Security für moderne Rechenzentren

Von Dr. Larry Ponemon, Vorsitzender und Gründer des Ponemon Institute

Unternehmen sind einer Vielzahl von Cyber-Bedrohungen ausgesetzt. Nach Studien des Ponemon Institute erschweren Angriffsformen wie Exploits von Software- und Anwendungsschwachstellen, Malware, Spear Phishing, Ransomware, DDoS-Angriffe und webbasierte Schadsoftware den Schutz von Rechenzentren. Besonders klassische Rechenzentren haben mit Problemen zu kämpfen, die auf diese Bedrohungen zurückgehen.

Aktuelle Studien zeigen, dass sich die Bedrohungslage nicht gebessert hat. Stattdessen sind neue Bedrohungen wie Cyber-Erpressung, kriminelle Malware und Ransomware hinzukommen, die Unternehmen noch höheren Risiken aussetzen. Die Mehrheit der in unseren zahlreichen Studien untersuchten Unternehmen berichtete von einer Datenpanne, die zum Verlust oder Diebstahl von mehr als 1000 Datensätzen mit sensiblen oder vertraulichen Kunden- oder Geschäftsinformationen führte, sowie von mindestens zwei Datenschutzverletzungen im gleichen Zeitraum. Die finanziellen Folgen können verheerend sein: Nach unserer Untersuchung *2020 Cost of Data Breach* zu den Kosten von Sicherheitsverletzungen kann eine Datenpanne im Durchschnitt mit umgerechnet 3,4 Millionen € zu Buche schlagen.

Warum ist die Sicherheit von Rechenzentren wichtig? In Rechenzentren befindet sich wichtigstes Unternehmenskapital – wie geschäftskritische Anwendungen, geistiges Eigentum, Geschäftsinformationen und Kundendaten. Das allein macht ein Rechenzentrum interessant für Kriminelle. Aber neben dem Abgreifen von Daten wollen Kriminelle dem Unternehmen auch ernsten Schaden durch Performance-Einbußen, Ausfallzeiten und das Aufweichen der allgemeinen physischen Sicherheit zufügen. Wie unsere Studie zeigt, führen Cyber-Sicherheitsvorfälle in Unternehmen zur erheblichen Störung der IT- und Geschäftsprozesse. Verfügt ein Rechenzentrum jedoch über ein starkes Sicherheitsprofil, ist der Netzwerk-Verkehr weniger anfällig für kriminelle Eindringlinge und deren Manipulationen.

In den letzten fünf Jahren haben sich Rechenzentrumsumgebungen stark verändert. Das zeigt sich z. B. in der zunehmenden Umstellung von klassischen auf hybride Rechenzentren oder in der Skalierung zu unternehmenseigenen Hyperscale-Rechenzentren. Letztere umfassen in der Regel Drittlösungen wie AWS, Microsoft, Google und Apple und werden vor allem von Großunternehmen mit riesigen Kundenstämmen wie in der Finanzbranche oder im Gesundheitswesen eingesetzt.

Hyperscale-Rechenzentren bieten einzelnen Anwendern und Unternehmen hochskalierbare Anwendungen, Speicher- und Datenbankdienste, sind jedoch unter Sicherheitsaspekten nicht unproblematisch. Besonders bei steigenden Geschäftsanforderungen wird schnell die Sicherheit geopfert, um die Nutzererfahrung nicht zu beeinträchtigen. Das liegt daran, dass nur wenige Security-Geräte auf dem Markt die notwendige Schnelligkeit bieten. Das Fehlen einer ausreichenden Sicherheit führt jedoch zu zahlreichen Problemen, die von illegitimem Web-Traffic bis hin zu DDoS-Angriffen (Distributed Denial of Service) reichen.

Ein hybrides Rechenzentrum ist eine Computer-Umgebung, die On-Premises-Rechenzentren und Co-Locations kombiniert und sich auf mehrere Clouds erstreckt. Angesichts weltweit steigender Traffic-Volumen in Rechenzentren kann sich ein Unternehmen mit einer Hybrid-Infrastruktur besser auf schwankende Verkehrsaufkommen einstellen und Kapazitäten bei Bedarf bereitstellen.

Problematisch ist nur, dass eine Hybrid-Cloud-Umgebung zu Lasten der Transparenz geht: Es gibt mehr „tote Winkel“, eine höhere Komplexität und zunehmende externe Risiken durch Angreifer, die Schwachstellen ausnutzen und Datenpannen verursachen können.

Früher wurde der Netzwerk-Traffic im Rechenzentrum als vertikal oder Nord-Süd-Datenverkehr betrachtet, um den Traffic zwischen Clients und Servern zwischen dem Rechenzentrum und einem externen Standort außerhalb des Rechenzentrum-Netzwerks zu beschreiben. Heutzutage können sich Daten aber auch seitlich innerhalb des Rechenzentrums bewegen, was als Ost-West-Datenverkehr bezeichnet wird. Damit fließt der Datenverkehr jetzt im Rechenzentrum in zwei Richtungen: zwischen Nord und Süd sowie zwischen Ost und West.

Die Migration in die Cloud und die digitale Transformation erhöhen den Bedarf an hochsicheren Rechenzentren.

Ob hybrides Rechenzentrum oder Hyperscale-Datacenter: In den meisten Unternehmen herrscht kein Vertrauen in das Security-Management. Auch fehlt es an Transparenz und einer klaren Abgrenzung der Zuständigkeiten bei Sicherheitsfragen.

- **Durch die Migration in die Cloud sind kritische Daten im Rechenzentrum einem größeren Risiko ausgesetzt.** Trotz großer Hoffnungen in Cloud-Implementierungen, wenn es um das Erreichen von Geschäftszielen geht, bezweifelte fast die Hälfte der Teilnehmer bei einer Studie des Ponemon Institute,[1] dass ihre Rechenzentren derzeit die eigenen Anforderungen an den Datenschutz und die Sicherheit von Daten erfüllen. Tatsächlich verhalten sich Unternehmen beim Schutz des sensiblen Datenverkehrs in einer hybriden Rechenzentrumsumgebung reaktiv statt proaktiv: Nur 44 % der Befragten überprüften cloudbasierte Software oder Plattformen in Rechenzentren auf Risiken für die Datensicherheit – und nur 39 % gaben an, dass im Unternehmen festgelegt wird, welche Informationen zu sensibel sind, um in der Cloud gespeichert zu werden.

- **Mangelnde Transparenz über den Netzwerk-Traffic im Rechenzentrum gefährdet kritische Daten, die in der Cloud gesammelt, verarbeitet und gespeichert werden.** Nur 29 % der Befragten gaben an, dass ihr Unternehmen über die erforderliche 360-Grad-Sichtbarkeit der in der Cloud gesammelten, verarbeiteten und/oder gespeicherten kritischen Daten verfügt. Auch herrscht Unsicherheit in Unternehmen, ob man wirklich alle implementierten Cloud-Anwendungen und Cloud-Plattformen kennt, die man selbst implementiert hat.

- **Die digitale Transformation erhöht das Risiko eines Security-Exploits im Rechenzentrum.** Laut einer aktuellen Studie des Ponemon Institute[2] sind sich die IT-Security-Experten einig: Wettbewerbsfähigkeit und das Erreichen von Geschäftszielen hängen von der digitalen Wirtschaft ab. Um jedoch in diesem neuen Geschäftsumfeld erfolgreich zu bestehen, müssen Unternehmen in der Lage sein, während der digitalen Transformation und in dadurch entstehenden neuen Umgebungen ihre Daten zu schützen.

- **Komplexe, intransparente Geschäftsprozesse, zu geringe Sichtbarkeit von Personen und mangelnde interne Fachkenntnisse sind die Haupthindernisse für einen sicheren digitalen Transformationsprozess:** Die Komplexität von Geschäftsprozessen muss überwunden werden, um einen sicheren digitalen Transformationsprozess zu erreichen. Unternehmen müssen sich auch mit der unzureichenden Sichtbarkeit von Personen und Geschäftsprozessen sowie dem Mangel an qualifiziertem oder fachkundigem Personal befassen, um kritische Daten im Rechenzentrum zu schützen.

---

1 *Data Protection and Privacy Compliance in the Cloud: Privacy Concerns Are Not Slowing the Adoption of Cloud Services, but Challenges Remain.* Unabhängige Studie des Ponemon Institute im Auftrag von Microsoft, Januar 2020.

2 *Bridging the Digital Transformation Divide: Leaders Must Balance Risk & Growth.* Unabhängige Studie des Ponemon Institute im Auftrag von IBM Security, März 2018.

- **Zunahme verschlüsselter Daten:** Unternehmen schützen sensible und vertrauliche Daten während der Übertragung durch Verschlüsselung. Ob Daten korrupt sind, lässt sich aber nur schwer feststellen. Ohne den richtigen Schlüssel zur Dechiffrierung bleibt die Entschlüsselung der Daten ein mühsamer Prozess.

- **Sicherheitslücken in flachen Netzwerken:** Flache Netzwerk-Topologien entstehen bei herkömmlichen Tiered-Netzwerken, die auf Routern und Switches basieren und keine Sicherheitsüberprüfung und -durchsetzung haben. „Flach" bedeutet, dass es innerhalb des Netzwerks keine herkömmlichen Sicherheitstechnologien wie Firewalls, Filter oder andere Security-Appliances gibt. Diese Entwicklung führt – besonders in Kombination mit dem impliziten Vertrauen, das allen internen Benutzern gewährt wird – zu sehr hohen internen Risiken. Durchbricht beispielsweise ein Angreifer den Netzwerk-Perimeter, kann er unbemerkt im Netzwerk bleiben und sich erst später quer durch das Netzwerk bewegen.

Security für moderne Rechenzentren

Neben der Sicherheit hat die Verfügbarkeit in der Regel höchste Priorität. Zu den Best Practices gehören auch ausreichende verfügbare Ressourcen, um Rechenzentren bei ungeplanten Ausfällen schnell wieder in Betrieb zu nehmen. Wie aber aktuelle Studien zeigen, verlagern Unternehmen ihre Sicherheits-kontrollen zunehmend vom Netzwerk-Kern auf die Endpunkte und Endgeräte.

Im Folgenden finden Sie Empfehlungen, wie sich eine effektive Security-Strategie für Rechenzentren umsetzen lässt.

- **Umstellung auf eine Zero-Trust-Architektur:** Bei einem Zero-Trust-Modell gilt jede Transaktion, Bewegung oder Iteration von Daten grundsätzlich als verdächtig. Eine systematische Zero-Trust-Security verfolgt das Netzwerk-Verhalten und den Datenfluss in Echtzeit, überprüft jeden, der Daten aus dem System abruft, und alarmiert bei anormalem Verhalten Mitarbeiter oder widerruft Zugriffsrechte von Benutzern. Die Bedrohungserkennung muss stark sein – unabhängig davon, ob sie auf verschiedene Security-Systeme verteilt ist oder zentral von einer Netzwerk-Firewall übernommen wird. Die Durchsetzung kann mit einer Netzwerk-Firewall oder über ein NAC-Gerät (Network Access Control) erfolgen. Auch kann die Security über eine zentrale Konsole verwaltet werden, die das zentrale Management und die operative Steuerung kritischer Computersysteme überwacht (in den meisten Unternehmen befinden sich diese normalerweise im Rechenzentrum und in Großrechnern).

- **Integrierte Sicherheitsstufen und Redundanz für Rechenzentren:** Um die Datensicherheit zu gewährleisten, sind Sicherheitskontrollen und Systemprüfungen erforderlich, die für jeden Layer in die Struktur eines Rechenzentrums integriert werden.

- **Schutz aller Endpunkte:** Jedes mit dem Rechenzentrums-Netzwerk verbundene Gerät – z. B. Server, Tablets, Smartphones oder Laptops – ist ein Endpunkt und muss daher geschützt werden.

- **Dokumentation von Sicherheitsverfahren:** Strenge, genau definierte und dokumentierte Verfahren sind von entscheidender Bedeutung. Etwas so Simples wie eine regelmäßige Bereitstellung muss gut geplant werden.

- **Regelmäßige Security-Audits:** Die Audits können von täglichen Sicherheitsüberprüfungen wie physische Walkthroughs bis hin zu vierteljährlichen PCI- und SOC-Audits oder automatisierten Berichten zur Erkennung von Fehlkonfigurationen und anderen nicht konformen Praktiken reichen.

- **Intrusion Detection und Prevention-Systeme (IDPS) sind wichtig:** IPS-Überprüfungen sind für den Schutz kritischer Netzwerk-Infrastrukturen und schwer zu patchender Legacy-Anwendungen unverzichtbar. Das Erkennen dieser Art von netzwerkbasierten Angriffen erfordert eine Echtzeit-Überwachung der Netzwerk- und Systemaktivität auf ungewöhnliche Ereignisse, gestützt von künstlicher Intelligenz und maschinellem Lernen.

- **Segmentierung des Systems:** Die Segmentierung des Netzwerks auf verschiedenen Ebenen ist entscheidend, um die seitliche Ausbreitung von Bedrohungen zu verhindern. Segmentierungstechniken können z. B. host- oder netzwerkbasiert sein. Bei der hostbasierten Segmentierung wird auf jedem Host ein Agent ausgeführt und die Klassifizierung des gesamten Datenverkehrs in verschiedene Segmente erfolgt abhängig von der Endpunkt-Identität. Andere Techniken arbeiten z. B. mit einer Mikrosegmentierung, die jedoch die abgestimmte Steuerung (Orchestrierung) der Benutzerzugriffe auf Anwendungen und Dienste verkompliziert. Besonders einfach lassen sich Sicherheitsrichtlinien mit einer netzwerkbasierten Segmentierung durchsetzen, in der eine Netzwerk-Firewall die Segmente anlegt. Grundsätzlich wird bei einer Segmentierung jedes Segment in einem unabhängigen Subnetz isoliert und ist damit von allen anderen Segmenten getrennt. Potenzielle Bedrohungen werden in einem einzelnen Subnetz abgeschottet, was das Übergreifen von Bedrohungen auf andere Geräte und Netzwerke verhindert. Die Segmentierung kann auch auf Anwendungsebene, Portebene oder mit Containern erfolgen. Bei der Port-Segmentierung kann z. B. eine Switch-Schnittstelle direkt von einer Netzwerk-Firewall oder mit einer NAC-Lösung blockiert werden.

- **Überwachung seitlicher Bewegungen:** Laterale Angriffe umfassen mehrere Techniken, mit denen sich Angreifer quer durch das Netzwerk sowie auf verschiedenen Geräten bewegen und sich dabei umfassende Zugriffsrechte aneignen können. Haben Angreifer ein System infiltriert, scannen sie alle Geräte und Apps auf anfällige Komponenten. Wird die Kompromittierung nicht frühzeitig erkannt, können sich Angreifer weitreichende Zugriffsrechte sichern und verheerenden Schaden anrichten. Mit einer Überwachung seitlicher Bewegungen lässt sich die Zeit begrenzen, in der Sicherheitsbedrohungen für Rechenzentren in den Systemen aktiv sind.

- **Security auf Netzwerk-Ebene:** Bei der Verschlüsselung auf Netzwerk-Ebene wird Kryptografie auf der Datenübertragungsschicht angewendet – das ist der Netzwerk-Layer, der für die Konnektivität und das Routing zwischen zwei kommunizierenden Einheiten zuständig ist. Die Verschlüsselung ist während der Datenübertragung aktiv und funktioniert unabhängig von jeder anderen Verschlüsselung. Sie stellt also eine eigenständige Lösung dar.

- **Implementierung von SSL und einer Bedrohungsabwehr:** Diese Lösungen führen eine SSL-Inspektion durch (u. a. nach dem neuesten TLS1.3-Standard), erkennen versteckte Bedrohungen, beenden das Abgreifen von Daten und stoppen Angriffe auf die Security-Infrastruktur.

- **Hyperscale-Security:** Sicherheitslösungen umfassen ultraschnelle Firewalls, die sehr hohe Benutzerzahlen bewältigen können und Schutz vor DDoS-Angriffen bieten, mit denen kritische Unternehmensprozesse heruntergefahren werden sollen.

- **Umfassende Automatisierung:** Sicherheitslösungen bieten effiziente, skalierbare Automatisierungs- und Orchestrierungs-Tools, die eine konsequente Implementierung von Sicherheitsrichtlinien für alle Infrastrukturen gewährleisten – unabhängig vom Standort.