Erkennen und reagieren

Neue Verteidigungsansätze: EDR und XDR

Endpoint und Extended Detection and Response (EDR, XDR) sollen kompromittierte Systeme erkennen und die Incident Response unterstützen. Was leisten diese noch jungen Techniken wirklich?

Prominente Sicherheitsvorfälle wie der Hackerangriff Sunburst auf zahlreiche Institutionen verdeutlichen die Grenzen heutiger IT-Sicherheitsmaßnahmen eindrucksvoll. In diesem Fall drangen Hacker bei der Firma SolarWinds ein und bauten dort unbemerkt eine Malware in die gemeinsame Plattform der IT-Produkte von SolarWinds ein. Kunden von SolarWinds wurden daraufhin durch das Einspielen von Updates für die SolarWinds-Produkte mit dieser Malware infiziert und ihre Firewalls, AV-Suiten oder andere Sicherheitsprodukte hatten keine Möglichkeit, dies zu erkennen oder zu verhindern, da die Administratoren das Update bewusst eingespielt und ihm vertraut hatten.

Dieses und viele andere Beispiele zeigen, dass präventive Sicherheitsmaßnahmen allein nicht ausreichen, um die eigene Organisation vor Angriffen zu schützen. Bei einem professionellen und motivierten Angreifer ist es nur eine Frage der Zeit, wann dieser erfolgreich in das anvisierte Unternehmen einbrechen kann. Die Fähigkeit, Kompromittierungen in der eigenen Infrastruktur frühzeitig zu erkennen und darauf zu reagieren, wird daher immer wichtiger.

Prävention allein reicht nicht

Das bedeutet selbstverständlich nicht, dass Prävention ihre Bedeutung verliert, weil ohne umfassende Maßnahmen zum Verhindern von Malware- und Hackereinbrüchen der Betrieb von Erkennungsprodukten gar nicht machbar wäre. Denn sonst übersteigt die Anzahl der Alarme, die analysiert beziehungsweise verifiziert werden müssen, die Manpower, die eine Organisation sich leisten kann – vom Aufwand und den Kosten zur Wiederherstellung und Bereinigung nach Vorfällen ganz zu schweigen. Eine solide Prävention ist daher eine notwendige Voraussetzung, um sich Erkennung und Reaktion wirklich leisten zu können.

Vor zwanzig Jahren hofften die Unternehmen, Angreifer mit sogenannten Intrusion-Detection-Systemen (IDS) erkennen zu können. Dies hat sich leider in den meisten Fällen als nicht praktikabel herausgestellt. Zu viele Fehlalarme brachten den Betriebsaufwand in eine unwirtschaftliche Zone.

Danach versuchte man, durch den Einsatz von Security-Information-and-Event-Management-Systemen (SIEM) im Unternehmen verschiedenste Events zu korrelieren, um eine bessere Erkennung zu erreichen. Aber auch hier zeigte sich, dass das Verhältnis zwischen Aufwand und Nutzen viele Unternehmen abschreckte. Vor allem kleinere Unternehmen entschieden meist für sich, ein solches Produkt auf gar keinen Fall selbst zu betreiben, sondern allenfalls als Service von einem externen Dienstleister einzukaufen.

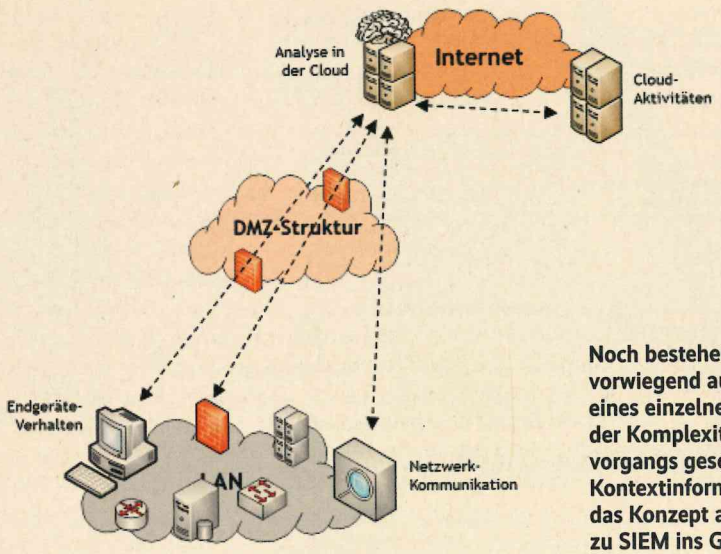
Größere Unternehmen, die bereits ein SIEM aufgebaut haben, oder Anbieter, die eines für ihre Kunden betreiben, stehen vor der Herausforderung, dass das Überprüfen der Alarme des Systems sehr viel Zeit benötigt und sich immer wieder die Frage stellt, was auf einem betroffenen Endgerät tatsächlich passiert ist.

Besserung durch EDR und XDR

In den letzten Jahren kamen dann neue Techniken auf den Markt, die unter dem Namen „Endpoint Detection and Response" (EDR) oder „Extended Detection and Response" (XDR) Abhilfe versprechen. EDR-Lösungen werden auf den Endgeräten installiert und beobachten dort zunächst das Verhalten aller Prozesse. Dabei geht es nicht um das Verhalten der Anwender, sondern um technische Vorgänge wie den Zugriff auf Dateien, Registry, Kommunikation, das Starten von Prozessen, Manipulationen am Speicher von Prozessen und vieles mehr.

All diese Aktionen werden im Gesamtbild betrachtet, meist auch unter Verwendung moderner KI-Methoden. Entdecken die Sicherheitsprofis hierbei ein Verhaltensmuster, das auf das Vorhandensein von Malware oder auf Hacker hindeutet, wird ein Alarm ausgelöst. Im Gegensatz zu einem SIEM-Produkt, dem meist sehr viel weniger Details zu Verfügung stehen, hat ein EDR-Werkzeug die Information aller Details des Endgeräts im Zugriff und kann sie im Gesamtkontext bewerten.

Beispielsweise stehen Informationen zur Verfügung, woher ein ausführbares bösartiges Programm kam, wer es gestartet, auf welchen Server es zugegriffen und welche Dateien es geschrieben hat. Für diese Informationen muss kein Analyst manuell Regeln definieren und immer wieder anpassen, um



Noch bestehen XDR-Lösungen vorwiegend aus Komponenten eines einzelnen Herstellers, was der Komplexität des Integrationsvorgangs geschuldet ist. Dank der Kontextinformationen bringt sich das Konzept aber als Alternative zu SIEM ins Gespräch.

dann den Kontext zu rekonstruieren, soweit dies überhaupt möglich ist. Eine EDR-Software stellt solche Zusammenhänge automatisch her, da sie auf dem betroffenen Endgerät läuft und alle Details kennt.

Damit kann EDR Kompromittierungen auf Endgeräten genauer und zuverlässiger erkennen als frühere Ansätze. Organisationen, die EDR eingeführt haben, um damit die Alarme eines SIEMs zu verifizieren, stellen fest, dass das EDR nicht nur zur Verifikation wertvoll ist, sondern eine primäre Quelle für die Erkennung wird.

Funktionen für die Reaktion auf Vorfälle

EDR-Produkte beobachten und korrelieren aber nicht nur das Verhalten der Prozesse auf dem Endgerät. Wie der Name bereits suggeriert, bieten sie auch Funktionen zur Reaktion auf Vorfälle. Diese variieren je nach Produkt und Hersteller vom aktiven Eingreifen zum Stoppen bösartiger Prozesse, dem Zurückrollen von Modifikationen, die eine Malware vorgenommen hat, bis zu einem interaktiven Zugriff auf das betroffene System für den Incident-Response-Fall. Die Grenze zwischen einem Werkzeug für die Erkennung und einem Werkzeug für Incident Response und Live-Forensik verschwimmen dabei.

Auch die aktive oder automatisierte Suche nach Indikatoren für eine Kompromittierung (IoCs), die oft als „Hunting" bezeichnet wird, ist eine Funktion, die viele EDR-Werkzeuge unterstützen. Die Hersteller bieten dazu entweder eigene Threat-Intelligence-Feeds an, über die Hashwerte bekannter Malware-Dateien, IP-Adressen von Command-and-Control-Servern (C&C) oder Registry-Einträge von Malware geliefert werden, oder sie bieten Schnittstellen, über die eigene beziehungsweise öffentliche Threat-Intelligence-Quellen eingebunden werden können. Auch in diesem Punkt beginnen EDR-Werkzeuge, sich mit einem SIEM zu überschneiden.

Die Anbieter von EDR waren wie so oft in der Securitybranche zunächst kleine Start-ups, die dynamisch und innovativ neue technische Ideen implementierten. Die großen, etablierten Hersteller von Endpoint-Security-Produkten sind dabei meist etwas schwerfälliger oder sie kaufen Start-ups auf und erweitern so ihre Produktsuiten. Es ist naheliegend, dass ein großer Anbieter im nächsten Schritt versucht, die zugekaufte EDR-Software in bestehende Produkte zu integrieren, sodass beispielsweise ein Alarm aus einer bestehenden Netzwerkanomalieerkennung automatisch vom EDR-Produkt verifiziert wird.

Aber nicht nur große Hersteller von Sicherheitsprodukten verfolgen die direkte Integration von Sensoren an verschiedenen Stellen. Auch kleine Start-ups haben von Anfang an diese Integration mit eigenen, neu entwickelten Sensoren verfolgt. Neben dem Endgerät ist dabei das Einbinden eines Netzwerksensors oder auch von Sensoren für Aktivitäten in Cloud-Umgebungen und Containern naheliegend.

Ein X für erweitertes EDR

Um die eigenen integrierten Produkte von denen der Konkurrenz abzugrenzen, entstand dabei die Bezeichnung Extended Detection and Response (XDR). XDR ist damit die naheliegende Weiterentwicklung von EDR. Hersteller, die neben einem EDR-Produkt auch Erkennungstechniken im Netzwerk oder sogar in weiteren Bereichen im Portfolio haben, tendieren fast alle dazu, dies als XDR zu bewerben. In einzelnen Fällen wird XDR dabei anders ausgeschrieben und das „X" statt als „Extended" als „Cross-Layer" (schichtenübergreifend) übersetzt. Das soll deutlich machen, dass Erkennung und Reaktion auf verschiedenen Ebenen stattfinden.

Bisher gibt es kein Produkt, das XDR mit Werkzeugen unterschiedlicher Hersteller ermöglicht. Bei XDR geht es eigentlich immer um die Integration eines einzelnen Herstellers. Das ist aber auch verständlich, denn die nötige Integration ist weitaus komplexer als nur das Zusammenfassen einzelner Events. Um wirklichen Mehrwert zu erzeugen, müssen die Einzelteile einer XDR-Lösung eng verzahnt sein, Informationen mit Kontext austauschen und aktiv zusammenarbeiten.

Alternative zum klassischen SIEM

XDR wird damit noch viel deutlicher eine Alternative zum klassischen SIEM-Ansatz, der Events ohne Kontext korreliert, um daraus den Kontext zu rekonstruieren. Auch bei der Automatisierung sieht man die Überlappung und die Gegensätze. SIEM-Lösungen werden oft mit Funktionen oder Tools für „Security Orchestration, Automation and Response"

Anbieterübersicht zu Endpoint Detection and Response (EDR) und Extended Detection and Response (XDR)

Hersteller	Produkt	Link
Cisco	SecureX	https://www.cisco.com/c/de_de/products/security/what-is-secureX.html
CrowdStrike	eXtended Detection & Response	https://www.crowdstrike.de/
Cynet	Cynet 360	https://www.cynet.com/platform/
Fidelis	Fidelis Elevate XDR	https://fidelissecurity.com/products/elevate/
FireEye	FireEye Mandiant Advantage	https://www.fireeye.de/
Fortinet	Fortinet Security Fabric	https://www.fortinet.com/de/solutions/enterprise-midsize-business/enterprise-security
Kaspersky	Kaspersky Managed Detection and Response	https://www.kaspersky.de/enterprise-security/managed-detection-and-response
MacAfee	McAfee MVision	https://www.mcafee.com/enterprise/de-de/solutions/xdr.html
Microsoft	Azure Defender/Microsoft 365 Defender	https://www.microsoft.com/de-de/security/business/threat-protection
Palo Alto	Cortex XDR	https://www.paloaltonetworks.de/cortex
SentinelOne	XDR Marketplace	https://de.sentinelone.com/
Sophos	Intercept X	https://www.sophos.com/en-us/solutions.aspx
Trend Micro	Trend Micro Vision One	https://www.trendmicro.com/de_de/business/products/detection-response.html

(SOAR) ergänzt, um nicht nur Alarme und manuelle Arbeit zu erzeugen, sondern bei einem Alarm automatisch Aktionen für das Anreichern mit Zusatzinformationen, das Verifizieren oder die Reaktion anzustoßen.

Wie schon bei SIEM muss auch SOAR dies für zahlreiche Produkte unterschiedlicher Hersteller leisten und dabei die Schnittstellen bei jeder Änderung eines Drittprodukts aktualisieren. Beim XDR-Ansatz kommen die Teilprodukte eines einzelnen Herstellers zusammen, der die Schnittstellen selbst bereitstellt und kontrolliert. Der Integrationsaufwand fällt daher beim Hersteller und Entwickler selbst an und nicht beim Kunden, der seine SIEM- und SOAR-Produkte selbst konfigurieren muss.

Neben der Software bieten einige Hersteller auch gleich den Betrieb von EDR- oder XDR-Produkten zusammen mit der Dienstleistung für die Reaktion auf Vorfälle an und titulieren dies dann als „Managed Detection and Response" (MDR), wobei dieser Begriff je nach Anbieter ganz unterschiedlich interpretiert werden kann. Man findet sowohl Anbieter, die eine EDR- oder XDR-Lösung als MDR betreiben, als auch solche, die nur Logdaten mit einem SIEM auswerten und darauf reagieren wollen.

Die zentrale Intelligenz und Verwaltung einer XDR-Lösung ist fast immer in der Cloud des Herstellers angesiedelt. Dies passt zu der Intention, den Aufwand weitgehend beim Hersteller zu belassen und den Betrieb von XDR für den Kunden so einfach wie möglich zu gestalten.

Alles aus einer Hand?

Für den Kunden stellt sich damit vor allem die Frage, inwieweit er sich von einem einzelnen Hersteller abhängig machen möchte und wie viel Geld und Aufwand es ihm wert ist, einzelne Produkte verschiedener Hersteller selbst zum Zusammenspielen zu bringen – die klassische Diskussion über die Ansätze „Best of Breed" versus „One Vendor".

Im Fall von XDR bekommt die Diskussion jedoch eine größere Bedeutung, denn bisher war der Betrieb einer Firewall von Hersteller A mit dem Mail-Relay von Hersteller B und den Authentisierungstoken von Hersteller C keine große Sache. Ein SIEM und vielleicht sogar noch eine SOAR-Lösung dazu selbst aufzubauen und zu betreiben, ist dagegen für viele Organisationen nicht machbar, und auch entsprechende Managed-Service-Angebote sind sehr teuer und oft nicht so effektiv wie gewünscht.

XDR als „Out-of-the-Box"-Produkt aus der Hand eines einzelnen Herstellers, bei dem die verschiedenen Sensoren aufeinander abgestimmt sind und automatisch zusammenarbeiten, ist auf der einen Seite eine interessante Perspektive. Einige Hersteller gehen sogar noch weiter und integrieren nicht nur Techniken zur Erkennung von Kompromittierungen, sondern auch Schwachstellenmanagement, um unsichere Fehlkonfigurationen oder fehlende Patches zu erfassen und in das Gesamtbild einfließen zu lassen. Durch die starke und automatische Integration, die deutlich weniger Fehlalarme zur Folge hat, sowie die Bereitstellung der zentralen Komponente in der Cloud des Herstellers wird bei solchen Lösungen ein Eigenbetrieb für viele Organisationen attraktiv.

Auf der anderen Seite macht sich ein Unternehmen durch die Einführung eines XDR-Produkts noch stärker von einem einzelnen Hersteller abhängig. Das mag noch harmlos sein, wenn XDR nur aus einer Endpoint-Software und zusätzlichen Netzwerksensoren besteht. Wenn aber XDR voraussetzt, dass auch die Firewall sowie das Web- und Mail-Gateway vom gleichen Hersteller kommen oder sogar das Betriebssystem der Endgeräte, dann entsteht eine Abhängigkeit und Monokultur, die kritisch zu bewerten ist.

Beim eingangs erwähnten Angriff über SolarWinds wären Kunden einiger EDR-Werkzeuge schon deshalb nicht betroffen gewesen, weil die dort verwendete Malware zunächst anhand einer langen Liste geprüft hätte, ob EDR- oder Forensikwerkzeuge auf dem Zielsystem installiert sind, und gegebenenfalls keine Infektion durchgeführt hätte. Das zeigt, dass auch aus Sicht der Malware-Autoren EDR- und XDR-Werkzeuge geeignet sind, irreguläre Aktivitäten frühzeitig aufzudecken.

Schlussfolgerung

So attraktiv die Idee von XDR auch klingen mag, in der Realität ist das Konzept relativ jung und die Produkte entwickeln sich noch stark weiter. So kommt es vor, dass die effektive Erkennungsleistung eines XDR-Tools trotz konzeptioneller Versprechungen in der Praxis nicht an die Erkennungsleistung eines guten EDR-Werkzeugs herankommt. Die Kombination von schwächeren Einzelteilen führt eben nicht automatisch zu einem stärkeren Gesamtprodukt. Oder es kommt vor, dass die Erkennungsleistung der EDR-Lösung zwar überraschend gut ist, aber die Management-Oberfläche so wirr und unübersichtlich aufgebaut ist, dass man in der Praxis nicht damit arbeiten möchte.

Trotz aller konzeptionellen Vorzüge der Idee hinter XDR kommt es deshalb auf die tatsächliche Produktqualität im Einzelfall an. Um diese zu testen, benötigt eine Organisation jedoch meist die Unterstützung von Experten, die während der Testphase realistische Angriffe simulieren. Das einfache Starten von ein paar Malware-Samples oder Exploits in einer Testumgebung sagt wenig aus.

Zudem ist der Markt jung und in Bewegung, sodass zu erwarten steht, dass kleinere Anbieter von größeren Herstellern aufgekauft und integriert werden und sich dabei die Produktstrategie ändert. Wie man am Beispiel Aviras, eines der größten AV-Hersteller, gesehen hat, kann dies jedoch auch bei großen und etablierten Anbietern passieren. (ur@ix.de)

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