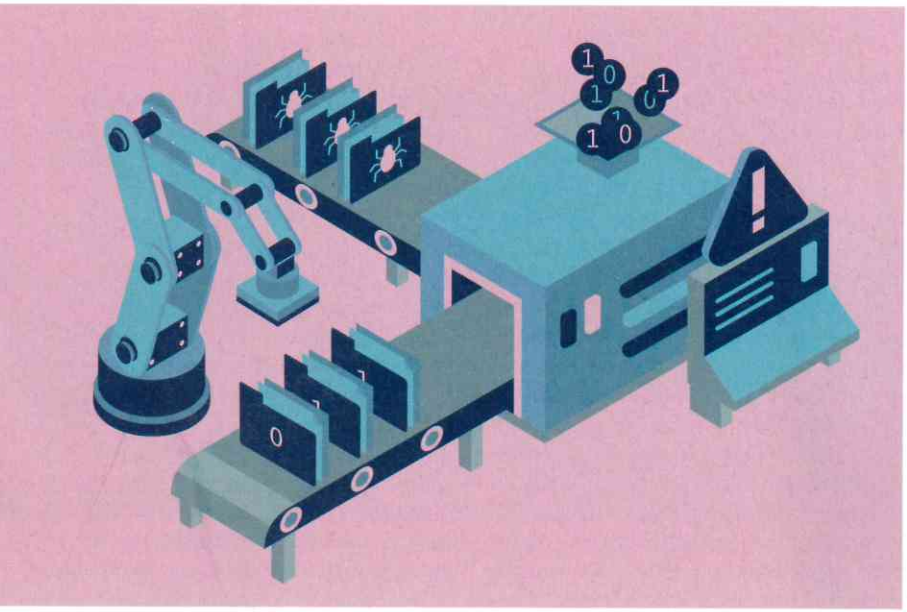


MDR: Moderne Endpunktsicherheit für alle?

Die permanenten komplexen Angriffe der letzten Jahre haben zu einer enormen Weiterentwicklung intelligenter Erkennungs- und Verteidigungsmechanismen geführt. „Managed Detection and Response", so das Schlagwort, krempelt den Markt der Dienstleistungen für Endpoint Security um.

Von Stefan Strobel

Aus den einstigen minimalistischen Maßnahmen zur Absicherung von Endgeräten wie Virenschutz entstanden im Lauf der letzten Jahre umfassende technische und organisatorische Konzepte und Produkte der Endpoint Security [1]. Diese Weiterentwicklungen, Produkte der Kategorie Endpoint Detection and Response (EDR) oder darüber hinausgehend Extended Detection and Response (XDR), liefern eine detaillierte Sicht auf Vorgänge und mögliche Kompromittierungen auf den Arbeitsplatz-PCs von Mitarbeitern oder sogar auf Servern.

Zudem enthalten viele EDR-Produkte Funktionen für aktives Threat Hunting, also das Durchsuchen von Netzwerken nach möglichen Bedrohungen, und ermöglichen den Analysten im SOC (Security Operations Center), Alarme interaktiv auf verdächtigen Endgeräten zu verifizieren. Für ein Security Operations Center hat sich EDR damit zu einer der wichtigsten Komponenten entwickelt.

Gleichzeitig bieten fast alle Hersteller von EDR oder XDR zu ihren Lizenzen optional auch einen Managed Detection and Response Service (MDR) zum Überwachen und Betreiben der Produkte an, der sich zumindest in Teilbereichen als Konkurrenz zu einem klassischen extern betriebenen SOC positioniert. Das Management dieser Produkte läuft dabei in der Cloud des Herstellers und nicht mehr beim Kunden oder seinem Dienstleister.

EDR- und XDR-Produkte ändern damit den Markt und die etablierten Architekturen eines Security Operations Centers und ermöglichen neue Betriebsmodelle für ein SOC, bei dem der SOC-Dienstleister gar kein eigenes SIEM (Security Information an Event Management) mehr betreibt, sondern auf ein zentrales XDR-Management in der Cloud des Herstellers zugreift. Ob der Anbieter dies dann als dezidierten SOC-Service oder als MDR-Service bezeichnet, ist in der Praxis nur ein Unterschied im Marketing.

Wie war das noch gestern?

Der klassische Weg zur Überwachung sicherheitsrelevanter Ereignisse in einer Organisation besteht meist darin, alle Events von Betriebssystemen, Applikationen und Datenbanken, Sicherheitsgeräten wie Firewalls, VPN-Appliances und Authentisierungssystemen unterschiedlichster Hersteller an ein zentrales SIEM-System zu schicken. Dort werden die Events in ein gemeinsames Format gebracht und mithilfe von Regeln korreliert, um so bestimmte Detektionsszenarien zu erkennen, die man oft Use Cases nennt.

Typische Beispiele dafür sind Häufungen von falschen Passworteingaben, die auf einen Brute-Force-Angriff hindeuten könnten, oder Anmeldeversuche für einen Account von zwei geografisch weit auseinanderliegenden Orten innerhalb kurzer Zeit. Letzteres könnte darauf hindeuten, dass die Zugangsdaten zu einem Konto in falsche Hände geraten sind.

Anbieter von SOC-Services werben oft damit, dass ein Kunde „nur" alle seine Events an das SOC weiterleiten müsse und dort die Experten mit ihrem Fachwissen und einem SIEM mit Hunderten vorhandener Use Cases erkennen könnten, wenn etwas Gefährliches in der IT-Infrastruktur passiert (Abbildung 1).

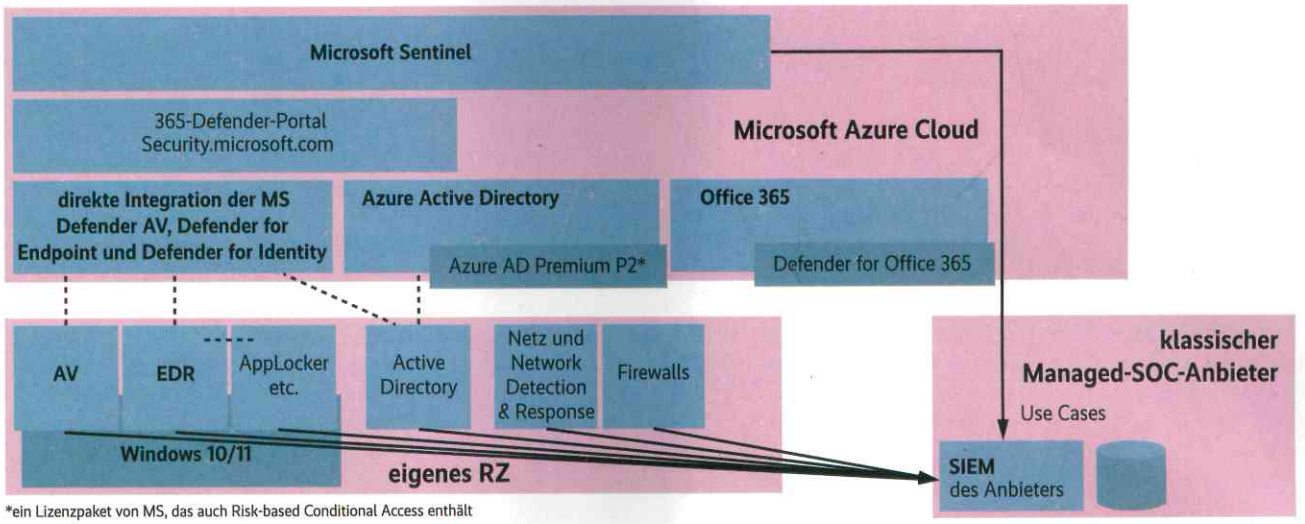
In der Praxis zeigt sich jedoch, dass allein das sogenannte Onboarding, also die Anbindung des Kunden an das SOC, die Abstimmung der Prozesse und die Weiterleitung aller Events an das SOC mehr als sechs Monate dauert. Hinterfragt man die angepriesenen Use Cases im Detail, stellt man fest, dass die meisten dieser Szenarien gar nicht zur Infrastruktur und den konkret vorhandenen Produkten des Kunden passen beziehungsweise dass die nötigen Ausgangsdaten für die individuellen Use Cases gar nicht vorhanden sind.

Nicht alles, was glänzt …

Das ungläubige Erwachen folgt spätestens dann, wenn ein externes Red Team die Leistung des SOC prüft und innerhalb weniger Tage nach Beginn der Angriffssimulation Domänenadministrationsrechte besitzt und die volle Kontrolle über das Netzwerk des Kunden erlangt hat, ohne dass das SOC davon etwas mitbekommen hat.

Ein Wechsel von einem SOC-Anbieter zu einem anderen ist machbar, aber mit

Klassisches externes SOC



*ein Lizenzpaket von MS, das auch Risk-based Conditional Access enthält

Im klassischen externen SOC werden alle Eventdaten gesammelt, korreliert und anhand der Erkennungsszenarien ausgewertet – die aufwendigen Vorbereitungen führen aber nicht immer zum Erfolg (Abb. 1).

hohem Aufwand und Kosten verbunden. Ein wechselwilliger Kunde muss nicht nur den Onboarding-Prozess ein weiteres Mal durchlaufen, alle Eventweiterleitungen umkonfigurieren und Prozesse neu abstimmen, sondern auch die für das Onboarding fälligen Gebühren beim neuen Anbieter bezahlen.

Der Aufbau eines eigenen SOC in der eigenen Infrastruktur ist gerade für mittelständische Kunden kaum eine Alternative, denn das Geld für die nötige Infrastruktur und das nötige Personal ist meist ebenso wenig vorhanden wie qualifiziertes Personal selbst. Anbieter, die ein SIEM in der Infrastruktur des Kunden per Remote-Zugriff betreiben, gibt es zwar, aber der Aufwand für den Betrieb verschiedener, nicht standardisierter SOC-Infrastrukturen von Kunden ist aufseiten des Dienstleisters nicht nur aufwendiger und ineffizienter, auch die Erkennungsqualität leidet oft darunter (Abbildung 2).

Anbieter von EDR- und XDR-Produkten versprechen eine effizientere Alternative zu dieser Situation. Bei EDR erfasst ein Softwareagent auf den Endgeräten und Servern das Verhalten aller Prozesse und meldet dieses Verhalten inklusive Kontext an ein zentrales Managementsystem. Bei XDR läuft das Managementsystem in der Cloud des Herstellers und integriert nicht nur die Informationen seines EDR-Produktes, sondern auch die anderen Sicherheitsprodukte des Herstellers. In der Regel geht es bei XDR auch nur um die Produkte eines einzigen Herstellers oder weniger ausgewählter Partner, sodass die Rohdaten und der Kontext der einzelnen Sicherheitsprodukte und Sensoren in einem gemeinsamen Management zusammenlaufen und ausgewertet werden können.

X-TRACT

- Die Weiterentwicklung der Endgerätesicherheit in den letzten Jahren ermöglicht neue Modelle für Security Operations Center und andere Dienstleister zur Angriffserkennung und -bekämpfung.
- Kranken die klassischen Sicherheitsauswertungen oft daran, dass Daten erst zentral an ein SIEM geschickt, korreliert und anhand häufig unzureichender Use Cases ausgewertet werden mussten, so ermöglichen die geschlossenen XDR-Systeme ein effizienteres Integrieren und Auswerten der Rohdaten.
- Das Microsoft-Defender-Universum als Beispiel einer XDR-Umgebung bietet hier einige Vorteile: SOC-Dienstleister, die Defender-Produkte des Kunden überwachen, können in der Umgebung des Kunden arbeiten, Zusatzfeatures nutzen und im Notfall auf die Endgeräte der Kunden zugreifen.
- Der Weg von offenen zu geschlossenen, effizienteren Systemen bietet zahlreiche Vorteile wie geringere Kosten oder bessere Datenlage. Dem stehen allerdings Nachteile wie das Befördern von Monokulturen entgegen.

Neue Techniken, neue Möglichkeiten

Im Gegensatz zu einem offenen SIEM, bei dem einzelne Events verschiedener Produkte und Hersteller ohne Kontext mit Regeln korreliert werden müssen, um den Kontext zu rekonstruieren oder zu erraten, ist eine XDR-Lösung ein proprietäres und geschlossenes System, was dem Hersteller ein viel effizienteres Integrieren der Rohdaten ermöglicht. Entsprechend muss ein XDR-Produkt nicht Hunderte von exotischen und meist gar nicht passenden Erkennungsszenarien vorhalten, sondern kann sich auf die herstellereigenen Produkte konzentrieren und beispielsweise auch gemeinsame Objektdatenbanken des Managementsystems nutzen.

XDR ist damit weniger offen und vom Umfang im Vergleich zu einem SIEM klar beschränkt. Für viele Unternehmen reicht der Umfang aber aus, insbesondere da mit der EDR-Komponente die Arbeitsplätze der Mitarbeiter gut abgedeckt sind und hier das Risiko einer Infektion oder Kompromittierung am größten ist.

Für den Betrieb ergeben sich bei diesem Weg andere Optionen als bei einem klassischen SOC, denn ein externer Dienstleister, der Alarme bewerten und verifizieren soll, muss keine eigene SIEM-Infrastruktur in einem eigenen abgesicherten Rechenzentrum aufbauen.

Zugriff auf das XDR-Management des Kunden, das ja in der Cloud des Herstellers für den Kunden bereitgestellt wird, reicht für seine Aufgaben weitgehend aus.

Viele EDR- oder XDR-Produkte enthalten auch Funktionen für Threat Hunting (also proaktive Schwachstellensuche), Ticketing oder sogar Automatisierung und Verwundbarkeitsmanagement. Ein externer Dienstleister kann damit fast alle Services abdecken, die auch ein klassisches SOC mit eigenem Rechenzentrum und SIEM sowie SOAR-Produkten (Security Orchestration, Automation and Response) anbietet. Die Grenzen von XDR werden jedoch dann erreicht, wenn beispielsweise Firewalls von anderen Herstellern oder Webapplikationen und Datenbanken in die Überwachung und Angriffserkennung integriert werden sollen, für die der XDR-Hersteller keine eigenen Produkte anbietet.

Daten auswerten, wo sie ohnehin sind

Am Beispiel von Microsoft kann man dieses Prinzip in sehr ausgeprägter Form betrachten: Die verschiedenen Defender-Produkte von Microsoft werden über die Azure-Cloud im Tenant des jeweiligen Kunden verwaltet. Defender Antivirus deckt dabei den klassischen Virenschutz auf den Endgeräten ab, Defender for Endpoint P2 ist die EDR-Komponente, die alle Aktivitäten auf den Endgeräten erfasst und grundlegendes Verwundbarkeitsmanagement ermöglicht, Defender for Identity erkennt Angriffe auf das interne Active Directory, Defender for Office 365 deckt Teams, SharePoint Online und Exchange Online ab und so weiter.

Da das Management all dieser Komponenten ohnehin in Azure und dem Tenant des jeweiligen Kunden stattfindet und auch alle Erkennungsszenarien dort zusammenlaufen, benötigt ein externer Dienstleister lediglich Zugriffsrechte auf den jeweiligen Azure-Tenant seiner Kunden (Abbildung 3).

Dieser Ansatz lässt sich sogar dann weiterverfolgen, wenn man über XDR hinausgehend zusätzlich zu den Microsoft-Defender-Produkten die Events von Drittsystemen wie internen Firewalls, Webapplikationen oder Sicherheitsprodukten anderer Hersteller in die Überwachung integrieren möchte. Dafür kommt bei Microsoft das Produkt Sentinel als SIEM-System in der Azure-Cloud ins Spiel.

Ein Unternehmen kann die Logdaten seiner Drittsysteme an Sentinel in seinem Azure-Tenant weiterleiten – ähnlich wie es dies im klassischen Betriebsmodell eines externen SOC an das SIEM des SOC-Dienstleisters geschickt hätte. Dafür fallen dann allerdings Zusatzkosten an, denn wie auch bei jedem anderen SIEM-System ist der Preis von Umfang und Speicherdauer der Events abhängig, die an das SIEM geschickt werden.

(Nicht nur) eine Frage des Preises

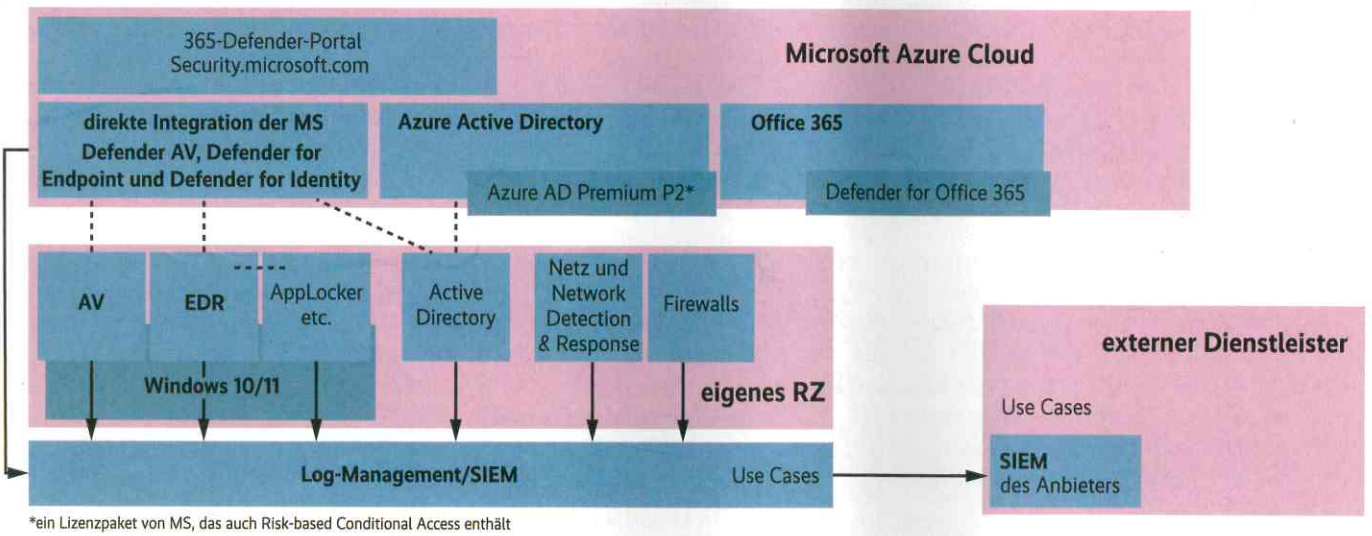
Hier sieht man einen interessanten Unterschied: Während bei einem klassischen SIEM-Ansatz alle Events an das SIEM weitergeleitet werden müssen und der Preis gerade aufgrund der Massen von Events auf den Endgeräten steigt, sind die Daten der verschiedenen Defender-Produkte von Microsoft ohnehin schon in der Azure-Cloud und dort auch für den Sentinel ohne Zusatzkosten verfügbar. Lediglich eine verlängerte Aufbewahrungsdauer und die zusätzlichen Datenquellen wie Firewalls oder interne Applikationen erhöhen die Lizenzkosten von Sentinel.

Ein externer SOC-Dienstleister, der seinen Service auf Basis von Microsoft Sentinel und der Microsoft-Defender-Reihe erbringt, kann über die ihm gewährten Zugriffsrechte auch eigene Use Cases konfigurieren, Threat Hunting durchführen und im Fall eines Sicherheitsvorfalls aktiv über den Defender for Endpoint auf betroffene Endgeräte seines Kunden zugreifen.

Falls das Unternehmen den Dienstleister wechseln möchte, ändert sich an der Weiterleitung der Events nichts, denn die Daten der Defender-Produkte waren und bleiben im eigenen Azure-Tenant des Kunden und auch die zusätzlichen Events werden weiterhin an Sentinel im eigenen Tenant geschickt. Ebenso wenig müssen sich die Konfiguration und individuelle Erkennungsszenarien ändern und bleiben im eigenen Sentinel vorhanden, wenn der Vertrag mit einem bisherigen Dienstleister gekündigt und stattdessen ein neuer beauftragt wird.

Ganz ohne Aufwand bleibt ein Dienstleisterwechsel in diesem Szenario den-

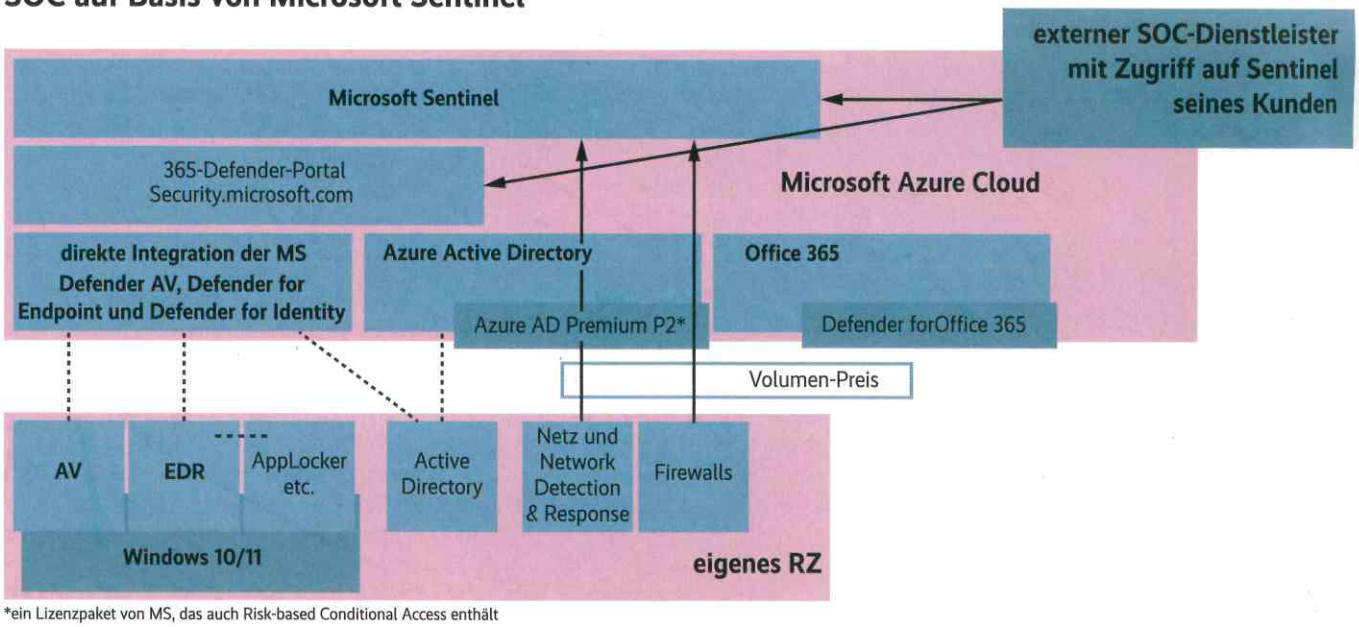
Eigenes SIEM mit externem Betrieb



*ein Lizenzpaket von MS, das auch Risk-based Conditional Access enthält

Nicht die beste Wahl: Der Remote-Zugriff des Dienstleisters auf die Kundeninfrastruktur ist umständlich und führt nicht immer zum gewünschten Ergebnis (Abb. 2).

SOC auf Basis von Microsoft Sentinel



*ein Lizenzpaket von MS, das auch Risk-based Conditional Access enthält

Die wahrscheinlich eleganteste Variante besteht in der Nutzung vorhandener Daten und Systeme durch den Dienstleister. Aber auch diese Methode ist nicht frei von Nachteilen (Abb. 3).

noch nicht, denn die Abstimmung der Prozesse und insbesondere der Umgang mit Alarmen und die angemessene Reaktion erfordert weiterhin einiges an Zusammenarbeit. Auf der technischen Seite jedoch vereinfacht XDR die Architektur und verringert die Abhängigkeit von Dienstleistern, während gleichzeitig die Abhängigkeit vom Hersteller der XDR-Lösung steigt.

In der Praxis ist diese Steigerung der Abhängigkeit von einem Hersteller oft gar nicht so spürbar, denn viele Organisationen haben bereits in der Vergangenheit versucht, sich auf wenige Lieferanten zu konzentrieren, um nicht in jedem Teilbereich der IT zahlreiche Managementkonsolen verschiedener Hersteller betreiben zu müssen. Auf der Seite der Hersteller ist der Trend zu XDR offensichtlich. Fast alle großen Anbieter von Sicherheitsprodukten sind auf den Zug aufgesprungen, bewerben ihre cloudbasierte XDR-Architektur und decken sowohl Endgeräte als auch Komponenten im Netzwerk ab. Die eigenen Produkte sind darin je nach Hersteller schon mehr oder weniger stark integriert und für Drittprodukte versuchen viele eine SIEM-Variante als Ergänzung in ihrer Cloud bereitzustellen.

Viele Vorteile – und ein Aber

Für die Kunden wäre es schön, wenn sich die XDR-Produkte in Zukunft weiter öffnen würden und man so ein gemeinsames Management und eine gemeinsame Überwachung und Erkennung von Kompromittierungen direkt in der Cloud der Hersteller erreichen könnte, ohne dafür zusätzliche SIEM- oder SOAR-Produkte zu benötigen. Tatsächlich bewerben auch einzelne Hersteller eine offene XDR-Lösung, die in der Lage ist, zahlreiche Produkte von anderen Herstellern in der Cloud zu integrieren. Oft fehlen dabei jedoch das gemeinsame übergreifende Management und die native Integration der Rohdaten der einzelnen Produkte.

Offenes XDR entpuppt sich dann als SIEM in der Cloud, bei dem nur die Events der einzelnen angebundenen Drittprodukte korreliert werden. Entsprechend skaliert auch der Preis der Lösung mit den Events von allen Datenquellen, und zu den einzelnen bereits vorhandenen Herstellern kommt ein zusätzlicher Cloud-SIEM-Hersteller hinzu. Zudem ist der Betrieb einer solchen Architektur aufwendiger als bei einer proprietären XDR-Architektur, denn die einzelnen Sicherheitsprodukte haben nach wie vor ihre eigene Managementkonsole.

Welcher Weg der richtige oder sogar der beste ist, kommt auf das einzelne Unternehmen an. Wer Wert auf Herstellerunabhängigkeit und einen klassischen „Best of Breed"-Ansatz legt, bei dem man ein EDR-System unabhängig von der AD-Security-Überwachung, den Firewalls und der Virenschutzlösung auswählt, der wird mit einer proprietären XDR-Architektur nicht glücklich. In diesem Fall ist ein klassisches SIEM oder ein offenes XDR-Produkt, das im Kern ein SIEM in der Cloud ist, naheliegend.

Für viele nicht ganz so große Unternehmen ist dieser Ansatz jedoch zu komplex und nicht bezahlbar. Hier bietet der proprietäre XDR-Weg interessante Perspektiven. Die Architektur wird einfacher und die Abhängigkeit von einem externen Dienstleister für den Betrieb sinkt. Gleichzeitig steigt aber auch die Fokussierung auf den Hersteller des XDR-Produkts und damit die Abhängigkeit von dieser Firma. Im Fall von Microsoft kann dies zu einer sehr starken Monokultur führen, wenn die Organisation sowohl die Betriebssystemplattform Windows als auch die Office-Produkte, die präventiven Sicherheitsprodukte und darüber hinaus die Sensoren und das SIEM zur Zusammenfassung aller Events von Microsoft bezieht. Ob man so eine Architektur als Problem oder als Chance für die IT-Sicherheit sieht, ist sicherlich Geschmackssache. (ur@ix.de)

Quellen

Konstantin Bücheler, Martin Hartmann, Alain Rödel, Stefan Strobel; Auf dem Radar; Endpoint Detection and Response: Gefahren schnell erkennen und reagieren; iX 11/2021, S. 52

STEFAN STROBEL

ist Buchautor sowie Gründer und Geschäftsführer des IT-Sicherheitshauses cirosec.