



McAfee[®]
An Intel Company

SCHUTZ VON RECHENZENTREN

Lösungsleitfaden

Epsilon nach dem Datenschutzverstoß

Im Jahr 2011 gelangten durch einen Datenschutzverstoß beim E-Mail-Vermarktungsunternehmen Epsilon die Namen und E-Mail-Adressen von Millionen Kunden an die Öffentlichkeit. Da die Dienste von Epsilon von einer Reihe namhafter Unternehmen in Anspruch genommen werden, mussten die Kunden umgehend benachrichtigt werden, um sie vor einem möglichen Betrug zu warnen. Zu den Unternehmen, die ihre Kunden warnen mussten, zählten u. a.: Barclaycard US, Capital One, Best Buy, JPMorgan, Citigroup, TiVo, Disney Destinations, New York & Company, Walgreens und Marriott. (Quelle: <http://mcaf.ee/5342e>)

Security Connected

Das Security Connected-Framework von McAfee ermöglicht die Integration mehrerer Produkte, Dienste und Partnerschaften, um eine zentrale, effiziente sowie effektive Risikominimierung zu erreichen. Mit der Basis von mehr als zwei Jahrzehnten bewährter Sicherheitspraktiken, hilft der Security Connected-Ansatz Unternehmen aller Größen und Bereiche aus der ganzen Welt bei der Verbesserung ihrer Sicherheitslage, der Optimierung der Sicherheit für eine höhere Wirtschaftlichkeit sowie bei der strategischen Sicherheitsausrichtung auf Geschäftsinitiativen. Die Referenzarchitektur für McAfee Security Connected bietet einen konkreten Weg von der Idee zur Implementierung. Nutzen Sie sie, um die Security Connected-Konzepte an Ihre speziellen Risiken, Ihre Infrastruktur und Geschäftsziele anzupassen. McAfee ist stets auf der Suche nach neuen Möglichkeiten, um seine Kunden umfassend zu schützen.

Stärkerer Schutz für ein flexibleres Rechenzentrum

Herausforderungen

Rechenzentren führen Unternehmen. Zu den Aufgaben eines Rechenzentrums zählen Umsatzgenerierung, die Speicherung vertraulicher Daten und die Bereitstellung unternehmenswichtiger Dienste. Sie sind aufgrund ihrer Wichtigkeit und ihres Wertes Ziele. Vertrauliche Daten, Geschäftsanwendungen, Datenbanken, Netzwerkgeräte, Speicher und unterstützende Infrastrukturen befinden sich seit langem im Fadenkreuz externer und interner Angreifer sowie von Auditoren mit behördlichen Befugnissen.

Praktisch jedes Sicherheitsproblem und jede behördliche Vorgabe in Bezug auf Rechenzentren hat zu einer Einzellösung geführt. Dieser reaktive Vorgang, aus dem jedes Mal neue Einzellösungen hervorgehen, hat dazu geführt, dass Kontrollmaßnahmen für Rechenzentren kompliziert, zahlreich, teuer sowie unzusammenhängend geworden sind und somit die meisten Unternehmen überwältigen. Zusätzlich zu vorhandenen Anforderungen kommen ständig neue Bedrohungen und Trends hinzu. Unternehmen fordern von ihren Rechenzentren beispielsweise die Unterstützung von Mobilität und Web 2.0 sowie Schutz gegen gezielte und opportunistische Angriffe. Gleichzeitig sollen sie Ausfallzeiten minimieren und regelmäßig Berichte zum Nachweis von Compliance generieren.

Bei der klassischen Rechenzentrums-Sicherheit fehlt es an Handlungsfähigkeit für den schnellen und nahtlosen Einsatz neuer Anforderungen, an Sicherheits-Management für Effizienz und Effektivität, an der Verfügbarkeit und Integrität, die für heutige geschäftskritische Vorgänge notwendig sind, sowie an der optimierten Auslegung für die Wirtschaftlichkeit. Rechenzentren haben sich entwickelt und sind jetzt geschäftskritischer als je zuvor. Heutige IT-Abteilungen gehen neue Wege. Wir können nur darüber spekulieren, was in fünf Jahren das nächste große Ereignis ist, aber wenn die letzten fünf Jahre ein Maßstab sein sollen, dann wird das, was wir als wirksamen Schutz erachteten, uns nicht weiter schützen können. Ein strategischer Rahmen wird benötigt, der dabei hilft, die zuvor inkompatiblen Elemente zu verbinden.

Nach dem im März 2011 vom Ponemon Institute veröffentlichten Bericht „Cost of a Data Breach“ kostet jeder kompromittierte Datensatz 214 Dollar, so dass ein Datenschutzverstoß im Durchschnitt Kosten von 7,2 Millionen Dollar nach sich zieht.²

Heartland Payment Systems nach dem Datenschutzverstoß

2010 schloss Heartland einen Vergleich mit VISA und zahlte 60 Millionen US-Dollar, um alle potenziellen Klagen infolge des Datenschutzverstoßes von 2009 beizulegen. Ein Jahr zuvor hatte Heartland mit Amex bereits einen ähnlichen Vergleich in Höhe von 3,5 Millionen US-Dollar geschlossen.¹



Lösungen

Unternehmensflexibilität

Das Team, das den Betrieb des Rechenzentrums sicherstellt, ist mit diversen Aufgaben betraut: vom Aufbau von Lösungen für dauerhafte Compliance über Virtualisierung bis hin zur Konsolidierung und Nutzung der Cloud. Ein Sicherheits-Framework sollte flexibel genug sein, um schnelle Änderungen und die Anpassung an neue Trends ohne zusätzliche Risiken zu ermöglichen. Ein robustes Sicherheits-Framework, das ein solches Maß an Flexibilität ermöglicht, wirkt sich sowohl auf sicherheitsbezogene als auch geschäftliche Betriebsvorgänge positiv aus.

Sicherheits-Management

Datenschutzverstöße sind eine kostspielige Angelegenheit: Bußgelder wegen Gesetzesverstößen, Sammelklagen und PR-Ausgaben bis hin zu verringerter Markentreue, Kundenverlusten und letztlich Umsatzeinbußen können die Folge sein. Aufgrund der Komplexität von Rechenzentren im Zusammenhang mit einigen der genannten Tendenzen und Bedrohungen ist für eine erfolgreiche Risikominimierung eine ganzheitliche Sicherheitsstrategie erforderlich. Zur Verwaltung von Rechenzentren aller Größen- und Komplexitätsordnungen sollte daher eine zentrale Sicherheits-Management-Lösung eingesetzt werden, die Einzellösungen für den Schutz von Daten, Endpunkten, Netzwerk und der Cloud zusammenführt. Ein ausbaufähiges Sicherheits-Management ist unverzichtbar für Transparenz bezüglich der Anwendungen und Datenbanken, mit denen Transaktionen verarbeitet werden, und der Speichergeräte, auf denen die Daten aufbewahrt werden.

Verfügbarkeit und Integrität

Es stellt durchaus eine Herausforderung dar, angesichts interner und externer Bedrohungen einerseits Verfügbarkeit und Integrität aufrecht zu erhalten, andererseits aber auch neue Trends wie mobile Webseiten-Entsprechungen zu unterstützen, eine Integration in Web 2.0-Dienste von Drittanbietern zu ermöglichen oder die Vorteile diverser Cloud-Infrastrukturen zu nutzen. Außerdem kann es außerordentlich riskant sein, wenn nicht sorgfältig genug darauf geachtet wird, sich ein zuverlässiges Sicherheitskonzept zuzulegen, das nicht kurzfristig auf den reinen Schutz von Inhalten oder des Netzwerks beschränkt ist, sondern den Schutz für Endpunkte, Inhalte sowie das Netzwerk miteinander verknüpft und dabei die Integration mit der Cloud ermöglicht. Ein Sicherheits-Framework sollte minimale Latenzen

aufweisen, das Risiko manueller Konfigurationsfehler verringern, die Installation schädlicher Software unterbinden und Daten unabhängig davon, wie das Rechenzentrum strukturiert ist, schützen – ob konsolidiert, virtualisiert oder cloud-basiert. Schutz für virtuelle Umgebungen, also virtuelle Server und virtuelle Desktop-Infrastrukturen (VDI), ist unverzichtbar. VDI-Installationen sind auf allen Geräten vom Smartphone bis hin zu Laptops und virtuellen Servern gängig – und in Rechenzentren der Normalfall. Bei den heutigen Lösungen besteht Optimierungsbedarf zur Anpassung an den Trend zur Virtualisierung, aber darüber dürfen die Grundlagen nicht vernachlässigt werden. Hohe Latenzen und außerplanmäßige Ausfallzeiten kommen für geschäftskritische Umgebungen nicht in Frage. Netzwerkbetrieb, Zugriffssteuerung, Schutz von Endpunkten und Firewalls müssen allesamt auf die IT-Anforderungen ausgelegt werden. Sicherheit allein genügt nicht, denn unterdurchschnittliche Sicherheitslösungen, die hohe Latenzen mit sich bringen, können sich genauso schädlich auswirken wie ein Angriff.

Sicherheitsoptimierung

Die Sicherheitsoptimierung führt Unternehmen weg von den rein technischen Fragen in Bezug auf Sicherheitskontrollen – „Ist es machbar?“ – und hin zur Art der Umsetzung – „Wie lässt es sich am besten realisieren?“. An Sicherheitslösungen herrscht kein Mangel, und die meisten leisten gute Dienste. Aber in der Summe führen sie zu Unübersichtlichkeit, dem größten Feind der Sicherheit. Voneinander isolierte Wege, Lösungen mit fehlenden Schnittstellen zueinander, und die Abhängigkeit des Betriebs von immer mehr Ressourcen sind auf lange Sicht nicht tragbar. Stattdessen sollten aktuelle Sicherheits-Frameworks ein optimiertes Sicherheitsmodell unterstützen, das auf eine zentrale Verwaltung der Sicherheitskontrollen abzielt, Synergieeffekte zwischen diesen Kontrollen ermöglicht, die Lösungen in Einklang mit den geschäftlichen Prioritäten bringt und dabei Kosteneinsparungen im Sicherheitsbereich bewirkt. Da sich Bedrohungen ständig weiterentwickeln und auf zahlreiche Trends schnell aufgesprungen wird, wird ein optimiertes Sicherheits-Framework in Zukunft für kostengünstigen, effizienten und sicheren Geschäftsbetrieb unabdingbar sein. Optimierte Lösungen sind ein untrennbarer Bestandteil der Automatisierung des Compliance-Prozesses, so dass Sicherheitsaufgaben und -prozesse im Zusammenhang mit behördlichen Auflagen aufeinander abgestimmt werden, ohne dass dadurch zusätzlicher Aufwand entsteht.

Empfehlenswerte Vorgehensweisen

- Machen Sie sich bewusst, dass Rechenzentren einen schnellen Wandel durchleben, der sich in Konsolidierung, Virtualisierung und Cloud Computing äußert
- Implementieren Sie Lösungen, die den Anforderungen nach Flexibilität, Sicherheits-Management, Verfügbarkeit und Integrität sowie Sicherheits-Optimierung gerecht werden
- Bringen Sie Lösungen aus, mit denen Sicherheitsabläufe für wichtige Komponenten des Rechenzentrums – Netzwerke, virtuelle Lösungen, Datenbanken, Server und Speichergeräte – zentralisiert werden können
- Stellen Sie sicher, dass Sie die genutzten Sicherheitslösungen auch bei der Compliance-Automatisierung unterstützen
- Achten Sie bei Sicherheits-themen auch darauf, dass Grundvoraussetzungen für den Betrieb wie Verfügbarkeit und Latenz berücksichtigt werden

Nach Angaben der Data Loss DB Open Security Foundation waren zum April 2011 75 Prozent der Datenverluste auf kriminelle Tätigkeiten zurückzuführen, der Rest auf Nachlässigkeit.³

Wertsteigernde Faktoren

Ihre Initiativen bezüglich des Rechenzentrums sollten auf sicherheitsbasierte Technologie zur Steigerung der betrieblichen Effizienz beruhen. Ziehen Sie die folgenden Bereiche in Betracht, in denen Optimierungspotenzial für Ihr Rechenzentrum besteht:

- *Konsolidierung* – Die Lösungen sollten zur Konsolidierung über die gesamte Hard- und Software- sowie Support-Infrastruktur hinweg ausgebracht werden.
- *Standardisierung* – Die Lösungen sollten die Standardisierung der Schutzfunktionen für Endpunkte, Daten und das Netzwerk unterstützen. Dadurch lässt sich leichter sicherstellen, dass die Analyse von Bedrohungen sowie die Reaktionen darauf effizient und wirkungsvoll sind.
- *Verringerte Audit-, Compliance- und Überwachungskosten* – Die Lösungen sollten eine Kostenreduzierung für IT-Audits und Compliance bewirken (oder dadurch gerechtfertigt sein), da sich ein Audit der Gesamtsysteme und -prozesse durchführen lässt, anstatt alle Nodes einzeln zu prüfen.
- *Geringerer Netzwerkverkehr* – Die Lösungen im Netzwerkkern dienen zum Schutz, sollten aber auch unnötigen Netzwerkverkehr sowie Spam beseitigen.
- *Reduzierung der Helpdesk-Kosten* – Die Bemühungen um den Schutz des Rechenzentrums Kerns sollten dazu führen, dass weniger Endbenutzer den Helpdesk wegen Sicherheitsvorfällen kontaktieren.

Dazugehöriges Material aus der Referenzarchitektur für McAfee Security Connected

Stufe II

- Schutz von Informationen
- Steuerung und Überwachung von Änderungen

Stufe III

- Bewertung von Schwachstellen
- Durchsetzung von Compliance auf Endpunkten
- Schutz vor Denial-of-Service (DoS und DDoS)-Angriffen
- Schutz von Servern

Weitere Informationen zur Referenzarchitektur für McAfee Security Connected finden Sie unter:
www.mcafee.com/de/enterprise/reference-architecture/.

Informationen zum Autor



Brian Contos, CISSP, ist Director of Global Security Strategy bei McAfee. Er ist ein anerkannter Sicherheitsexperte mit beinahe zwei Jahrzehnten Erfahrung im Bereich Sicherheits-Engineering und -Management. Darüber hinaus ist er Autor diverser Bücher, darunter *Enemy at the Water Cooler* („Der Feind am Wasserkühler“) und *Physical and Logical Security Convergence* („Die Konvergenz von physischer und logischer Sicherheitsinfrastruktur“). Er hat mit Regierungsorganisationen und Unternehmen aus der Forbes Global 2000-Liste auf dem gesamten amerikanischen Kontinent, in Europa, im Nahen Osten und in Asien zusammengearbeitet. Auf wichtigen Branchenveranstaltungen wie der RSA, Interop, SANS, OWASP und SecTor wurde er bereits als Sprecher eingeladen. Darüber hinaus schreibt er Fach- und Wirtschaftsartikel für Publikationen wie *Forbes*, die *New York Times* und *London Times*. Contos ist Distinguished Fellow des Ponemon Institute und Absolvent der University of Arizona.

brian_contos@mcafee.com || <http://siblog.mcafee.com/author/brian-contos/> || @BrianContos

¹ <http://mcaf.ee/gvxxh>

² <http://www.ponemon.org/local/upload/fckjail/generalcontent/18/file/2010%20Global%20CODB.pdf>

³ <http://datalossdb.org/>

