WHITEPAPER

Security Operation Center: *OnPrem vs Cloud*

sure[secure]

Security Operation Center – On-Premise oder Cloud?

Wir beleuchten die möglichen Betriebsmodelle.

1. Einleitung

Unabhängig davon, ob ich ein Security Operation Center als Dienstleistung einkaufe oder selbst aufbaue: Am Anfang steht ein Konzept.
Bei der Erstellung dieses Konzepts stellt sich irgendwann die Frage, wie das Security Operation Center betrieben werden soll.
Prinzipiell gibt es drei mögliche Modelle:

1. **Security Operation Center On-Premise**
   Ein On-Premise SOC befindet sich physisch innerhalb der Unternehmensinfrastruktur. Hier werden Security Monitoring und Response lokal durchgeführt. Dies ermöglicht eine direkte Kontrolle über alle Sicherheitsaspekte.
2. **Security Operation Center – Hybrid**
   Das hybride SOC kombiniert Elemente sowohl des On-Premise- als auch des Cloud-basierten SOC-Modells. Dieser hybride Ansatz ermöglicht es Unternehmen, von den Vorteilen beider Modelle zu profitieren und gleichzeitig Flexibilität und Skalierbarkeit zu erhalten.
3. **Security Operation Center – Cloud**
   Ein Cloud SOC nutzt Cloud-Plattformen von Drittanbietern, um Sicherheitsdienste bereitzustellen. Dies ermöglicht eine flexible Skalierung, reduziert den Bedarf an lokaler Hardware und bietet schnellen Zugriff auf erweiterte Sicherheitsfunktionen.

Im weiteren Verlauf dieses Whitepapers wollen wir herausfinden, was die wichtigsten Vor- und Nachteile der beiden Modelle sind.

2. Was ist eigentlich die Ausgangssituation?

Entscheidend für die Wahl des Betriebsmodells ist die Ausgangssituation. Ein SOC hat immer die Aufgabe, das Unternehmen zu schützen. Dazu werden Logfiles verschiedenster Systeme und Applikationen gesammelt, aufbereitet und korreliert. Die Priorität sollte dabei auf der Anbindung kritischer Systeme liegen - also der Systeme, die für die Wertschöpfung zwingend notwendig sind. Daraus ergeben sich weitere Fragen:

- Wie sieht die Architektur meiner IT- und ggf. OT-Infrastruktur eigentlich aus und welche Ressourcen benötige ich eigentlich, um diese in Takt zu halten?
- Wie hoch muss die Verfügbarkeit der Daten sein und wie lange will bzw. muss ich diese vorhalten?
- Welche Anforderungen habe ich an die Technik und welche Funktionalitäten sind für mich prioritär?
- Welches Budget steht zur Verfügung?

Und diese Fragen sind sicherlich noch nicht vollständig.
Aber, all das ist ausschlaggebend für die Entscheidung.

Ein Beispiel:

Wir skizzieren ein Vertriebsunternehmen.
Das Unternehmen hat verschiedene Standorte in Europa. Vor Ort gibt es in der Regel nur wenige Server und Clients bzw. Endgeräte. Dazu kommen die mobilen Geräte der Mitarbeitenden. Es gibt 13 Standorte mit der Zentrale in Wien, an denen insgesamt 250 Mitarbeitende beschäftigt sind. Die IT-Abteilung besteht aus 6 Spezialisten, 5 Administratoren und einem IT-Leiter.

Hauptsächlich werden Microsoft-Produkte in der Cloud-Variante eingesetzt. Daneben gibt es einige andere Systeme wie ein CRM und Warenwirtschaftssysteme. Außerdem gibt es einige Sicherheitssysteme wie Firewalls und einen Server- und Endpoint-Schutz.

In diesem Szenario befinden sich fast alle Daten bereits in der Cloud und es gibt wenig komplexe, individuelle Log-Quellen. In Anbetracht der Anfangsinvestition beim On-Prem Modell und der überschaubaren IT-Abteilung, wäre die Empfehlung hier wahrscheinlich ein Security Operation Center as a Service einzukaufen.

Es geht aber nicht nur um die Infrastruktur, sondern auch um den Betrieb der Plattform, insbesondere bei der Implementierung eines On-Premise SOC.

3. Betriebsaufwände

Wenn ich das SOC in die eigene Infrastruktur hole, bin ich für den Betrieb verantwortlich. D.h. es entstehen zusätzliche Aufwände, die auf die IT-Abteilung des Unternehmens zukommen.

3.1 SOC Plattform Betrieb

Zu einem State-of-the-Art SOC gehört in der Regel vor allem eine SIEM Technologie, um Daten sammeln und korrelieren zu können und auch ein Vulnerability Scanner, um zu wissen, wo meine Infrastruktur mögliche Angriffspunkte bietet. Was bedeutet das nun für meine On-Prem Infrastruktur? Unter anderem werden folgende Dinge benötigt:

- Virtuelle Maschinen, die mit dem von der Anwendung unterstützten Betriebssystem laufen.
- Ausreichend Datenbanken
- Benutzer- und Servicekonten sowie ein entsprechendes Berechtigungskonzept
- Diverse Firewall-Freigaben, da das SIEM Daten aus allen Netzwerken erhalten muss

All diese Anforderungen kommen auf das IT-Betriebsteam zu und führen zu ungeplanten, zusätzlichen Aufwänden. Dieser Aufwand entsteht nicht einmalig, sondern kontinuierlich. Die SOC-Architektur wird sich sukzessive ändern und damit auch die Plattform.

Diese Aufwände fallen auch im hybriden Betriebsmodell an, da auch hier eine lokal installierte Plattform benötigt wird.

Jona Ridderskamp

CEO sure[secure]

3.2 Log Management und Wartung

Nachdem der Betrieb aufgenommen wurde, können Logs gesammelt werden. Log-Daten können prinzipiell von jedem Asset im Netz erzeugt und auch geliefert werden. Manche Daten können sofort verarbeitet werden, andere müssen erst aufbereitet werden. Wichtig ist aber immer zu wissen:

- Welches Asset liefert welche Daten an?
- Wo befindet sich dieses Asset?
- Wie gelangen die Daten in das SIEM?

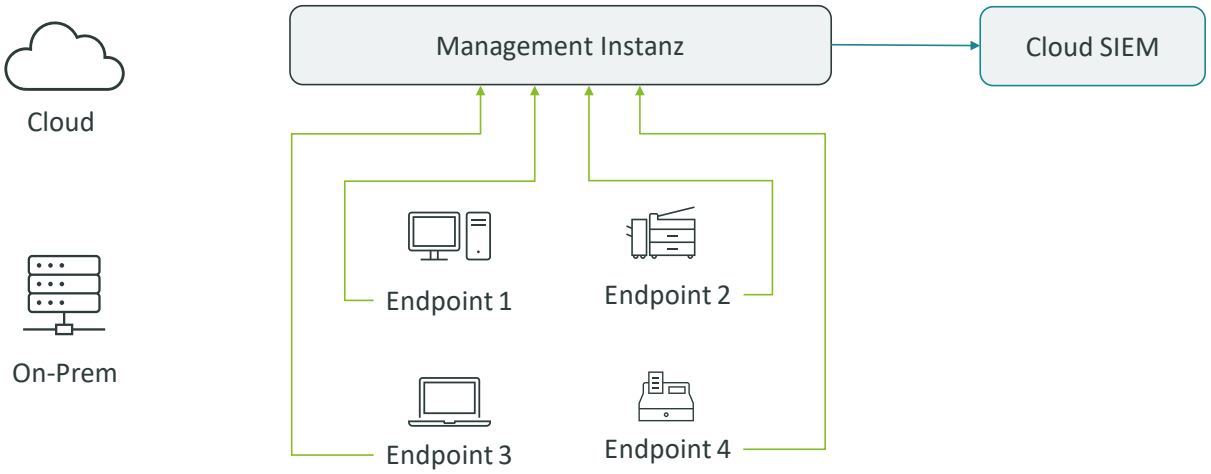
Ziel ist es, diese Daten sichtbar zu machen und mit anderen Datenströmen zu korrelieren, um Anomalien frühzeitig zu erkennen. Ohne die oben genannten Informationen kann ich eben nicht zurückverfolgen, wo der möglicherweise schädliche Datensatz seinen Ursprung hat.

Bei der Konzeption des Log-Managements muss auch berücksichtigt werden, ob an den Übergabepunkten genügend Bandbreite zur Verfügung steht, um die Daten in der erforderlichen Qualität und Zeit übertragen zu können. Je mehr Assets angeschlossen werden, desto größer wird auch das Datenvolumen. Da das Monitoring nahezu in Echtzeit erfolgen soll, muss dieser Punkt im Vorfeld berücksichtigt werden.

Wie werden die Logs eigentlich von den Applikationen zur Verfügung gestellt? Ein Beispiel-Case:

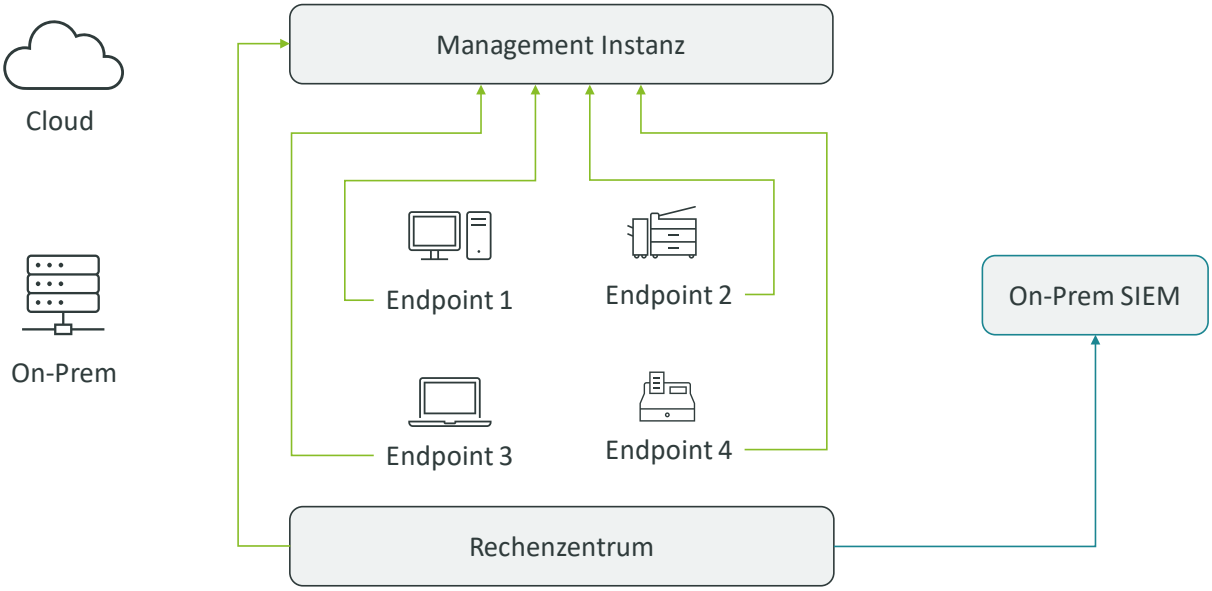
Die meisten Enterprise Software Produkte haben eine Management Komponente. D.h. die Software ist zwar auf einem lokalen PC installiert, wird aber über eine zentrale Komponente gesteuert. Die zur Analyse benötigten Logdaten werden an die Management Plattform geliefert. Dadurch ist es nicht notwendig, die Daten von jedem Client abzuholen, sondern es ist wesentlich effizienter, die Daten von der Management Plattform abzuholen.

Die Management Instanzen befinden sich in der Regel bereits in der Cloud und könnten die gesammelten Datensätze direkt an das Cloud SIEM weiterleiten.



Quelle: Eigene Darstellung

Im anderen Modell gehen die Datensätze den Umweg über das eigene Rechenzentrum.



Quelle: Eigene Darstellung

Ein ähnlicher, weit verbreiteter Fall ist die Erfassung von Anmeldedaten in Unternehmen. In den meisten Unternehmen wird dies heute über das Active Directory abgebildet. Dort werden alle Anmeldevorgänge an einer zentralen Stelle gesammelt und überwacht.

D.h. wenn an einem Sonntagmorgen plötzlich hunderte von Anmeldeversuchen für Max Mustermann registriert werden und Max Mustermann gar kein mobiles Endgerät besitzt, dann handelt es sich mit hoher Wahrscheinlichkeit um einen bösartigen Vorgang, den das SIEM auf Basis dieser Datensätze sofort als Alarm ausgeben kann.

3.3 IT-Ressourcen

Den Betriebsaufwand haben wir bereits beleuchtet, aber wie sieht es mit den IT-Ressourcen aus? Damit die Softwarekomponenten ihre Aufgaben erfüllen können, ist eine Aufrüstung notwendig.

Dazu gehört z.B. ausreichend Festplattenspeicher, um die Daten - je nach Art der Daten - für den vorgeschriebenen Zeitraum vorhalten zu können. Maßgeblich sind hier nicht nur die Aufbewahrungspflichten aus dem Handelsgesetzbuch, sondern auch die Vorgaben des Bundesamtes für Sicherheit in der Informationstechnik (BSI).

Darüber hinaus müssen die Ressourcen ständig verfügbar sein. Denn wenn die Software ausfällt, ist das SOC nicht mehr funktionsfähig. Deshalb darf es in der Architektur und im Design keinen Single Point of Failure geben.

Ein SOC benötigt viele Ressourcen - egal ob Cloud oder On-Premise. In der On-Premise-Variante ist dies aber mit hohen Investitionen verbunden. Die großen Hyperscaler wie Amazon, Google oder Microsoft verfügen über schier unendliche Ressourcen in Rechenzentren von mehreren Millionen Quadratkilometern.

4. Cloud vs. On-Premise - jetzt geht‘s ans Eingemachte

Dass das Cloud-Modell ressourcenschonender zu sein scheint, wurde schon oft erwähnt. Doch wo liegen hier die kritischen Punkte? Wir werfen einen Blick auf die Nach- bzw. Vorteile beider Modelle.

4.1 Ab in die Cloud

Bedenken hinsichtlich der Datensicherheit

Die Auslagerung von zum Teil sensiblen Daten in die Cloud kann Datenschutzbedenken aufwerfen, insbesondere wenn es um die Kontrolle über diese Daten geht. Unternehmen müssen sicherstellen, dass ihre Daten gemäß den gesetzlichen Anforderungen und internen Richtlinien geschützt sind. Zudem gilt in der Cloud-Welt das Modell der geteilten Verantwortung: Der Provider garantiert nur die Sicherheit der Hardware, nicht aber die Sicherheit der Daten.

- **Abhängigkeit von Cloud-Anbietern**
  Die Abhängigkeit von einem Cloud-Anbieter kann Risiken bergen, insbesondere wenn es zu Ausfällen kommt oder der Anbieter seine Services oder Preismodelle anpasst.

- **Netzwerkkonnektivität**
  Die Effektivität eines Cloud SOC hängt stark von der Netzwerkkonnektivität ab. Eine schlechte Internetverbindung oder Ausfälle können die Reaktionszeit auf Sicherheitsvorfälle beeinträchtigen.

- **Kostenüberlegungen**
  Cloud-Dienste sind oft flexibel skalierbar, aber je mehr Datenquellen angeschlossen werden, desto höher können die Kosten im Laufe der Zeit werden, insbesondere wenn keine sorgfältige Überwachung und Verwaltung erfolgt.

4.2 Was passiert, wenn man On-Premise bestellt?

Dann bekommt man On-Premise und auch das hat seine Schwächen. Die hohe Anfangsinvestition und auch die mangelnde Skalierbarkeit haben wir schon mehrfach angesprochen, daher schauen wir uns noch weitere wesentliche Punkte an.

- **Fachkräftemangel:**
  Der Aufbau und Betrieb eines On-Premise SOC erfordert hochspezialisierte Sicherheitsexpert:innen. Der Fachkräftemangel in diesem Bereich kann die Rekrutierung von qualifiziertem Personal erschweren.
- **Komplexe Wartung und Updates:**
  Die Verantwortung für Wartung und Updates liegt vollständig beim Unternehmen. Dazu gehören regelmäßige Software-Patches, Firmware-Updates und die Aktualisierung von Sicherheitsrichtlinien. Fehlende Ressourcen oder Fachkenntnisse können zu Sicherheitslücken führen.
- **Eingeschränkte geografische Flexibilität:**
  Ein On-Premise SOC ist an den physischen Standort des Unternehmens gebunden. Dies kann zu Herausforderungen führen, wenn Unternehmen geografisch verteilte Niederlassungen haben oder Remote-Arbeitsmodelle nutzen.
- **Verzögerter Zugang zu Innovationen:**
  Die Implementierung neuer Sicherheitstechnologien und -dienste kann sich bei einem On-Premise SOC verzögern. Unternehmen müssen möglicherweise ihre Infrastruktur aktualisieren, um von den neuesten Innovationen profitieren zu können.

5 Worauf muss ich achten? Was sollte ich tun?

Die Entscheidung für ein SOC-Betriebsmodell erfordert eine gründliche Analyse der spezifischen Anforderungen und Umstände. Bei der Bewertung von Cloud- und On-Premise SOC-Optionen gibt es mehrere Schlüsselfaktoren:

- **Kosten**:
  On-Premise SOCs erfordern erhebliche Investitionen in Hardware, Software und die Ausbildung von Fachpersonal. Im Gegensatz dazu bieten Cloud-Lösungen flexible Preismodelle, die sich besser an die Bedürfnisse von Unternehmen anpassen lassen. Dabei ist es wichtig, alle Kostenfaktoren einschließlich der laufenden Betriebskosten zu berücksichtigen.
- **Skalierbarkeit:**
  Cloud SOCs bieten die Möglichkeit, Ressourcen nach Bedarf zu skalieren, was insbesondere für wachsende Unternehmen von Vorteil ist. On-Premise-Lösungen erfordern zusätzliche Investitionen, um mit dem Unternehmenswachstum Schritt zu halten.
- **Kontrolle und Sicherheit:**
  On-Premise SOC-Modelle bieten die volle Kontrolle über System, Daten und Infrastruktur. Dies kann für Branchen mit strengen Compliance-Anforderungen entscheidend sein. Im Gegensatz dazu bieten Cloud-Anbieter fortschrittliche Sicherheitsmaßnahmen, aber die Kontrolle über die physische Infrastruktur liegt nicht direkt in den Händen des Unternehmens.
- **Fachwissen und Ressourcen:**
  Die Implementierung und Verwaltung eines SOC vor Ort erfordert ein spezialisiertes Team von Sicherheitsexpert:innen. Cloud-Lösungen entlasten Unternehmen von der Notwendigkeit, internes Fachpersonal vorzuhalten.
- **Verfügbarkeit und Performance:**
  Cloud-Anbieter versprechen in der Regel eine hohe Verfügbarkeit ihrer Dienste. Dennoch ist es wichtig, die Service Level Agreements (SLAs) zu prüfen und sicherzustellen, dass sie den Anforderungen des Unternehmens entsprechen.

Eine pauschale Aussage zu diesem Thema ist daher nie zielführend. Für jedes SOC-Projekt ist es zwingend notwendig, eine Analyse durchzuführen und auf Basis der Daten ein fundiertes Konzept zu erstellen.

suresecure GmbH
Dreischeibenhaus 1
40211 Düsseldorf

Telefon: +49 (0) 2156 974 90 60
Telefax: +49 (0) 2156 975 49 78

E-Mail: kontakt@suresecure.de
www.suresecure.de