner ThinkSystem Single-Socket-Server vor, die auf Advanced Micro Devices AMD EPYC 702 Serie Prozessoren basieren. Die neuen Erweiterungen des Lenovos Server-Portfolios sind speziell darauf ausgelegt, die zukünftigen, datenintensiven Workloads der Kunden wie Video-Sicherheit, softwaredefinierter Speicher und Netzermittlung zu bewältigen. Sie unterstützen auch virtuelle und Netzperipherie-Umgebungen, wo Sicherheit an erster Stelle steht. Das Ergebnis ist eine Lösung, die für Kunden, die Wert legen auf Durchlaufausgleich und Sicherheit bei leichter Skalierbarkeit. Lenovo erklärt, die beiden neuen ThinkSystem Server „stellen die Leistung eines Dual-Socket-Servers zum Preis eines Single-Socket-Servers zur Verfügung" und haben das Potenzial, die Softwarelizenzierungskosten der Kunden um bis zu 73 % und TCO um bis zu 46 % zu reduzieren.

Highlights der Cisco UCS-Sicherheitsumfrage

- **Ciscos Unified Computing System (UCS)** ist weiterhin gut im Rennen und konnte die 2,3 Minuten Ausfallzeit pro Server halten, die es erstmals in der ITIC-Umfrage 2020 Global Server Hardware, Server OS Mid-Year Update Survey erreichte. Von Januar bis Mitte Juni 2021 blieben die Server von Cisco konstant, bei einer Ausfallzeit von 2,3 Minuten pro Server. Dies ist eine beachtliche Leistung, wenn man bedenkt, dass viele Cisco UCS-Server an der Netzperipherie positioniert sind, die die erste Verteidigungslinie gegen Sicherheitsangriffe darstellt. Dennoch gaben 87 % der Teilnehmer der Cisco UCS-Umfrage an, dass sie in der Lage waren, Sicherheitshacks unverzüglich oder innerhalb der ersten 10 Minuten zu finden, zu isolieren und abzuwehren. Die Teilnehmer der Cisco UCS-Umfrage berichteten außerdem, dass ihre Server in den letzten 18 Monaten jeweils sieben (7) erfolgreiche Sicherheitsangriffe erlebt haben. Als

Reaktion auf die zunehmenden Datenschutzverletzungen, hat Cisco mit der Veröffentlichung des Cisco UCS Hardening Guide begonnen. Das Dokument ist zum kostenlosen Download verfügbar. Es enthält detaillierte Informationen, um Anwendern zu helfen, die Geräte der Cisco UCS-Plattform zu schützen und die Netzsicherheit zu verbessern. Gegliedert um die drei Ebenen, nach denen die Funktionen einer Netzeinheit kategorisiert werden, bietet dieses Dokument einen Überblick über jede Cisco UCS Softwarefunktion und verweist auf Referenzliteratur. Zusätzlich hat Cisco eine Reihe von Management- und Leistungs-Upgrades eingeführt, die darauf abzielen, TCO zu verbessern und die Installation und Bereitstellung zu beschleunigen. Cisco erklärt, dass sein UCS eine Verkleinerung von 86 %in der Verkabelung ermöglicht und in nur wenigen Minuten (statt Tagen oder Wochen) eingerichtet werden kann, während die Ausgaben um mehr als 40 % reduziert werden. Die Hersteller versichern den Anwendern eine hundertprozentige Kompatibilität zwischen und unter den Komponenten. Und der Lastausgleich ist kein Thema.

Highlights der HPE-Sicherheitsumfrage

- **HPEs Superdome** Server-Linie (einschließlich der Modelle Integrity und Flex) weisen ebenfalls eine hohe Zuverlässigkeit von fünf und sechs Neunen für 92 % seiner Kunden auf. Und 89 % der Befragten der HPE-Umfrage gaben an, dass ihre Unternehmen Sicherheitsverletzungen „sofort oder innerhalb der ersten 10 Minuten“ entdecken und abwehren. Die ITIC-Umfragedaten zeigen, dass HPE Superdome Server jeweils drei (3) erfolgreiche Sicherheitshacks innerhalb der letzten 18 Monate erlebt haben. Damit gehören die HPE-Hardware-Plattformen zu den Top-Five der am besten geschützten Systemen. Das Superdome-Portfolio profitiert auch von der inhärent starken Stabilität der HPE-Hardware. HPE hat Sicherheit, Funktionen/Leistungsinnovation und technischen Service und Support zu seinen Top-Prioritäten gemacht. All dies ist im zunehmend unsicheren, komplexen und vernetzten digitalen Zeitalter von hoher Bedeutung. HPE ist in unternehmensweiten Unternehmen, von KMUs bis hin zu den größten multinationalen Unternehmen, fest verankert. Der HPE Superdome Flex Server verfügt über RAS-Fähigkeiten und durchgängige Sicherheit, um notwendige Workloads zu schützen. So bietet zum Beispiel der HPE Superdome Flex Server eine Skalierbarkeit von bis zu 32 Sockets. Dies entspricht der 2,3-fachen Skalierbarkeit früherer Server. Außerdem verfügt er über ein speicherinternes Design und eine Speicherkapazität von 768 GB - 48 Terabyte auf einer einzelnen Plattform. HPE Superdome Flex Server hat einen modularen Aufbau, der flexibel von 4 bis 32 Sockets in 4-Socket-Schritten skaliert. HPE sagt auch, dass der Superdome Flex Server mit 4 Sockets einen kosteneffizienteren Eingangspunkt für unternehmenskritische Workloads hat, er liefert bis zu 45 % niedrigere Anschaffungskosten im Vergleich zu Vorgänger-Modellen. HPE hebt ebenfalls die Zuverlässigkeit hervor und verweist auf die fünf Neunen der eingebetteten RAS-Fähigkeiten des Superdome Flex Servers (99,999 %) der Einzelsystem-Verfügbarkeit. HPE erklärt auch, dass der Superdome Flex Server über seine prädiktive Fehlerbehandlung seitens der Error Analysis Engine menschliches Versagen reduziert. Sicherheit und menschliches Versagen sind zwei Themen, die eng miteinander verbunden sind und die Sicherheit und Zuverlässigkeit untergraben. Diese Engine prognostiziert Hardware-Fehler und initiiert automatische Fehlerbehebung ohne manuellen Eingriff oder „Hilfe seitens des Betreibers". Mit dem „Firmware First“-Ansatz von HPE dämmt sie Fehler an der Firmware ein, einschließlich Speicherfehler, bevor eine Unterbrechung an der Betriebssystemschicht auftreten kann. HPE bietet auch Stabilität für Linux-Workloads mit seiner HPE Serviceguard for Linux (SGLX) mit hoher Verfügbarkeit und Notfallwiederherstellung Clustering-Lösung. Dies ermöglicht Unternehmen, ihre unter Linux

laufenden Server gegen eine Vielzahl von Infrastruktur- und Anwendungsfehlern in horizontalen physischen oder virtuellen Umgebungen aus jeder Entfernung abzusichern.

Highlights der Huawei-Sicherheitsumfrage

- In den letzten fünf Jahren hat sich Huawei, mit Hauptsitz in Shenzhen, China, zu einem der weltweiten Top-Five der Server-Hardwareanbieter entwickelt, mit seinen geschäftskritischen KundLun-Servern und seinen allgemeinen FusionServer x 86-basierten Servern. Basierend auf der Umfrage von ITIC aus dem Jahr 2021 (Global Server Hardware, Server OS Reliability) und der ITIC-Umfrage aus dem Jahr 2021 (Global Server Hardware Security), gehören die Server Huawei KunLun und Fusion ebenfalls zu den besten 3 Hardware-Plattformen in Bezug auf Zuverlässigkeit und Sicherheit. 91 % der Teilnehmer an der Huawei-Umfrage gaben an, dass ihre IT- und Sicherheitsadministratoren versuchte Sicherheitsverletzungen „sofort oder in weniger als 10 Minuten“ erkennen und abwehren. Die Befragten der Huawei-Umfrage gaben an, dass die KunLun- und Fusion-Server in den letzten 18 Monaten jeweils 1,5 Mal gehackt wurden. Seit 2015 hat Huawei die fortschrittlichen Funktionen, die inhärente Sicherheit und Gesamtleistung seiner Server verstärkt. Um erfolgreich mit Konkurrenten wie Cisco, Fujitsu, HPE, IBM, Inspur, Lenovo und anderen zu konkurrieren, umfasst Huaweis Server-Produktfamilie allgemeine Rack-Server und Blade-Server sowie geschäftskritische Hardware für Hochleistungsrechner (High Performance Computing, HPC). Huawei hat seine Server auch mit intelligenten Fähigkeiten ausgestattet, um neu entstehende rechenintensive Anwendungen zu unterstützen, z. B. KI, Big Data-Analytik, Deep Learning und maschinelles Lernen. Huawei unterstreicht die Sicherheit durch Best-Practice-Dokumente zum Thema „Einrichten proaktiver Abwehrsysteme" über seine HiSec-Lösung, die eine intelligentere Erkennung von Bedrohungen, Bedrohungsintervention, Sicherheitsoperationen und Wartung ermöglicht. Laut Huawei verbessert HiSec die Bedrohungspräventionsfähigkeiten von Unternehmensnetzwerken und der Telekommunikations-Infrastruktur und erhöhe so die Sicherheit und O&M-Effizienz und reduziere O&M-Kosten. Außerdem bietet Huawei mehrere neue Sicherheitsangebote für seine verschiedenen Serverlösungen im Rechenzentrum, der Cloud und dem Netzwerk.

Schlussfolgerungen

Sicherheit ist das größte Problem für die Zuverlässigkeit und Verfügbarkeit von Server-Hardware, Server-Betriebssystemen und geschäftskritische Anwendungen. Alle Unternehmen sollten Sicherheit zu einer Priorität machen und eng mit ihren Anbietern zusammenarbeiten, um Sicherheitsrisiken auf ein zulässiges Maß zu reduzieren.

Jede zusätzliche Sekunde und Minute an Serverausfallzeit und Nichtverfügbarkeit von Anwendungen wirkt sich negativ auf Geschäftsoperationen, Mitarbeiterproduktivität und Umsatz aus.

Die Ergebnisse der ITIC-Umfrage 2021 zur Zuverlässigkeit von Server-Hardware und Server-Betriebssystemen (Global Server Hardware and Server OS Reliability) zeigen, dass IBM Z Mainframe, IBM Power Systems, dicht gefolgt von den Servern Lenovo ThinkSystem, Huawei KunLun und HPE Integrity Superdome ihren Status als zuverlässigste Server-Hardware weiter festigen und verbessern.

Die IBM Z Unternehmensplattform ist die einzige, die eine fehlertolerante Zuverlässigkeit von sechs und sieben Neunen bietet: 99,9999 und 99,99999 % Zuverlässigkeit für mehr als 93 % ihrer Unternehmensnutzer. Mit Ausnahme von Supercomputern und Hardware mit hoher Verfügbarkeit (High Availability, HA) gibt es keine Serverplattformen, die auch nur annähernd mit den Ergebnissen von Z in Bezug auf Zuverlässigkeit, Verfügbarkeit und nahezu lückenloser Verfügbarkeitszeit und Sicherheit vergleichbar sind.

Neun von zehn Umfrageteilnehmern bestätigten, dass die Lösungen von IBM Power Systems und Lenovo ThinkSystem sowohl fünf als auch die gepriesenen sechs Neunen (99,999 % und 99,9999 %) in Bezug auf Zuverlässigkeit und Verfügbarkeit verzeichnen. Die Plattformen von IBM Power Systems und Lenovo ThinkSystem sind bis zu 30x zuverlässiger und bis zu 36x kosteneffektiver und wirtschaftlicher als die leistungsschwächsten markenlosen White-Box-Server.

Ein weiterer bemerkenswerter Erfolg ist, dass IBM und Lenovo in den Kategorien Zuverlässigkeit und Verfügbarkeit den ersten oder zweiten Platz belegten oder in den Metriken Verfügbarkeitszeit, Sicherheit oder Verwaltbarkeit den ersten oder zweiten Platz belegten.

Verlässlichkeit ist fliessend, nicht statisch. Kein Server, kein Einzelteil – Festplatte, Speicher oder CPU; Betriebssystem; Anwendung, Gerät oder Konnektivitätsmechanismus ist immun gegen inhärente Probleme oder Ausfälle.

Server sind das Fundament, auf dem die gesamte Netzinfrastruktur und das erweiterte direkte Geschäftsumfeld des Netzes ruhen. Wenn Server ausfallen, wird der Datenzugriff verweigert. Das Geschäft wird unterbrochen. Die Produktivität lässt nach. Das Einkommen leidet. Rund 88 % aller Unternehmen benötigen heute eine Mindestzuverlässigkeit von 99,99 % für ihre Server-Hardware, Betriebssystemen und Hauptgeschäftsanwendungen, um die Produktivität sicherzustellen und einen ununterbrochenen Datenzugriff zu liefern. Hohe Zuverlässigkeit und Verfügbarkeit sichert auch die täglichen Unternehmensaktivitäten, Datenressourcen und geistiges Eigentum (IP), Personaldaten der Mitarbeiter, Geschäftsprozesse und Einnahmenstrom.

Im Jahr 2021 und darüber hinaus stellen Sicherheit, menschliches Versagen und Endnutzer die größten Bedrohungen dar, die die Zuverlässigkeit und Verfügbarkeit von Servern, Betriebssystemen und Anwendungen untergraben können.

Niemand weiß, wie lange die weltweite COVID-19 Pandemie andauern wird. Und selbst wenn die Pandemie offiziell für beendet erklärt wird, werden ihre negativen Auswirkungen wahrscheinlich noch jahrelang bestehen, insbesondere im Hinblick auf die Bedrohungen für Sicherheit und Datenschutzverletzung.

Das ist die neue Normalität: Organisierte Hacker sind auf dem Vormarsch. Sie werden diese Pandemie weiter nutzen, um Sicherheitslücken auszunutzen. Hacker werden weiterhin jede Gelegenheit nutzen, um aus Unternehmens- und Mitarbeiterdaten-Assets Nutzen zu ziehen.

Server-Zuverlässigkeit, unterbrechungsfreier Zugriff auf Daten und Anwendungen und Sicherheit sind immer unerlässlich – insbesondere in der COVID-19-Epoche mit Telearbeit und Fernunterricht. Jede zusätzliche Sekunde und Minute an Serverausfallzeit und Nichtverfügbarkeit von Anwendungen wirkt sich negativ auf Geschäftsoperationen, Mitarbeiterproduktivität und Umsatz aus.

Ein signifikanter Teil der Unternehmensserver und Anwendungen befinden sich mittlerweile in virtualisierten Cloud-Umgebungen und an der Netzperipherie. Seit Beginn der Pandemie vor mehr als 18 Monaten haben viele Unternehmen ihre Mitarbeiter auf Telearbeit umgestellt; auch Schulen und Universitäten haben sich dem Fernunterricht angeschlossen. Dies stellt Organisationen und überforderte IT- und Sicherheitsadministratoren unter größeren Druck, Verfügbarkeitszeit und Verfügbarkeit aller Datenressourcen sicherzustellen.

Sicherheit ist extrem wichtig. Anbieter müssen weiter an integrierter Server-Sicherheit feilen; schnell Fixes und Patches anbieten, wenn Schwachstellen gefunden werden und mit Kunden zusammenarbeiten, um präskriptive Anleitungen zur Verfügung zu stellen. Unternehmen müssen auch Verantwortung übernehmen, um die Zuverlässigkeit und Sicherheit der gesamten Server- und Netzinfrastruktur und wichtiger Geschäftsanwendungen in Rechenzentren und der Cloud sicherzustellen. Es ist wichtig, dass Unternehmen strenge Sicherheitsrichtlinien und Verfahren für **alle Mitarbeiter,** insbesondere Telearbeiter und Studenten, implementieren und umsetzen. Verlässlichkeit und Sicherheit sind Kernbestandteile der Netzinfrastruktur. Beides ist notwendig, um ununterbrochene tägliche Unternehmensaktivitäten sicherzustellen, Datenzugriff zu schützen und den Einnahmenstrom zu sichern.

Die ITIC 2021 Global Server Hardware, Server OS Security-Umfrage unterstreicht die Notwendigkeit für **alle** Organisationen, ungeachtet der Größe und vertikaler Branche, proaktiv und kontinuierlich danach zu streben, das wachsende Spektrum von zunehmend ausgereiften und zielgruppenspezifischen Cyberattacken aufzudecken und zu verhindern.

Das bedeutet, dass alle geeigneten Sicherheitsmaßnahmen durchgeführt werden müssen. Der Erlass und die Durchsetzung von strengen IT-Sicherheitsrichtlinien und Verfahren für **alle Mitarbeiter der Firma**, von Chefetage-Führungskräften bis zu Firmenvertragsarbeitern und Praktikanten, ist zwingend erforderlich. Unternehmen müssen angemessene Budgets für den Kauf von Sicherheitsprodukten reservieren und die nötige Zeit und entsprechende interne und externe Drittpartei-Ressourcen zur Verfügung stellen, um Endnutzern und IT-Administratoren sowie Sicherheitsexperten Sicherheits-Tools und Sicherheitsschulungen bereitzustellen.

Eine hundertprozentige Sicherheit existiert nicht. Doch mehrschichtige Sicherheitsabwehr, gestärkt durch Anfälligkeitstests und Sicherheitsbewusstseinstraining, können die Zahl der Datenschutzverletzungen und Ransomware-Hacks verhindern und das Risiko auf ein annehmbares Niveau reduzieren.

Geschäftskritische Systeme von Cisco, HPE und Huawei haben sich ebenfalls hervorragend geschlagen und in den vergangenen 18 Monaten seit dem Ausbruch der COVID-19-Weltpandemie keine Einbußen in Bezug auf Zuverlässigkeit erfahren. Die Cisco-, HPE- und Huawei-Server haben aufgrund der inhärenten Zuverlässigkeit der Kern-Hardware nahezu die gleiche Zuverlässigkeit wie IBM und Lenovo erreicht.

Ciscos UCS-Server haben den Zuverlässigkeits-Zuwachs in ITICs neuestem 2021 Global Server Hardware, Server OS Reliability Survey Mid-Year-Update gehalten. Seit 2019 sind die von Cisco UCS

Server-Shops gemeldeten Ausfallzeiten von knapp über vier (4,1) Minuten im der vorherigen ITIC-Umfrage zur Zuverlässigkeit auf knapp über zwei (2,3) Minuten pro Server/pro Jahr gesunken, was auf Hardwarefehler zurückzuführen ist. Das ist wichtig. Ein signifikanter Teil von Ciscos UCS-Servern wird an der Netzperipherie implementiert – lange Zeit galt dieser als einer der anfälligsten Punkte des direkten Geschäftsumfeldes.

Kein Softwareanbieter kann sich auf seinen Lorbeeren ausruhen. Der Wettbewerb im weltweiten Server-Hardware-Vertrieb ist intensiv. Es ist und bleibt ein Käufergeschäft. Während viele Unternehmen, insbesondere KMUs, ihre Kaufentscheidungen auf Basis des Preises treffen, wählt ein erheblicher Teil der Unternehmen stabilere Hardware, ausgestattet mit eingebetteter Sicherheit, intelligentem Management, KI und Big-Data-Analysefunktionalität.

Die Umfragedaten zeigen, dass Unternehmen extrem hohen Wert auf technischen Service und Support legen. Die Unternehmen verlangen von den Anbietern, dass sie schnell handeln, wenn Probleme auftreten. Anbieter sollten Kunden realistische Empfehlungen und präskriptive Anleitungen für Systemkonfigurationen und Produktlebenszyklen zur Verfügung stellen, um optimale Leistung und Verfügbarkeit zu erreichen und zu verwalten.

Wie immer hält ITIC fest, dass die Anbieter auch die Zuständigkeit tragen, Patches, Fixes und Updates zeitnah zu liefern und die Kunden nach bestem Wissen und Gewissen über alle bekannten Inkompatibilitätsprobleme zu informieren, die sich möglicherweise auf die Leistung auswirken könnten. Verkäufer sollten auch ehrlich mit Kunden sein und sie über Probleme oder Verzögerungen bei der Lieferung von Ersatzteilen benachrichtigen.

Empfehlungen

Keine Serverplattform, kein Server-Betriebssystem und keine Geschäftsanwendung wird absolute Sicherheit bieten. Allerdings stellen IBM, Lenovo, Huawei, HPE und Cisco, die zu den zuverlässigsten Serverplattformen gehören, auch die größten Niveaus an inhärenter Sicherheit zur Verfügung. Dies ermöglicht Kunden, die größten Skaleneffekte zu erzielen und ihre sensiblen IP- und Datenressourcen abzusichern. Sicherheit ist eine 50/50-Aussage. Während Anbieter ein hohes Sicherheitsniveau liefern müssen, sind Unternehmen für die Aufrechterhaltung der Zuverlässigkeit ihrer Server und umfassenden Netzinfrastruktur verantwortlich. ITIC rät den Unternehmen dringend:

- **Inventur zu machen.** Zu wissen, was sich in Ihrem Netz befindet. Dies bedeutet, dass ***alle*** Server, geschäftskritische Anwendungen; Netzgeräte (Firewalls, Router) im gesamten direkten Geschäftsumfeld, einschließlich des Rechenzentrums, remote angeschlossenen Büros, öffentlichen, privaten und hybriden Clouds, IoT-Geräte und die Netzperipherie, katalogisiert werden sollten.
- **Angemessene Server-Hardware**. Die Server-Hardware muss stabil genug sein, um sowohl die aktuelle Arbeitslast als auch die zu erwartenden höheren Arbeitslasten und größeren Anwendungen zu bewältigen.

- **Regelmäßiges Austauschen, Anpassen und Aktualisieren der Server-Hardware.** Dies bedeutet, notwendige Patches, Updates und Sicherheitsfixes ***nach Bedarf*** auf dem Laufenden zu halten, um den Systemzustand zu bewahren und eine hohe Systemleistung zu erreichen.
- **Software zu aktualisieren.** Wann immer möglich, bleiben Sie niemals hinter mehr als zwei Revisionen der Server-Betriebssysteme und wichtigen serverbasierten Anwendungen zurück.
- **Umsetzung strenger Sicherheitsrichtlinien und -verfahren.** Es ist zwingend erforderlich, dass Unternehmen aller Größen und Branchen unternehmensweite Sicherheitsrichtlinien und Verfahren festlegen. Verteilen Sie sie in Papierform und per E-Mail an alle Mitarbeiter. Die IT-Sicherheitsrichtlinien sollten ein integraler Bestandteil der gesamten unternehmensweiten Richtlinien sein und bestimmte Bestimmungen und Sanktionen für erste, zweite und dritte Verstöße enthalten. Den Unternehmen wird auch empfohlen, alle Mitarbeiter verbindlich an einem IT-Sicherheitstraining teilnehmen zu lassen, ähnlich der Schulung bezüglich sexueller Belästigung.
- **Service Level Agreements (SLAs) genau zu überwachen.** Achten Sie genau auf SLA-Verträge, um sicherzustellen, dass die Hardware-, Software- und Cloud-Anbieter Ihres Unternehmens die Bedingungen der SLAs erfüllen oder überschreiten, um die vereinbarten Zuverlässigkeitsstufen zu liefern.
- **Durchführung von Sicherheitslücken-Tests.** Angesichts der anhaltenden Steigerung aller Arten von Sicherheitshacks und Datenschutzverletzungen, z. B. Ransomware, Phishing-Attacken und CEO-Betrug, um nur einige zu nennen, sollten alle Unternehmen mindestens einmal im Jahr und bei Bedarf Anfälligkeitstests durchführen. ITIC empfiehlt, dass Unternehmen mit unabhängigen Drittpartei-Fachleuten arbeiten.
- **Erstellen eines Governance- und Korrekturplan.** Geben Sie eine Korrektur- und Governance-Planung in Auftrag, sollte Ihre Firma erfolgreich gehackt worden sein. Bestimmen Sie eine Hierarchie der Verantwortlichen im Fall von Datenschutzverletzungen oder eines Netzausfalls. Die Governance- und Korrekturplanung sollte auch bestimmten Gruppen und Einzelpersonen bestimmte Aufgaben zuweisen. Stellen Sie sicher, dass die Planung auch die relevanten Kontaktinformationen für alle Anbieter und Drittpartei-Dienstleister enthält.
- **Sicherheits- und IT-Administratoren zu schulen und zu zertifizieren.** Stellen Sie sicher, dass Sicherheits- und IT-Fachleute eine angemessene Ausbildung erhalten und über die erforderlichen Sicherheitszertifizierungen verfügen.
- **Schulung der Endbenutzer.** Stellen Sie sicher, dass sowohl Endnutzer als auch Vertragsarbeiter und vorläufig Beschäftigte ein angemessenes Sicherheitsbewusstseinstraining bezüglich der neuesten E-Mail- und Phishing-Betrügereien und Ransomware-Bedrohungen erhalten.

Methodik

Die ITIC-Umfrage 2021 *Global Server Hardware Security Reliability* befragte von Januar 2021 bis Mitte Juni 2021 Führungskräfte und IT-Manager in über tausend Unternehmen weltweit. Die unabhängige webbasierte Umfrage umfasste Multiple-Choice-Fragen und eine Textfrage. Um objektiv zu bleiben akzeptierte ITIC kein Sponsoring von Softwareanbietern. Kein Teilnehmer der Umfrage erhielt eine Vergütung. Die ITIC-Analysten führten auch zwei Dutzend persönliche Kundeninterviews durch, um wertvolle anekdotische Daten anzufordern und tiefere Einblicke und kontextuelles Wissen über die Auswirkungen von Sicherheitslücken und Datenverletzungen auf die Zuverlässigkeit der Unternehmensserver und Netzinfrastruktur zu gewinnen. Zu den Befragten gehörten Führungskräfte, IT- und Sicherheitsadministratoren sowie Endnutzer. ITIC setzte Authentifizierungs- und Protokollierungsmechanismen ein, um Verfälschung zu verhindern und mehrere Antworten desselben Befragten zu verhindern.

Demografische Daten der Umfrage

ITIC befragte für die Studie 1.100 Unternehmen aller Größen aus 28 vertikalen Märkten. Unternehmen aller Größen waren repräsentativ vertreten. Die Befragten stammten aus kleinen und mittleren Unternehmen (KMU) mit weniger als 50 Beschäftigten bis hin zu multinationalen Unternehmen mit mehr als 100.000 Mitarbeitern.

Alle Marktsektoren waren gleichermaßen vertreten: KMUs mit einem bis 100 Mitarbeitern machten 24 % der Befragten aus. Kleine und mittelständische Unternehmen (KMUs) mit 101 bis 1.000 Beschäftigten machten 28 % der Teilnehmer aus. Die restlichen 43 % der Befragten kamen aus großen Unternehmen mit 1.001 bis über 100.000 Beschäftigten. Die Befragten stammten aus 49 verschiedenen vertikalen Märkten. Etwa 61 % der Befragten kamen aus Nordamerika; 39 % waren internationale Kunden, die aus 22 Ländern europaweit, Asien, Australien, Neuseeland, Mittel-/Südamerika und Afrika stammten.

Anhänge

Dieser Abschnitt enthält Links zu den verschiedenen ITIC-Statistiken und Erhebungen, die in diesem Bericht zitiert werden.

ITIC-Website und Links zu Umfragedaten und Blogbeiträgen:

https://itic-corp.com/Blog/2019/11/ibm-lenovo-hpe-and-huawei-servers-maintain-top-reliability-rankings-cisco-makes-big-gains-ibm-lenovo-hardware-up-to-24x-more-reliable-28x-more-economical-vs-least-reliable-white-box-servers/

https://itic-corp.com/Blog/2019/11/1678/

https://itic-corp.com/Blog/2019/08/itic-poll-human-error-and-security-are-top-issues-negatively-impacting-reliability/

https://itic-corp.com/Blog/2019/08/itic-2019-server-reliability-mid-year-update-ibm-z-ibm-power-lenovo-system-x-hpe-integrity-superdome-huawei-kunlun-deliver-highest-uptime/

http://itic-corp.com/Blog/2017/07/ibm-z14-mainframe-advances-security-reliability-processing-power/

http://itic-corp.com/Blog/2017/06/ibm-lenovo-servers-deliver-top-reliability-cisco-ucs-hpe-integrity-gain/