eBOOK

www.security-insider.de

SECURITY INSIDER

Evolution der Endpoint-Sicherheit

Herkömmlicher Schutz reicht nicht mehr aus

Möglichkeiten und Schwächen von EDR

XDR ist der Endpoint-Schutz der Zukunft

Powered by:

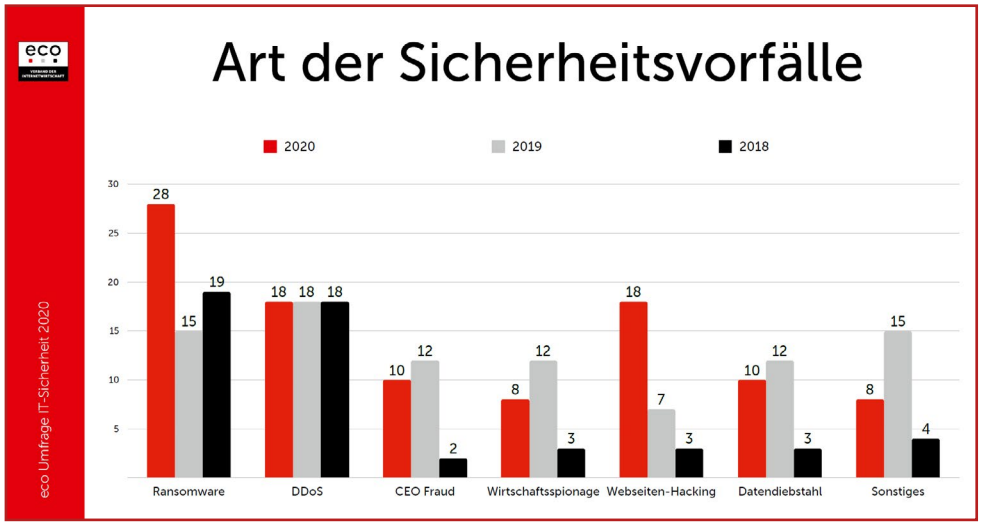
SentinelOne

Inhalt

Vogel IT-Medien GmbH
Max-Josef-Metzger-Str. 21
86157 Augsburg
Telefon +49 (0) 821/2177-0
E-Mail redaktion@security-insider.de
Web www.Security-Insider.de
Geschäftsführer: Werner Nieberle
Chefredakteur: Peter Schmitz, V.i.S.d.P.,
peter.schmitz@vogel-it.de
Erscheinungstermin: Januar 2021
Titel: Production Perig/stock.adobe.com

Endpoint Protection Platforms reichen nicht mehr aus

Viele Unternehmen unterschätzen die Risiken für Endpoints, sie halten ihre Endpunkte für gut geschützt und konzentrieren sich auf den Schutz der Cloud-Daten. Tatsächlich aber werden Endpoints durch neuartige Risiken bedroht, für die der klassische Endpunkt-Schutz nicht ausreicht. Die Endpoint Security muss sich dringend verändern.



Laut eco IT-Sicherheitsstudie 2020 gab es in fast jedem dritten Unternehmen (28 Prozent) im letzten Jahr mindestens einen gravierenden Sicherheitsvorfall. Meist handelte es sich dabei um Attacken mittels Ransomware. (Bild: eco)

Ausgaben für IT-Sicherheit steigen, aber auch die Schäden

Der Markt für IT-Sicherheit brachte im Jahr 2020 Umsatzrekorde. So wurden in Deutschland rund 5,2 Milliarden Euro für Hardware, Software und Services im Bereich IT-Sicherheit ausgegeben, 5,6 Prozent mehr als im bisherigen Rekordjahr 2019. Für das Jahr 2021 ist ein weiteres Wachstum um 9,3 Prozent auf 5,7 Milliarden Euro prognostiziert, so Berechnungen der Marktforscher von IDC im Auftrag des Digitalverbands Bitkom.

Gleichzeitig erleiden Unternehmen in Deutschland aber immer größere Schäden durch erfolgreiche Cyberattacken. Laut Bitkom entsteht der deutschen Wirtschaft durch Sabotage, Datendiebstahl oder Spionage jährlich ein Schaden von mehr als 100 Milliarden Euro. Drei von vier Unternehmen (75 Prozent) sind in den vergangenen zwei Jahren Opfer geworden, jedes achte Unternehmen (13 Prozent) vermutet dies.

Diese Entwicklung lässt zwei Schlüsse zu: Zum einen kann es Differenzen geben zwischen den tatsächlichen Bedrohungen und der Security-Strategie der Unternehmen. Zum anderen könnten Sicherheitslösungen zum Einsatz kommen, die nicht den gewünschten Schutz bieten, da sie neuartige Cyberattacken nicht erkennen und abwehren können.

Die Praxis zeigt: Beide Annahmen sind richtig, sowohl die Strategien der Unternehmen müssen verändert werden als auch die eingesetzten Schutzkonzepte.

Endpoints sind im Fokus der Cyberattacken

Befragt man Unternehmen in Deutschland nach der Sicherheit ihrer Endpunkte, so stufen die meisten ihre Endpoint Security als vollständig und erfolgreich ein, denn sie vertrauen auf den klassischen Schutz wie Anti-Virus und Firewall. Betrachtet man aber, welche Cyberangriffe die Unternehmen erleiden und nicht erfolgreich und schnell genug abwehren können, stellt man fest:

- Jedes fünfte Unternehmen (21 Prozent) musste feststellen, dass sensible digitale Daten abgeflossen sind, bei 17 Prozent wurden Informations- und Produktionssysteme oder Betriebsabläufe digital sabotiert.
- Bei jedem achten Unternehmen (13 Prozent) ist die digitale Kommunikation ausgespäht worden.
- Weiter auf dem Vormarsch ist das sogenannte Social Engineering. Dabei werden Mitarbeiter manipuliert, um an sensible Informationen zu kommen, mit denen dann in einem weiteren Schritt zum Beispiel Schadsoftware auf die Firmenrechner gebracht werden kann. Mehr als jedes fünfte Unternehmen (22 Prozent) war davon betroffen.

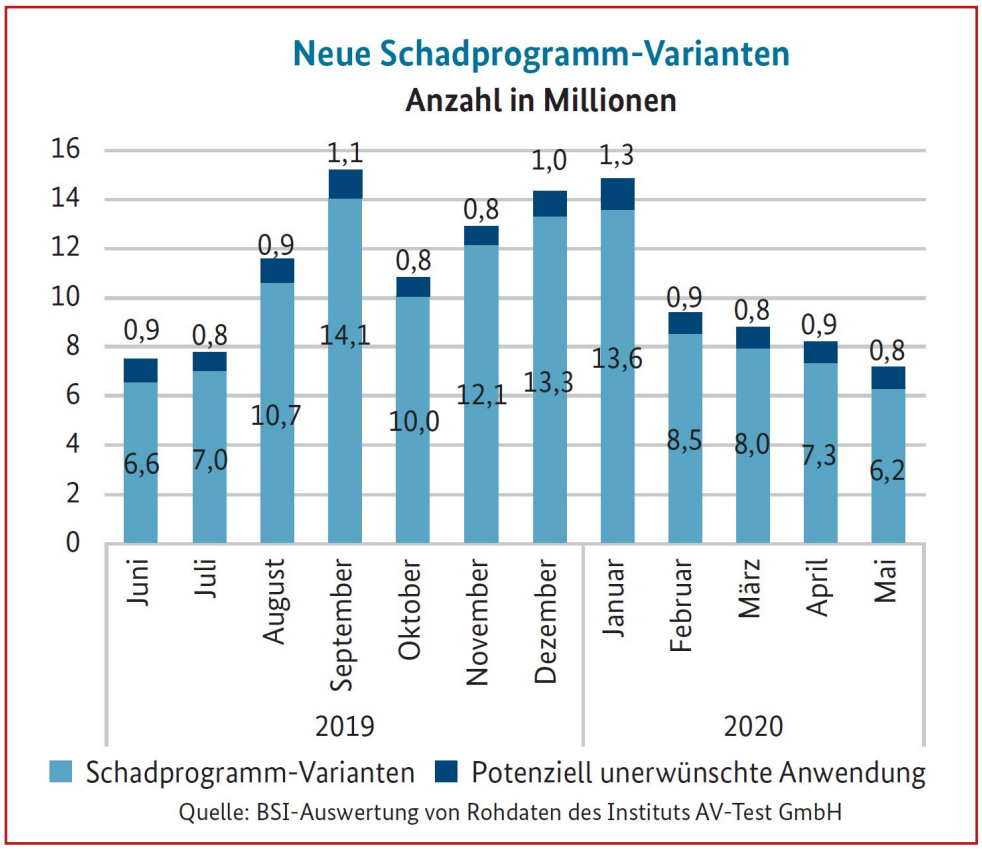
Auch der Verband der Internetwirtschaft eco berichtet von erfolgreichen Cyberattacken, die die Unternehmen in Deutschland erleiden. Laut eco IT-Sicherheitsstudie 2020 gab es in fast jedem dritten Unternehmen (28 Prozent) im letzten Jahr mindestens einen gravierenden Sicherheitsvorfall. Das sind zwei Prozent mehr als noch ein Jahr zuvor. Meist handelte es sich dabei um Attacken mittels Ransomware (28 Prozent).

Solche Cyberangriffe, von denen die Bitkom- und eco-Studien berichten, betreffen sämtlich direkt oder indirekt die Endpoints der Unternehmen: Entweder

Die 15 Top-Bedrohungen, die die EU-Agentur für Cybersicherheit ENISA ermittelt hat, richten sich alle direkt oder indirekt gegen Endpunkte. Das ist nicht verwunderlich, stellen Endpoints doch die wesentliche Schnittstelle hin zu den Nutzern und ihren Daten dar. (Bild: ENISA)

werden Daten auf den Endpoints selbst zwangsverschlüsselt, gestohlen oder ausgespäht oder die Angriffe nutzen unzureichend geschützte Endpunkte als Einfallstor für Datendiebstahl, Online-Erpressung und Schädigung der IT-Infrastrukturen.

Die Security-Investitionen und die Security-Strategien haben aber andere Bereiche im Fokus als die Angreifer, zum Beispiel den Schutz der Daten in der Cloud. So ergab zum Beispiel die eco IT-Sicherheitsstudie 2020, dass der Anstieg der Internetkriminalität und Cloud Computing die beiden größten Treiber für Veränderungen in der Security sind.



Im Berichtszeitraum sind laut BSI 117,4 Millionen neue Schadprogramm-Varianten hinzugekommen, somit etwa 320.000 neue Schadprogramme pro Tag. (Bild: BSI)

Dabei können auch Bereiche wie die Cloud-Sicherheit ohne eine funktionierende Endpoint-Sicherheit nicht bestehen, denn Endgeräte liefern die Zugänge zu den Clouds und Cloud-Daten.

Endpunkt-Risiken wandeln sich, der Endpunkt-Schutz muss dies auch tun

Es reicht nicht mehr aus, wenn alle Endpunkte im Unternehmen über einen klassischen Anti-Viren-Schutz und eine Firewall verfügen. Die klassischen Endpoint Protection Plattformen (EPP) haben sich zwar weiter entwickelt und basieren schon lange nicht mehr nur auf einer signaturbasierten Erkennung, bei der neue Schadsoftware so lange nicht erkannt werden kann, bis sie auch im Signatur-Update berücksichtigt ist. EPP arbeitet auch mit einer verhaltensbasierten Schutzfunktion, die jedoch alleine nicht ausreicht, um die neuartigen Angriffe zu erkennen.

So berichtet das Bundesamt für Sicherheit in der Informationstechnik (BSI) im neuen „Bericht zur Lage der IT-Sicherheit in Deutschland 2020" davon, dass die aktuelle Gefährdungslage geprägt ist von Cyber-Angriffen mit Schadsoftware, die in immer neuen Varianten und mit teils ausgefeilten Methoden eingesetzt wird. Die Zahl der Schadprogramme übersteigt demnach inzwischen die

Milliardengrenze. Allein im Berichtszeitraum sind laut BSI 117,4 Millionen neue Varianten hinzugekommen, somit etwa 320.000 neue Schadprogramme pro Tag.

Auch die Gefahr durch Erpresser-Malware (Ransomware) wandelt sich: Daten werden immer öfter nicht nur verschlüsselt, sondern von Cyber-Kriminellen kopiert und ausgeleitet. Die Angreifer drohen zusätzlich damit, die Daten an Interessenten zu verkaufen oder zu veröffentlichen. Damit erhöhen die Angreifer den Druck auf die Opfer, der Lösegeldforderung nachzukommen.

Beispiel: Dateilose Malware

Warum die klassische Suche nach verseuchten Dateien und Schadprogrammen mittels Endpoint Protection Platforms nicht mehr ausreichen kann, zeigen eindrucksvoll neuartige Bedrohungen wie Fileless Malware, also dateilose „Schadsoftware". Tatsächlich handelt es sich bei Fileless Malware um keine schädlichen Dateien oder Programme, deren Signatur man erkennen oder deren bösartiges Verhalten man ermitteln könnte.

Fileless Malware stellt eine Angriffstechnik auf Endpoints dar, bei der legitime Programme und Funktionen wie Administratorwerkzeuge genutzt werden, um bösartige Handlungen auszuführen und geschickt zu verschleiern.

Erst die kriminelle Kombination aus den missbrauchten legitimen Tools macht den Angriff aus, die einzelnen Programme, Module und Funktionen sind selbst nicht bösartig und werden auch nicht ohne weiteres als solches erkannt. Auch das Verhalten eines einzelnen Tools ist meist nicht auffällig, erst die Abfolge der einzelnen Schritte, die die Angreifer mit den legitimen Werkzeugen durchführen, macht die Attacke aus und könnte einen Hinweis auf die Bedrohung liefern.

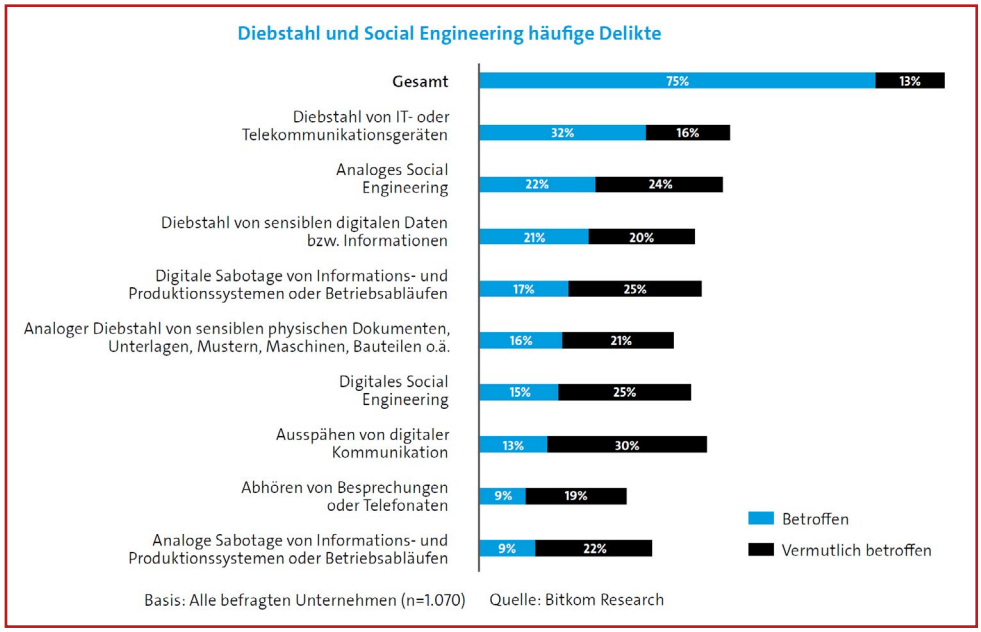
Doch klassischer Endpoint-Schutz kann solche Bedrohungsanalysen nicht durchführen, die mehrstufigen Attacken werden nicht rechtzeitig oder gar nicht erkannt. Erst die Folgeschäden fallen auf, wenn es schon zu spät ist für Gegenmaßnahmen.

Endpoint Security muss sich deshalb wandeln, um den sich verändernden Bedrohungen begegnen zu können. Möglich wird dies durch die Entwicklung hin zu EDR (Endpoint Detection and Response) und XDR (Extended Detection and Response), welche im Folgenden betrachtet werden.

Oliver Schonschek

Die Abwehr muss um Erkennung und Response erweitert werden

Viele Cyberangriffe auf Endpoints haben trotz klassischem Endpunkt-Schutz Erfolg und bleiben für längere Zeit unentdeckt. Es reicht nicht, wenn sich Unternehmen auf Endpoint Protection verlassen. Angriffe müssen im Erfolgsfall erkannt und die Folgeschäden abgemildert werden. Möglich wird dies durch Endpoint Detection and Response (EDR).



Die deutsche Wirtschaft wird erfolgreich aus dem Cyberraum angegriffen, wie eine Bitkom-Umfrage zeigt. Ein Endpoint-Schutz alleine ist deshalb nicht ausreichend. Die erfolgreichen Angriffe, die den Schutz überwinden, müssen entdeckt und die Folgeschäden gemindert werden. (Bild: Bitkom)

Erfolgreiche Endpoint-Attacken früher erkennen

Eigentlich ist es in der Security gut bekannt, dass es keine Frage ist, ob man als Unternehmen aus dem Cyberraum angegriffen wird, sondern nur, wann dies passieren wird. Ebenso sollte es keine Überraschung sein, dass es keinen hundertprozentigen Schutz in der Endpoint Security geben kann – zu vielfältig sind die Angriffsmöglichkeiten.

Trotzdem enden viele Konzepte für Endpunkt-Schutz mit der Protection, also der Abwehr von Angriffen, an eine Erkennung erfolgreicher Attacken und an die notwendige Antwort zur Eindämmung der Folgeschäden wird zu wenig gedacht.

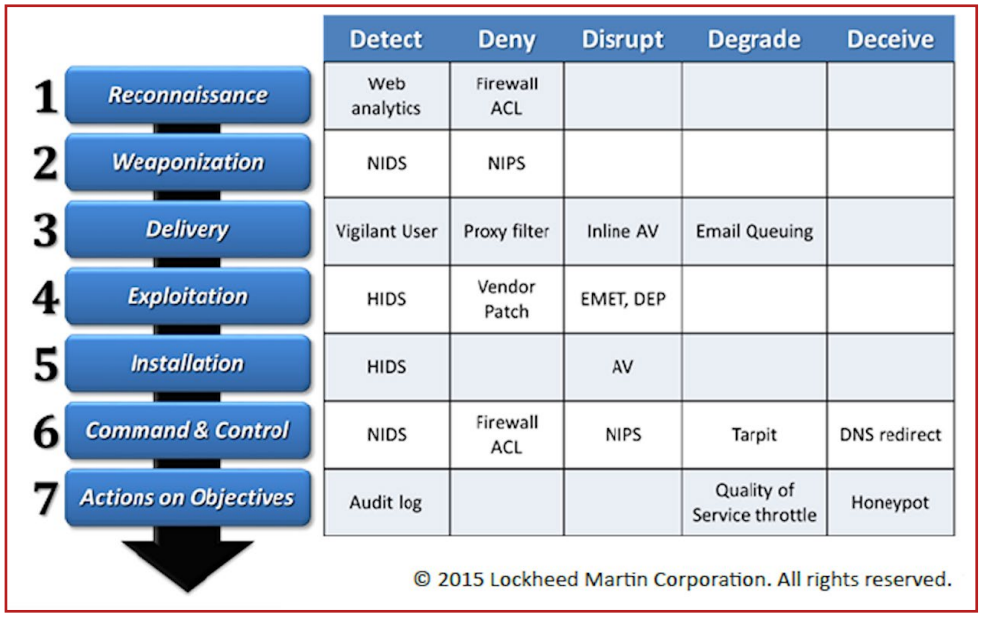
Der klassische Endpunkt-Schutz muss deshalb um Endpoint Detection and Response (EDR) erweitert werden. Marktforscher wie Gartner verstehen unter EDR „Lösungen, die Verhaltensweisen auf Endpoint-Systemen aufzeichnen und speichern, verschiedene Datenanalysetechniken verwenden, um verdächtiges Systemverhalten zu erkennen, Kontextinformationen bereitzustellen, böswillige Aktivitäten zu blockieren und Korrekturvorschläge zu

unterbreiten, um betroffene Systeme wiederherzustellen".

Was EDR leisten kann

EDR wertet die System- und Nutzungsdaten von Endpoints aus, bestimmt das Normalverhalten der Endpoints und sucht nach auffälligem Endpoint-Verhalten, das vom Normalzustand abweicht. EDR erkennt mögliche Attacken also nicht auf Basis von Signaturen, wie es klassische Anti-Malware macht, sondern durch eine Bestimmung des normalen Verhaltens der einzelnen Endpoints sowie der Überwachung, ob sich Anomalien bei den Endgeräten zeigen. Dadurch lassen sich auch bisher unbekannte Angriffstechniken besser erkennen, da sie zu einem veränderten Verhalten bei der Nutzung von Prozessen, Funktionen und Applikationen der Endpoints führen.

EDR ermöglicht die Suche nach sogenannten Indicators of compromise (IoCs), also Anzeichen für mögliche Angriffe. Die Aktivitäten auf den Endpoints können übergreifend analysiert werden: Einzelne Aktionen auf einem Endpunkt können harmlos und legitim erscheinen, betrachtet man aber die Kombination aus verschiedenen Aktionen, kann sich ein Verdacht auf eine Attacke ergeben. Dies ermöglicht es EDR-Lösungen, auch dateilose Angriffe zu erkennen, die keine Schadsoftware an sich nutzen, sondern vorhandene Funktionen und Prozesse des angegriffenen Systems missbrauchen.



Die Lockheed Martin Cyber Kill Chain sieht mehrere Angriffsstufen vor. Diese Stufen bilden die Struktur und den Ablauf einer Attacke ab. (Bild: Lockheed Martin)

Wie sich mehrstufige Endpoint-Attacken erkennen lassen

Im Zuge einer Endpoint-Attacke gibt es mehrere Phasen, in denen eine EDR-Lösung verdächtiges Verhalten aufdecken kann. Besonders gut sichtbar wird dies auf Basis der Cyber Kill Chain: Im Jahr 2011 übertrug das unter anderem im Rüstungsbereich tätige Unternehmen Lockheed Martin das Kill-Chain-Modell auf die Cyber-Sicherheit. Das Modell trägt den inzwischen geschützten Namen „Lockheed Martin Cyber Kill Chain". Die Lockheed Martin Cyber Kill Chain sieht mehrere Angriffsstufen vor. Diese Stufen bilden die Struktur und den Ablauf einer Attacke ab. Zu jeder Stufe gibt das Modell an, welche Aktivitäten Angreifer unternehmen, sodass man nach diesen Aktivitäten bei den Endpoints suchen kann, um einen Angriff zu erkennen.

Eine EDR-Lösung kommt insbesondere bei den folgenden Angriffsstufen ins Spiel:

RECONNAISSANCE (Identify the Targets)

Angreifer: Sucht sein Ziel, sammelt Informationen über das Ziel (E-Mail-Adressen, Daten aus sozialen Netzwerken, Informationen über Unternehmen und IT-Systeme).

EDR: Wertet Zugriffe auf Server aus, um auf verdächtige Suchaktivitäten hinweisen zu können.

WEAPONIZATION (Prepare the Operation)

Angreifer: Stellt die passenden Angriffs-Tools zusammen (Malware, Exploit).

EDR: Sucht Spuren von Angriffsversuchen, analysiert entdeckte Malware und warnt davor.

DELIVERY (Launch the Operation)

Angreifer: Startet Angriff und verteilt Malware.

EDR: Überwacht die möglichen Angriffswege, analysiert entdeckte Angriffe (IT-Forensik) und warnt davor.

INSTALLATION (Establish Beachhead at the Victim)

Angreifer: Installiert und versteckt Malware, bringt Backdoor an.

EDR: Überprüft Installationen, Aktivitäten, Zertifikate und Berechtigungen und weist auf verdächtige Aktionen hin.

COMMAND & CONTROL (C2) (Remotely Control the Implants)

Angreifer: Sucht und öffnet Kommunikationskanäle, um die Schadfunktionen aus der Ferne steuern zu können.

EDR: Untersucht Malware-Aktivitäten, um Kommunikationskanäle aufzuspüren und entsprechend zu warnen.

ACTIONS ON OBJECTIVES (Achieve the Mission's Goal)

Angreifer: Missbraucht Zugänge und Berechtigungen, versucht weitere Berechtigungen zu erlangen, manipuliert und zerstört Daten und Systeme, stiehlt Informationen.

EDR: Sucht nach verdächtigen Aktivitäten, führt forensische Analysen durch, und schlägt Maßnahmen vor, um den Schaden einzudämmen.

EDR alleine reicht aber nicht

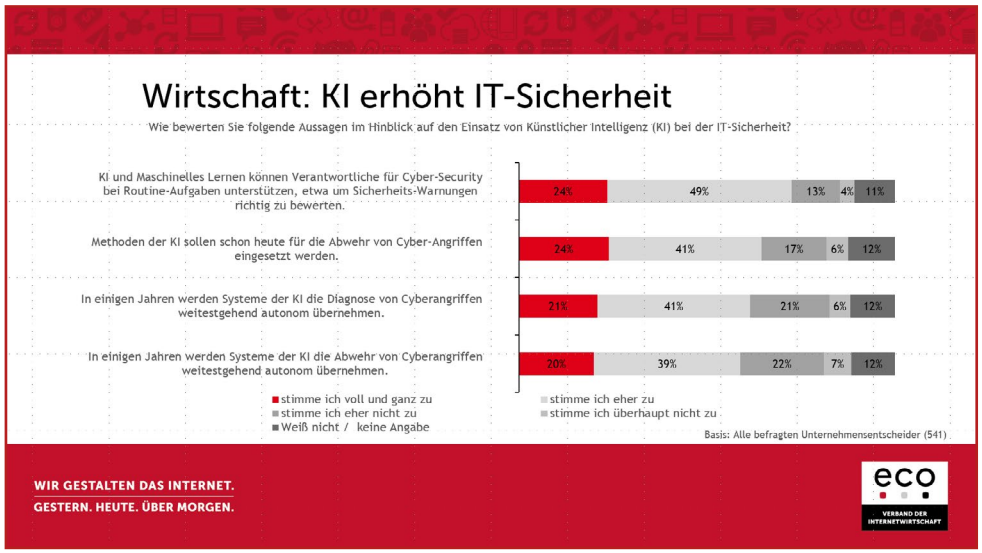
Der Einsatz von EDR bedeutet nicht, dass alle Angriffe automatisch erkannt und abgewehrt werden. EDR benötigt die Integration in weitere Security-Lösungen, mit denen die Response (zum Beispiel Blockade des Netzwerkzugriffs für ein verdächtiges Endgerät) durchgeführt werden kann, sowie die abschließende Bewertung von verdächtigem Endpoint-Verhalten.

Security-Experten können sich dank EDR auf wenige, mögliche Angriffszeichen (aufbereitete Alerts) konzentrieren und müssen nicht Tausende von Events und Logs auswerten. Security-Analysten werden unterstützt und entlastet. Kommt es zu einem Vorfall, können die Security-Analysten über EDR einen schnellen Überblick über die überwachten Endpoints erlangen.

Es zeigt sich: EDR bietet eine deutliche Erweiterung zu der reinen Endpoint Protection. Aber die Evolution der Endpoint Security geht noch weiter, ja muss weiter gehen, hin zu XDR (Extended Detection and Response), wie das nächste Kapitel zeigt. *Oliver Schonschek*

Warum XDR der Endpoint-Schutz der Zukunft ist

Lösungen aus dem Bereich EDR (Endpoint Detection and Response) unterstützen Security-Experten bei der Erkennung von Endpoint-Attacken und schlagen Maßnahmen zur Eindämmung der Schäden vor. Durch den Mangel an Security-Experten benötigt EDR aber eine Erweiterung durch Künstliche Intelligenz (KI), um möglichst automatisch auf Endpoint-Angriffe reagieren zu können. Hier kommt XDR als Extended Detection and Response ins Spiel.



Die Erwartungen an KI in der Security sind hoch. So ergab eine eco-Umfrage: 65 Prozent der befragten Unternehmensentscheider sagten, Methoden der KI sollten bereits für die Abwehr von Cyber-Angriffen eingesetzt werden. 59 Prozent denken, in einigen Jahren werden Systeme der KI die Abwehr von Cyberangriffen weitestgehend autonom übernehmen. Bei KI-basierten XDR-Lösungen wird dies bereits Realität. (Bild: eco)

Mehr über den Kontext der Endpoints erfahren

Viele Security-Konzepte machen den Fehler, die einzelnen IT-Infrastrukturen getrennt zu sehen und die Abhängigkeiten zwischen Endpoints, Netzwerken, Clouds und Applikationen zu unterschätzen. Die Angreifer jedoch machen dies nicht, sie nutzen die Abhängigkeiten aus und damit die Schwachstellen einer IT-Infrastruktur, um eine andere angreifen und missbrauchen zu können.

Ebenso zeigen sich die Angriffe auf Endpunkte zuerst in der Umgebung, also in den Netzwerken und den Cloud-Diensten. Nur bei physischen Attacken auf Endgeräte kann ein Angreifer direkt an den Endpunkt gelangen.

Aus diesen Gründen ist es wichtig und sinnvoll, auch den Kontext und damit die Umgebung der Endpunkte zu überwachen, um dort Anomalien feststellen zu können, die auf Attacken hinweisen können.

Zu diesem Zweck wurde das EDR-Konzept erweitert zum XDR: zu Extended

Detection and Response. Darunter verstehen die Marktforscher von Gartner einheitliche Plattformen für Sicherheits- und Vorfallreaktionen, die Daten von mehreren Komponenten sammeln und korrelieren. Dies konsolidiert mehrere Sicherheitsprodukte zu einem und kann dazu beitragen, insgesamt bessere Sicherheitsergebnisse zu erzielen, so Gartner. Unternehmen sollten in Betracht ziehen, diese Technologie zu verwenden, um die Sicherheit zu vereinfachen und zu optimieren.

Bedeutung von XDR steigt

Die Gartner-Analysten sehen in XDR einen der zentralen Security-Trends. Die Vorteile von XDR liegen auf der Hand: Beispielsweise kann ein Angriff, der Warnungen auf E-Mail, Endpunkt und Netzwerk verursacht hat, zu einem einzigen Vorfall kombiniert werden. Die Hauptziele einer XDR-Lösung sind die Erhöhung der Erkennungsgenauigkeit und die Verbesserung der Effizienz und Produktivität von Sicherheitsvorgängen.

Die Zentralisierung und Normalisierung von Daten trägt auch zur Verbesserung der Erkennung bei, indem Signale von mehreren Komponenten kombiniert werden, um Ereignisse zu erkennen, die ansonsten möglicherweise ignoriert werden, so Gartner.

Auch die Marktforscher von IDC sehen eine große Bedeutung von XDR für die Endpoint Security. Als vorteilhafte Funktionen von XDR nennt IDC:

- Kontextverbesserte Sichtbarkeit: Endpunkt-Sicherheit muss auch Daten nutzen, die außerhalb des Endpunkts liegen.
- Visualisierungstools für Angriffsketten: Bei Auswertungen kann man von einer Umgebung leicht in eine andere wechseln (z. B. Endpunkt zur Netzwerkansicht).
- Erhöhte Visibilität: Die Möglichkeit, einfache und komplexe Abfragen zu Aktivitäten in der gesamten Infrastruktur auszuführen.

Wie sich XDR von EDR unterscheidet

Doch warum reichen EDR-Konzepte nicht mehr aus und warum wird XDR als die Zukunft der Endpoint-Sicherheit gesehen?

EDR kann zu viele Warnungen liefern, die unvollständig sind und keinen Kontext haben. Es sind zeitaufwändige, komplexe Untersuchungen notwendig, die spezialisiertes Fachwissen erfordern. Die bereits knappen Security-Ressourcen sind bei EDR immer noch zu stark gefordert.

XDR dagegen bietet Einblicke in Daten über Netzwerke, Clouds und Endpunkte hinweg und setzt Analysen und Automatisierung ein, um den immer komplexer werdenden Bedrohungen von heute

zu begegnen. Mit XDR können Sicherheitsteams deshalb weiter entlastet werden.

Bedarf an Automatisierung und KI

Die weitere Entlastung der Security-Teams ist von hoher Bedeutung, denn bekanntlich herrscht gerade in der IT-Sicherheit ein großer Fachkräftemangel. Eine XDR-Lösung sollte deshalb so autark und autonom wie möglich arbeiten und Funktionen zur Automatisierung von Detection und Response besitzen.

Es reicht nicht aus, dass erfolgreiche Angriffe erkannt und gemeldet werden, auch die Reaktionen müssen umgehend erfolgen können, um die Folgeschäden gering zu halten. Engpässe im Security-Team können aber dazu führen, dass selbst erkannte Attacken nicht zeitnah beantwortet werden können. Deshalb sollte das Security-Team durch den Einsatz von KI (Künstlicher Intelligenz) verstärkt werden. Dank KI und Maschinellem Lernen kann es einer XDR-Lösung gelingen, Angriffe weitgehend automatisch erkennen und abwehren zu können.

Dafür ist es aber entscheidend, dass die XDR-Lösung in die restliche Security voll integriert ist. Andernfalls können zum Beispiel keine automatischen Response-Maßnahmen sichergestellt werden, wie die Blockade von Netzwerkzugriffen durch verseuchte Endgeräte.

Ebenso muss eine XDR-Lösung mit aktueller Bedrohungsintelligenz (Threat Intelligence) versorgt werden, damit die Entscheidungsgrundlagen und Erfahrungswerte zu der jeweiligen Gefahrenlage passen.

Ist dies der Fall, hat die Evolution der Endpoint Security ihr Ziel erreicht, von der klassischen Endpoint Protection ausgehend über die Endpoint Detection and Response bis hin zu einer KI-basierten XDR-Lösung. *Oliver Schonschek*

XDR als neues Sicherheits-paradigma

Die Welt der Cybersicherheit ist eine Welt der Akronyme. Von AV (Antivirus) über EPP (Endpoint Protection Plattform) bis hin zu EDR (Endpoint Detection and Response) – und jetzt auch XDR (Extended Detection and Response). Diese sich wandelnden Technologien und deren Bezeichnungen sind ein Beleg für eine sich wandelnde Cyberbedrohungslage.

Durch eine Kombination von Endpunkt-, Netzwerk- und Anwendungs-Telemetrie liefert XDR die Sicherheitsanalysen, die den neuen Bedrohungen wirkungsvoll begegnen können. (Bild: sdecoret/AdobeStock)

Sicherheitsverantwortliche müssen stets einen oder mehrere Schritte voraus sein, um sich vor Angreifern zu schützen. Im Zuge der sich verändernden Bedrohungslandschaft sind auch Innovationen in Unternehmen notwendig, denn um den Geschäftsbetrieb aufrechtzuerhalten und weiterzuentwickeln, dürfen sich Organisationen in Sachen Digitalisierung keine Auszeit gönnen.

Das alte „On-Premises"-Paradigma, das durch einen überschaubaren Netzwerkumfang begrenzt ist, gilt nicht mehr. Wir befinden uns nun in einer Welt, die zunehmend von einer dezentralen, Cloud-basierten Infrastruktur geprägt ist, in der die Remote-Arbeit die Komplexität der Geschäfts- und Betriebssicherheit noch weiter erhöht. Darüber hinaus nimmt, wie wahrscheinlich jeder CISO bestätigen wird, die Zahl der Cyberangriffe, Cyberangreifer und offensiven Toolsets täglich zu.

Die in der Vergangenheit konzipierten Sicherheitstechnologien wurden nicht gebaut, um mit der komplexen, sich schnell verändernden Bedrohungslandschaft von heute fertig zu werden. Die Beweise dafür sind eindeutig: Zunehmende Ransomware-Angriffe in Verbindung mit Datenverlusten und IP-Diebstahl, strapazierte SOC (Security Operations Center)-Teams, die sich

mit Alarmmüdigkeit und Personalmangel auseinandersetzen müssen, und die steigende Anzahl von Angriffen, die trotz des Einsatzes traditioneller Sicherheitstools erfolgreich sind – das sind nur einige der Beispiele für weit verbreitete Probleme in der heutigen IT-Sicherheit.

XDR wurde speziell als Lösung für eben diese (und viele weitere) Probleme konzipiert. In diesem Beitrag soll erörtert werden, was XDR ist und wie der Ansatz einen Wandel in der Cybersicherheit herbeiführt, um die Sicherheitsteams von Unternehmen zu stärken und Cyberkriminelle in Schach zu halten.

Was ist XDR?

XDR steht für Extended Detection und Response und repräsentiert die Weiterentwicklung von EDR, der Endpoint Detection und Response. EDR, insbesondere ActiveEDR, brachte Sichtbarkeit und automatische Reaktion auf Vorfälle auf Endpunkten wie Laptops und Workstations. Das typische Netzwerk von heute verfügt allerdings über eine enorme Vielzahl verschiedener Datenpunkte, die von Angreifern auf dem Weg zu einer erfolgreichen Kompromittierung ausgenutzt werden können, von Mobiltelefonen und IoT-Geräten bis hin zu Containern und Cloud-nativen Anwendungen. Um diese komplexen Netzwerkumgebungen adäquat zu schützen, bedarf es eines neuen und moderneren Ansatzes.

Was man heutzutage als XDR bezeichnet, ist ein Sicherheitsverfahren, das das althergebrachte EDR ersetzt, indem es Transparenz über alle Daten bietet, die das Netzwerk durchqueren – und nicht nur über die Daten der Endpunktebene. XDR-Plattformen wie die Singularity-Plattform von SentinelOne sammeln Daten von allen Assets in der gesamten Unternehmensumgebung, führen sie in einem einzigen Data Lake zusammen und wenden Sicherheitsanalysen und künstliche Intelligenz über mehrere Sicherheitsebenen hinweg an, um eine verbesserte automatische Erkennung und Reaktion auf Bedrohungen zu ermöglichen.

Die Weiterentwicklung von EDR

XDR ermöglicht eine schnellere, umfassendere und effektivere Erkennung und Reaktion auf Bedrohungen als EDR, basierend auf einem einzigen Pool von Rohdaten, die Informationen aus dem gesamten Ökosystem umfassen. Dabei werden verglichen mit EDR die Daten aus einem breiteren Spektrum von Quellen gesammelt und zusammengestellt.

Cyberangriffe betreffen in der Regel viele verschiedene Bereiche einer Organisation. Die durch XDR ermöglichte Transparenz ist die einzige Möglichkeit, einen vollständigen Überblick darüber zu erhalten, was, wann, wo und wie passiert ist. Dieselben kontextualisierten Handlungsstränge, die ActiveEDR auf der Endpunktebene bietet, können dann auf mehreren Ebenen erstellt werden: Cloud, Container, virtuelle Maschinen, IoT, Endpunkte, Server usw.

Diese umfassende Sichtbarkeit bringt eine Reihe von Vorteilen mit sich, unter anderem:

- bessere Erkennung verborgener Angriffe
- reduzierte Verweildauer von Daten und Analysen
- erhöhte Geschwindigkeit bei der Reaktion auf Angriffe

Darüber hinaus verringert die Lösung dank KI und Automatisierung die Belastung der Sicherheitsanalysten durch manuelle Arbeit. Eine XDR-Plattform wie Singularity kann proaktiv und schnell ausgefeilte Bedrohungen identifizieren, die Produktivität des Sicherheits- oder SOC-Teams steigern und dadurch den ROI des Unternehmens massiv erhöhen.

XDR vs. SIEM

Obwohl sowohl XDR- als auch SIEM-Tools Daten aus verschiedenen Quellen sammeln, haben sie ansonsten wenig gemeinsam. Im Gegensatz zu einer XDR-Plattform haben SIEMs (ebenso wie passive EDR-Tools) weder die Fähigkeit, aussagekräftige Entwicklungstrends zu erkennen, noch bieten sie automatische Erkennungs- oder Reaktionsmöglichkeiten. Außerdem erfordern SIEM-Systeme ein hohes Maß an manuellen Nachforschungen und Analysen, um ihren Nutzen zu entfalten.

Wenn ein Unternehmen in SIEM-Tools investiert hat, heißt das jedoch nicht, dass sie durch die XDR-Plattform überflüssig werden. Sie können direkt in den Datenspeicher der XDR-Plattform eingespeist werden, wodurch alle Rohdaten dem KI und Machine Learning der XDR-Lösung zugänglich gemacht werden.

Woran erkennt man ein leistungsfähiges XDR-Produkt?

Das erste Merkmal einer effektiven XDR-Lösung ist die Art und Weise, wie sie in das Netzwerk integriert ist. Sie muss nahtlos über den Sicherheits-Stack hinweg funktionieren und native Tools mit umfangreichen APIs bereitstellen. Hüten sollte man sich vor unausgereiften Lösungen, die sich oft als nicht mehr als eine Reihe alter und zusammengeschraubter Tools herausstellen. Die eigene XDR-Lösung sollte eine einzige Plattform bieten, die es dem Unternehmen ermöglicht, einfach und schnell einen umfassenden Überblick über sämtliche Assets und Vorgänge zu erhalten.

Zweitens ist eine Automatisierung, die durch fortschrittliche KI und bewährte Machine Learning-Algorithmen unterstützt wird, unerlässlich. Hat der Anbieter eine reiche Geschichte in der Entwicklung modernster KI-Modelle oder ist er in erster Linie für althergebrachte Ansätze bekannt und versucht nun lediglich auf den Zug moderner Technologien aufzuspringen?

Drittens: Wie einfach ist es, das Produkt zu verstehen, es zu warten, zu konfigurieren und zu aktualisieren? Einer der Hauptvorteile einer starken XDR-Lösung ist die erhöhte Produktivität der Mitarbeiter durch automatische Erkennung und Reaktion. Gleichzeitig möchte man natürlich auch sicherstellen, dass die Sicherheitsverantwortlichen nicht durch die Verwaltung oder Navigation einer komplizierten Lösung unverhältnismäßig gefordert werden.

Der Ansatz von SentinelOne: eine KI-gestützte XDR-Plattform für alle Zwecke

Die KI-getriebene XDR-Plattform Singularity von SentinelOne bietet alle Vorteile, die man von einer Komplettlösung erwartet: weitreichende Transparenz, automatische Erkennung und Reaktion, umfassende Integration und einfache Bedienung. Mit einer einzigen Codebasis und einem einzigen Bereitstellungsmodell ist Singularity das erste XDR-System, das den IoT (Internet of Things)- und CWPP (Cloud Workload Protection Platform)-Ansatz in einer einheitlichen Plattform vereint.

Alle IoT-Daten sind nahtlos in Singularity integriert, um das Threat Hunting zu erleichtern und einen vollumfänglichen Kontext zu ermöglichen. Durch den Einsatz der KI zur Überwachung und Steuerung des Zugriffs auf jedes IoT-Gerät ermöglicht Singularity XDR den Maschinen die Lösung von Problemen, die zuvor nicht in großem Maßstab gelöst werden konnten.

Der Autor Matthias Canisius ist Regional Director CE & EE bei SentinelOne. (Bild: SentinelOne)

Die Container-Workload-Protection wird auf allen wichtigen Linux-Plattformen unterstützt, sowohl physisch als auch virtuell, bei nativen Cloud-Workloads und Kubernetes-Containern. Sie bietet Prävention, Erkennung, Reaktion und Verfolgung von bekannten und unbekannten Cyberbedrohungen. Dazu gehört der Schutz vor Malware und Live-Angriffen in Cloud-nativen und containerisierten Umgebungen und erweiterte Reaktionsoptionen sowie autonome Gegenmaßnahmen in Echtzeit.

Fazit

Cybersicherheit wird oft mit einem Wettrüsten zwischen Angreifern und Verteidigern verglichen. Dieses Wettrüsten geht nun über die Ebene des Endpunkts hinaus. Da Unternehmen vermehrt auf Remote- und Cloud-Infrastrukturen setzen und damit eine immer größere Angriffsfläche schaffen, kann eine integrierte Plattform die erforderliche Transparenz und automatisierte Abwehr über alle Ebenen hinweg bieten. Durch die Kombination von Endpunkt-, Netzwerk- und Anwendungs-Telemetrie liefert XDR die Sicherheitsanalysen, die erforderlich sind, um dieses Rennen als Organisation mithilfe von verbesserter Erkennung, Einstufung und Reaktion für sich zu entscheiden.

Matthias Canisius, SentinelOne