5 geschäftliche Herausforderungen, die Sie mit einem Cloud-SIEM bewältigen

Stehen Sie vor der Frage, ob Sie Ihr SIEM (Security Information and Event Management) in die Cloud verlegen sollen? Oder strebt Ihr Unternehmen eine Cloud-First-Strategie an? Hier sind fünf geschäftliche Herausforderungen, die Sie mit einem cloudbasiertes SIEM bewältigen können.

1. Mitarbeitermangel

Über die

HÄLFTE

der Unternehmen leiden unter einem Mangel an IT-Sicherheitsfachleuten. Und das Problem verschärft sich.[1] Weltweit sind **2,93 Millionen Stellen in der IT-Sicherheit unbesetzt.**[2]

Gleichzeitig sind

84 %

der IT-Sicherheitsfachkräfte offen für Angebote anderer Arbeitgeber.[3] Unternehmen müssen deshalb zusehen, ihre Mitarbeiter zu halten.

So hilft ein cloudbasiertes SIEM

Mit einem cloudbasierten SIEM können sich die Sicherheitsteams auf das Threat Hunting und die Beseitigung realer Bedrohungen konzentrieren, statt auf die Behebung von Infrastruktur- oder Kapazitätsproblemen.

Bei einem cloudbasierten SIEM werden die Infrastruktur, die Kapazitäten, die Patches und die Verwaltung automatisch bereitgestellt. So können Ihre Sicherheitsmitarbeiter auf den Schutz Ihres Unternehmens fokussieren. Und haben mehr Zeit für die Aufgaben, die ihnen wichtig sind.

2. Kontinuitätsplanung

Können Sie gewährleisten, dass Ihr Betrieb auch nach einem Sicherheitsvorfall reibungslos weiterläuft?

In mehr als

50 %

der Unternehmen ereignete sich in den letzten fünf Jahren ein Vorfall, der zu einer Betriebsunterbrechung[4] von acht Stunden oder mehr führte.

Nur 35 % der Vorfälle gehen auf Naturkatastrophen zurück – 45 % dagegen auf betriebliche Probleme und 19 % auf menschliches Versagen.

So hilft ein cloudbasiertes SIEM

Wenn Ihr SIEM in der Cloud ist, ist es jederzeit und überall verfügbar. Falls Ihr Unternehmen wegen eines Zwischenfalls seinen Standort verlagern muss, wird der Dienst dadurch nicht unterbrochen – die Sicherheit bleibt also gewahrt.

Und da die Logdaten in der Cloud gespeichert sind, gehen sie auch dann nicht verloren, wenn Sie den Zugriff auf die lokalen Protokolle verlieren.

3. Kostenkontrolle

Denken Sie auch an Ihren CFO.

On-Premises-Software hat ihren Preis. Und die entstehenden CapEx-Kosten können einige Kopfschmerzen verursachen.

Die **Vorlaufkosten** sind erheblich. Der **künftige Kapazitätsbedarf** lässt sich schwer vorhersagen. Und die **Budgetgenehmigung** kann langwierig und mühsam sein.

So hilft ein cloudbasiertes SIEM

Wenn Sie Ihr SIEM in die Cloud legen, verlagern sich die Kosten von CapEx zu OpEx.

Ein Wechsel zur Cloud bedeutet: Keine hohen Vorlaufkosten für Hardware. Keine unnötigen Ausgaben für Personal, das nur in Spitzenzeiten ausgelastet ist. Keine kostspieligen Software-Upgrades – Sie erhalten die neuesten Versionen sofort und automatisch.

Reduzieren Sie Cashflow-Schwankungen, statt hohe Anschaffungskosten tätigen zu müssen. Außerdem können OpEx-Kosten steuerliche und bilanzielle Vorteile bringen.

4. Investition in Menschen statt Infrastrukturen

Tische und Stühle machen Ihr Unternehmen nicht sicherer. Serverracks und Klimaanlagen auch nicht. Was Sie brauchen, sind die richtige Software und qualifiziertes Personal. Doch allzu oft müssen Geld und Zeit in Hardware und Infrastruktur gepumpt werden.

Viele Unternehmen geben große Summen für den Bau und Betrieb von Rechenzentren aus, doch der zusätzliche Platz allein erhöht die Sicherheit nicht.

So hilft ein cloudbasiertes SIEM

Mit einem cloudbasierten SIEM können Sie bedarfsgerecht skalieren. Das heißt, dass Sie Ihre Ausgaben auf den Schutz Ihrer Daten und Ihres Unternehmens konzentrieren können.

Ein Cloud-SIEM ermöglicht es, hochqualifiziertes Sicherheitspersonal einzustellen, das strategischen Wert erbringt. So können Sie mit Ihren Daten arbeiten, um Ihr Unternehmen zu schützen, statt auf operative Belange und die Speicherung und Verwaltung von Daten fokussieren zu müssen.[5]

5. Stressfreie Upgrades und Patches

Ungepatchte Software ist ein gravierendes Sicherheitsrisiko. Aktualisierungen sind jedoch große Zeitfresser, und Ihr SOC hat anderes zu tun. Mitarbeiter wollen ihre Arbeit oft nicht wegen Updates und Patches unterbrechen und zögern sie deshalb hinaus oder unterlassen sie ganz, ohne sich ihrer Bedeutung bewusst zu sein.

Sollte ein hochqualifizierter Sicherheitsexperte seine Zeit mit Patches und Updates verbringen? Die Betroffenen selbst glauben das nicht. Laut einer Umfrage bevorzugen sie folgende Aufgaben[6]:

Threat Hunting
(55 Prozent)

Bedrohungen beseitigen
(55 Prozent)

Bedrohungen verhindern
(54 Prozent)

So hilft ein cloudbasiertes SIEM

Log-Monitoring, Patches und Richtliniendurchsetzung sind notwendig. Ein cloudbasiertes SIEM bietet dafür eine einfache Lösung.

Es sorgt dafür, dass Patches umgehend automatisch installiert werden. Dies räumt einen wichtigen Angriffsvektor von vornherein aus.

Keine Kompromisse.

Bei einem cloudbasierten SIEM sollten Sie keine Kompromisse eingehen müssen. Mehr Flexibilität und Komfort rechtfertigen keinen reduzierten Funktionsumfang.

LogRhythm Cloud vereint die Leistungsfähigkeit der LogRhythm NextGen SIEM-Plattform mit der Einfachheit und Flexibilität einer SaaS-Lösung.

Maximiert die Effektivität Ihres Sicherheitsteams

Verkürzt die mittlere Erkennungszeit (MTTD) & mittlere Reaktionszeit (MTTR)

Integriert Security Orchestration, Automation & Response (SOAR)

Unterstützt Cloud-First-Initiativen

LogRhythm Cloud

Die Stärken der LogRhythm NextGen SIEM-Plattform – jetzt auch in der Cloud

[1]The cybersecurity skills shortage is getting worse:
https://www.csoonline.com/article/3331983/the-cybersecurity-skills-shortage-is-getting-worse.html

[2]Cybersecurity Professionals Focus on Developing New Skills as Workforce Gap Widens:
https://www.isc2.org/-/media/ISC2/Research/2018-ISC2-Cybersecurity-Workforce-Study.ashx?la=en&hash=4E09681D0FB51698D9BA6BF13EEABFA48BD17DB0%5Ch

[3]What Employers Need to Know About Cybersecurity Jobseekers:
https://www.isc2.org/Research/Hiring-Top-Cybersecurity-Talent

[4]17 Shocking Statistics about Disaster Recovery and Business Resiliency—Where Does Your Organization Stand?: Part 1:
https://www.datacore.com/blog/17-shocking-statistics-about-disaster-recovery-and-business-resiliency-where-does-your-organization-stand-part-1/

[5]If Everything is a Service, Why Do We Need Data Centers?:
https://www.datacenterknowledge.com/archives/2017/05/31/everything-service-need-data-centers

[6]Cyber Security Training: What CISOs Must Do to Mitigate Talent Churn:
https://blog.5nine.com/cybersecurity-training-what-cisos-must-do-to-mitigate-talent-churn