Kaspersky Enterprise Cybersecurity

KASPERSKY lab

Ein Leitfaden für Investitionen in Endpoint Detection & Response für Unternehmen 2017–2018

www.kaspersky.de
#truecybersecurity

Inhalt

Einleitung

Ein wichtiges Geschäftsziel eines jeden Unternehmens ist es, die ständige Verfügbarkeit von Daten und Systemen aufrechtzuerhalten, die für eine zuverlässige Entscheidungsfindung verwendet werden können. Die Entwicklungen der Bedrohungslandschaft haben zu einem verstärkten Fokus auf Cybersicherheit geführt, der bis hin zur Vorstandsebene reicht. IT-Betriebs- und Sicherheitsteams sollten bei der Reaktion auf Sicherheitsvorfälle und Datenschutzverletzungen einen umfassenden, zusammenhängenden Ansatz verfolgen.

Endpoints an vorderster Front

Cybersecurity wird heute von der Geschäftsleitung im Streben nach Business Continuity auf dem Weg zum Geschäftserfolg als eine der Top-3-Prioritäten gesehen.

Führungskräfte benötigen heute ein Verständnis der konkret für ihr Unternehmen relevanten Cyberbedrohungslandschaft. Folgende Fragen sind relevant:

- Versteht meine Organisation die wichtigsten Bedrohungen und Sicherheitsrisiken für unsere Branche und uns selbst?
- Können wir Cyberangriffe schnell erkennen und stoppen?
- Wie positionieren wir die Verringerung von Cyberrisiken in der Gesamt-Entwicklungsstrategie für unser Unternehmen?

Unternehmens-Endpoints – Ihre Server, Workstations, Mobiltelefone usw. – sind die Punkte, an denen die Synergie zwischen Daten, Benutzern und Unternehmenssystemen stattfindet, die Geschäftsprozesse generieren und implementieren. Die vielen Einzelgeräte sind nach wie vor das Schlüsselelement in jedem Netzwerk, sowohl in geschäftlicher als auch in sicherheitstechnischer Hinsicht.

Um diese Endpoints zu schützen und ihre Verwendung als illegale Eintrittspunkte in Ihre Infrastruktur zu verhindern, sollten Ihre IT-Sicherheitsteams sich mit der Einführung von Prozessen und Technologien rund um hoch entwickelte Erkennung, Threat Hunting, IoC-Scannen, Malware-Analyse, digitale Forensik, die Umsetzung globaler Threat Intelligence und die Einrichtung eines formellen Prozesses zur Vorfallsreaktion befassen.

Doch wo soll man anfangen? Springen Sie auf den Zug namens „Maschinelles Lernen“ auf? Verbessern Sie das Threat Hunting? Konzentrieren Sie sich auf stärkere Überwachung und SOC? Besser wäre es vielleicht, diese und weitere Bereiche mit einer der neuen EDR-Lösungen (Endpoint Detection and Response) abzudecken. Aber was genau können Sie von EDR erwarten, und welche Art von Lösung sollten Sie wählen?

Dieses Dokument hilft Ihnen bei der Auswahl der EDR-Lösung, die für Sie die richtige ist. Unser Ziel ist es, die wesentlichen Unterschiede zwischen den verschiedenen Arten der auf dem Markt verfügbaren EDR-Funktionen aufzuzeigen und Ihnen dabei zu helfen, die wertvollsten Technologien für die Sicherung der Business Continuity und Sicherheit in Ihrem Unternehmen zu ermitteln.

Alles über Endpoint Detection and Response

Ein neuer Ansatz bei der Endpoint-Sicherheit

Schützen Sie Ihr Perimeter, um Angriffe zu verhindern. Das klang immer vernünftig: Wenn Ihr IT-Perimeter gut geschützt ist, wird der Endpoint-Schutz nur zu einer weiteren Ebene in Ihrer gesamten Sicherheitsstrategie.

In einer Welt, in der die Definition oder gar die Verteidigung des IT-Perimeters durch Technologien wie mobile Geräte, verbundene Geräte (IoT) und Cloud Computing zu einer Herausforderung wird und die Bedrohungsentwicklung einen defensiven perimeterbasierten Ansatz obsolet macht, ist dieser Ansatz nicht mehr zeitgemäß.

Gezielte Angriffe, eine starke Zunahme komplexer Penetrationstechniken, dateilose Malware, die Verwendung legaler Software, gestohlene Zugangsdaten normaler Benutzer, die berechtigte Nutzung, die Ausnutzung von Schlupflöchern und Fehlkonfigurationen von Sicherheitsrichtlinien – all dies hat dazu geführt, dass Unternehmen die Bedeutung integrierter Sicherheitslösungen und -strategien erkannt haben. Dies wiederum hat zur Zunahme der SIEM-Implementierungen und Security Operational Centers (SOCs) geführt. Cybersicherheit in Unternehmen ist – notgedrungen – proaktiv, mehrschichtig und hoch spezialisiert.

Die Welt verändert sich, und die Zeit für ein neues Paradigma bei der Endpoint-Sicherheit ist gekommen. Der Fokus hat sich wieder auf den Endpoint verlagert. Es gab schon immer weitsichtige IT-Abteilungen, die jeden Endpoint so behandelt haben, als ob er ein eigenes Sicherheitsperimeter benötigt. Und nicht zuletzt dank Organisationen, die diesen Ansatz **nicht** verfolgt haben und deren schlechte Transparenz der einzelnen Geräte zu einem insgesamt niedrigen Sicherheitsniveau geführt hat, sind Endpoints nach wie vor noch das Hauptziel von Cyberkriminellen.

Proaktiver werden

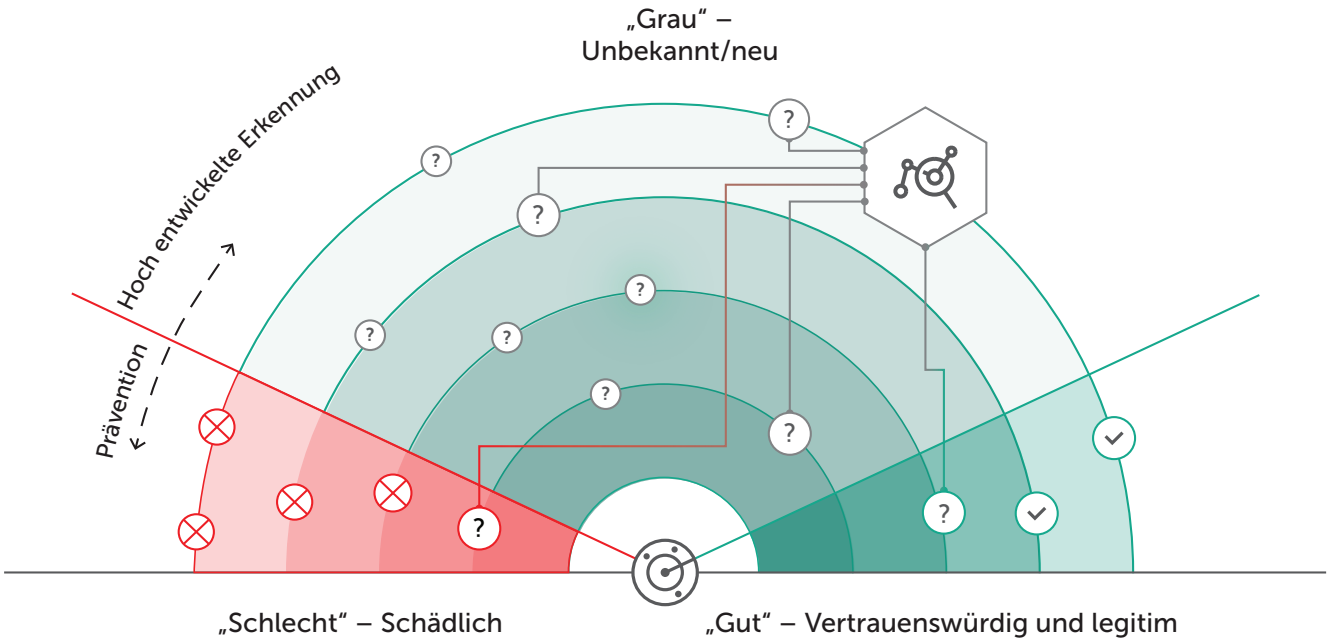
In der Zwischenzeit führen die Regulierungsbehörden neue Anforderungen ein (GDPR, PCI DSS usw.), die möglicherweise eine unterbrechungsfreie Überwachung und Aufzeichnung von Vorfällen über jeden Endpoint im Netzwerk erfordern. Bei den meisten Unternehmen steigt die Anzahl der von ihrer aktuellen Sicherheitslösung erfassten Ereignisse/Vorfälle immer weiter an, sodass die Überprüfung und Analyse jedes aufgezeichneten Ereignisses zu einem eigenen Problem wird. Es hilft nicht, dass Sicherheitsexperten, die über die notwendigen Kenntnisse im Bereich Reverse Engineering, Malware-Analyse, digitale Forensik und Vorfallsreaktion zur Bewältigung dieser Aufgaben verfügen, aktuell extrem begehrt und nicht leicht zu finden sind.

Zum gegenwärtigen Zeitpunkt sind die meisten Sicherheitsprozesse mit Fokus auf hoch entwickelte Bedrohungen und die meisten SOC-Überwachungsansätze im Wesentlichen alarmgesteuert und reaktiv. Sicherheitsbeauftragte warten auf Beweise für eine Sicherheitsverletzung, bevor sie den Sicherheitsanalytiker alarmieren, woraufhin das Incident Response Team Maßnahmen ergreifen kann. Im besten Fall identifiziert das Incident Response Team die Rückstände eines Angriffs im aktuellen Stadium der Kill Chain. Im schlimmsten Fall warten sie einfach nur darauf, den Schaden zu erfassen, teils Monate nach dem Eindringen in die Systeme. Das ist eindeutig nicht ausreichend. Daher überprüfen Unternehmen ihre Sicherheitsprozesse, insbesondere im Hinblick auf die proaktive Erkennung von Vorfällen und die Reaktion darauf.

Threat Hunting unterstützt Sie bei der Entdeckung hoch entwickelter Bedrohungen in Ihrem Unternehmen. Hierfür setzen hoch qualifizierte und erfahrene Sicherheitsexperten proaktive Techniken zur Bedrohungserkennung ein.

Wie wirkt sich das auf Endpoint-Lösungen aus?

Die jüngste Generation von Endpoint-Lösungen konzentriert sich auf die effektive Erkennung neuer Bedrohungen, die in die Organisation eindringen, in deren Rahmen Ereignisse in der „Grauzone", in der unbekannte, undefinierte Bedrohungen lauern können, überwacht und analysiert werden. Das nennen wir proaktives „Threat Hunting".



Jenseits des Endpoint-Schutzes

Effektives Threat Hunting hängt direkt mit den Fähigkeiten eines ausgereiften SOC zusammen. Ein Upgrade der gekauften Sicherheitslösungen reicht hier nicht aus: Es können nicht einfach neue Anforderungen an herkömmliche EPP-Lösungen (Endpoint Protection) gestellt werden – sie passen nicht oder funktionieren nicht wirksam.

Betrachten wir einige wichtige Probleme, die durch herkömmliche EPP-Lösungen effektiv behoben werden, und die neuen Herausforderungen, von denen Endpoint-Sicherheit jetzt steht, einmal näher:

Aspekte der Kontrolle und des Schutzes, die durch traditionelle EPP-Lösungen abgedeckt werden:	Neue Herausforderungen für Endpoint-Sicherheit:
Automatischer Schutz (sowohl in Bezug auf Prävention als auch auf Rollbacks) vor bestehenden Bedrohungen, einschließlich Ransomware und Crypto-Lockern	Proaktive Echtzeitsuche nach Anzeichen für ein Eindringen wie z. B. Gefährdungsindikatoren im gesamten Netzwerk
Zentrale Verwaltung und Durchsetzung von Sicherheitskontrollen für Web/ Programme/Geräte	Erkennung und Abwehr von Eindringlingen, bevor erheblicher Schaden angerichtet werden kann
Zentrale Verwaltung von Vulnerability-Assessment- und Patch-Management-Prozessen	Korrelation von Warnmeldungen von Netzwerksicherheitskontrollen, um die Vorgänge auf Endpoints in Echtzeit nachzuvollziehen
Schutz von Unternehmensdaten und Informationen auf Geräten	Validierung von Warnungen und potentiellen Vorfällen, die von anderen Sicherheitslösungen entdeckt wurden
Bereitstellung von Web- und E-Mail-Schutzrichtlinien auf Endpoint-Ebene	Schnelle Untersuchung und zentrale Verwaltung von Vorfällen auf Tausenden von Endpoints
Bereitstellung spezifischer Sätze von Sicherheitsdomänen für Endpoint-Nutzer, die auf deren Bedürfnisse zugeschnitten sind	Kosteneffizienz beim Vorfallsreaktionsprozess (manuelle Arbeit, Level-3-Fähigkeiten, Überlastung durch zu viele Alarme usw.) durch die Automatisierung von Routinemaßnahmen des Sicherheitsteams

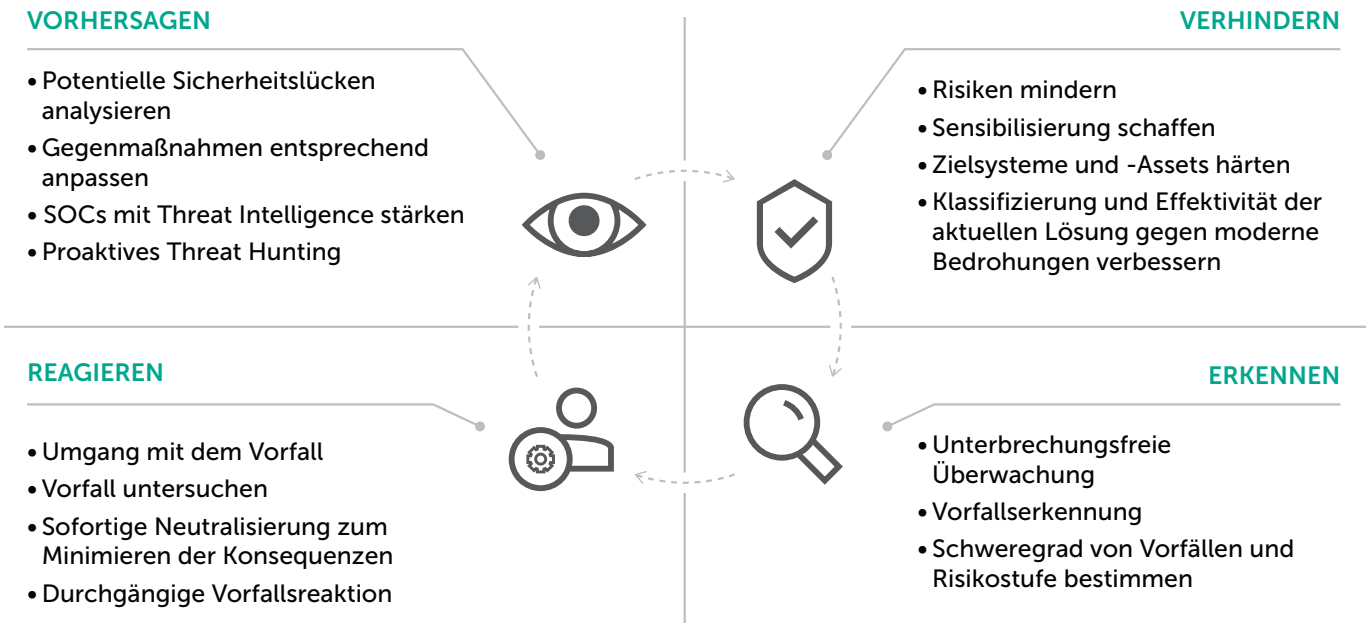
Wie können diese neuen Herausforderungen bewältigt werden?

Ihre Strategie für Endpoint-Cybersicherheit: anpassungsfähig, hoch entwickelt, vorausschauend

Gezielte Angriffe und hoch entwickelte Bedrohungen, die immer schwerer zu erkennen und häufig auch schwer zu eliminieren sind, fordern eine umfassende, anpassungsfähige Sicherheitsstrategie.

Eines der effektivsten anpassungsfähigen Security Frameworks basiert auf der von Gartner beschriebenen zukunftsweisenden Sicherheitsarchitektur. Der Ansatz dabei ist, einen Maßnahmenzyklus in vier Schlüsselbereichen anzubieten: Verhindern, Erkennen, Reagieren und Vorhersagen.

- **Verhindern** – sowohl Blockieren gemeinsamer Bedrohungen als auch das Härten der Kernsysteme, um das Risiko hoch entwickelter Bedrohungen zu verringern
- **Erkennen** – schnelle Erkennung von Aktivitäten, die auf einen gezielten Angriff oder eine vorhandene Sicherheitsverletzung hinweisen können
- **Reagieren** – präzise Eindämmung der Bedrohung, Durchführung von Untersuchungen und angemessene Reaktion auf Angriffe
- **Vorhersagen** – wissen, wo und wie neue zielgerichtete Angriffe auftreten könnten



Anpassungsfähiges Sicherheitsmodell

Dies setzt im Wesentlichen voraus, dass traditionelle Prävention, besonders in Bezug auf Endpoints, in Abstimmung mit hoch entwickelten Erkennungstechnologien, Bedrohungsanalysen, Reaktionsfunktionen und vorausschauenden Sicherheitstechniken funktionieren. So wird ein Cybersicherheitssystem geschaffen, das sich kontinuierlich an neue Herausforderungen für das Unternehmen anpasst und auf diese reagiert.

Mehrstufige, präventionsbasierte Technologien sind nach wie vor ein Schlüsselelement des neuen, proaktiven Ansatzes zum Schutz vor zielgerichteten Angriffen. Wenn der Angreifer jedoch ausreichend motiviert ist und vielleicht sogar von einem Dritten angeheuert wird, um einen erfolgreichen Angriff durchzuführen, wird ein reiner Präventionsansatz nicht ausreichen. Außerdem müssen Sie in der Lage sein, Bedrohungen schnell zu erkennen, Entscheidungen zu treffen und die Möglichkeit eines Eindringens zu antizipieren, dabei aber gleichzeitig den derzeitigen manuellen Betrieb vereinfachen und die Reaktionstools automatisieren.

Definieren von EDR

Hauptfunktionen einer EDR-ähnlichen Lösung

Wie wir gesehen haben, definiert Gartner EDR-Lösungen als Lösungen mit den folgenden Hauptfunktionen:

- Erkennen von Sicherheitsvorfällen
- Eindämmen des Vorfalls am Endpoint, sodass der Netzwerkverkehr oder die Prozessausführung aus der Ferne gesteuert werden kann
- Untersuchen von Sicherheitsvorfällen
- Wiederherstellen der Endpoints auf einen Zustand vor der Infektion

Endpoint Incident Detection

Erkennen von Sicherheitsvorfällen durch **Überwachung von Endpoint-Aktivitäten** und -Objekten, Richtlinienverstößen oder durch Validierung von extern gespeisten Gefährdungsindikatoren (IOCs)

Vorfallsuntersuchung

Untersuchung von Sicherheitsvorfällen. Die Untersuchungsfunktion sollte einen **Verlauf aller primären** Endpoint-Ereignisse enthalten, um sowohl die technischen Änderungen, die eingetreten sind, als auch die geschäftlichen Auswirkungen zu ermitteln.

(Ausweitung der Berechtigungen, Ausbreitung, Ausschleusung, Geolokalisierung von C&C und Zuschreibung zu Gegnern, wenn möglich)

Vorfallseindämmung und -reaktion

Eingrenzen des Vorfalls am Endpoint und **Wiederherstellen** der Endpoints in einen Zustand vor der Infektion

Entfernen bösartiger Dateien, Zurücksetzen und Reparieren anderer Änderungen oder Erstellen von Behebungsanweisungen, die anderen Tools zur Verfügung gestellt werden können

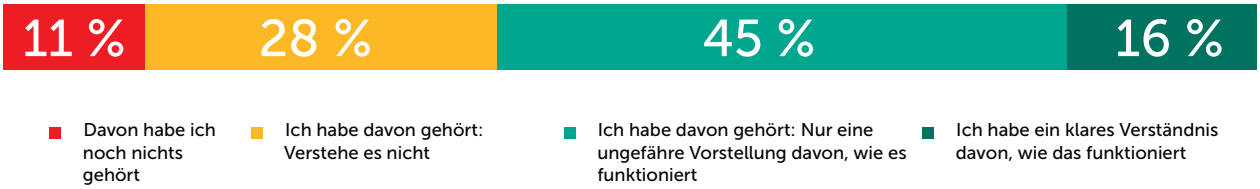
Datenerfassung aus Forensik

Sammeln von Datensätzen, RAM-Abbilder, HDD-Snapshots etc. für weitere Analysen

Wie gut verstehen Organisationen die Funktionsweise von EDR, und wie tragen diese Technologien zur Geschäftskontinuität bei? Eine Umfrage von Kaspersky Lab unter Unternehmen im Jahr 2016 lieferte einige beunruhigende Ergebnisse.

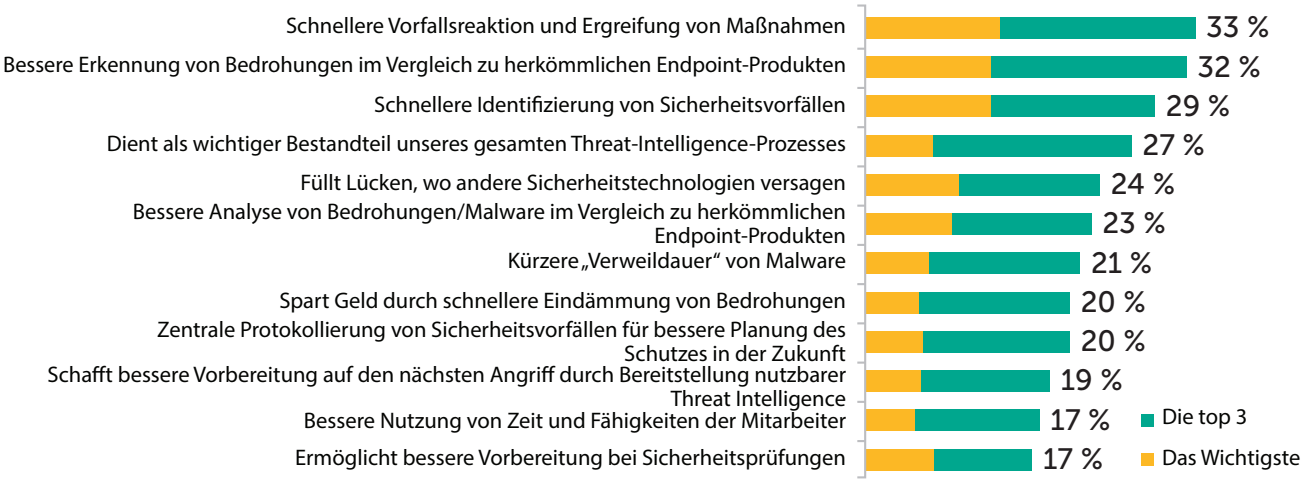
Frage: „Wie gut kennen Sie die Klasse der EDR-Lösungen?“

Antwort:



Quelle: IT-Experten in Unternehmen mit über 250 Mitarbeitern

Die befragten Unternehmensvertreter formulierten gleichzeitig klar die Grundlagen ihrer Erwartungen und die Ergebnisse, die sie sich vom Einsatz von EDR-Lösungen in ihren Organisationen wünschen:



Diese Kombination aus begrenztem Verständnis und klaren Erwartungen ist problematisch. EDR-Lösungsanbieter sind natürlich sehr daran interessiert, diese Erwartungen zu erfüllen, indem sie „Killer-Funktionen” entwickeln, die viel versprechen und in der Pilotphase spannend aussehen, sich aber oft als sehr viel weniger praktisch und kostengünstig erweisen, wenn sie in die neuen oder bereits vorhandenen Prozesse des Kunden für Vorfallsreaktion, Untersuchung oder Threat Hunting integriert werden.

Konsequenterweise wird EDR deshalb teilweise mit Misstrauen betrachtet.

Aufstieg und Fall der Lösungen für Endpoint Detection and Response

Erstanwender von EDR-Lösungen sind leider nicht immer die größten Fans der Technologie. Bei vielen der allerersten EDR-Lösungen gab es Mängel, was bei einigen Kunden für Enttäuschung und Frustration sorgte.

Leider gibt es noch keine etablierte Vergleichsanalyse und keinen unabhängigen Bericht, die alle wichtigen Funktionen und möglichen Varianten der heute auf dem Markt erhältlichen EDR-Technologien darstellen. Und viele First-Generation-Produkte in diesem noch unzureichend entwickelten Markt konnten in der Praxis zunächst nicht das liefern, was Experten und Organisationen erwartet hatten.

Die meisten Lösungen begannen mit einigen „Killer-Funktionen" anstelle von komplexen Funktionen. Statt einer integrierten Lösung, die Threat Intelligence für Netzwerksicherheit, Threat Hunting, Anti-Malware, Vorfallsreaktion und Forensikfunktionen vereinheitlichen und automatisieren kann, erwies sich EDR in der Praxis als eine Reihe von Analyse- und Forschungswerkzeugen. Und dieses Technologie-Toolkit erwies sich als kostspielig und für den durchschnittlichen Sicherheitsprofi als extrem schwer zu handhaben.

Einige EDR-Lösungen konnten auch die versprochene Effizienz nicht liefern. Bei der Reaktion auf einen Malware-Vorfall sammelt eine EDR-Lösung Informationen von Endpoints – Signaturen und Malware-Verhalten –, die zur Erkennung zukünftiger Infektionen verwendet werden können. Wenn die Lösung jedoch nicht in die Erkennungstechnologien und Sicherheitssysteme integriert ist, besteht ein hohes Risiko von Überschneidungen und Duplikaten, wodurch mehr manuelle Prozesse generiert werden und der Workflow behindert wird, anstatt die Effizienz und Wirksamkeit zu verbessern. Das EDR-System wird einfach zu einem zusätzlichen Speichersilo für sicherheitsbezogene Daten – Daten, anhand derer selbst Sie nicht erkennen können, wie das Ereignis zustande kam oder wie man es in Zukunft verhindern kann. Ohne eine in den Workflow integrierte Lösung auf Ursachenebene kann eine Organisation keine vollständige Behebung durchführen und das Risiko eines erneuten Auftretens reduzieren.

Ein weiteres Manko war, dass einige ursprünglich auf dem Markt angebotene Lösungen nicht wirklich darauf ausgelegt waren, APTs zu entdecken oder zu untersuchen. Dafür mussten EDR-Nutzer Maßnahmen an Experten – möglicherweise an die des Anbieters – auslagern oder teure Zusatzschulungen erwerben. Wenn bei jedem erkannten Verstoß ein externes Incident Response Team hinzugezogen werden muss, sollte die Kosteneffizienz der ursprünglichen EDR-Lösung möglicherweise infrage gestellt werden.

Ein zunehmender Trend ist die Verwendung von Cloud-Versionen von EDR, bei denen bestimmte Protokolle und Daten in die Cloud des Anbieters übertragen werden, anstatt sie auf installierten Agenten oder in einem zentralen Repository aufzubewahren. Dies hat jedoch dazu geführt, dass immer mehr Vorfälle mit langsamerer (und gelegentlich gar keiner) Reaktion auftreten.

Diese Situation gehört jedoch größtenteils der Vergangenheit an, und Interessierte, die sich zurzeit auf dem EDR-Markt umsehen, sollten die potentiellen Ergebnisse ihrer Investitionen nicht anhand der Erfahrungen dieser frühen Pioniere beurteilen. Der Markt ist gewachsen und hat sich weiterentwickelt.

Wonach sollten Sie also heute bei EDR suchen, und was ist zu beachten? Sehen wir uns fünf Herausforderungen an, die Sie vor der Umsetzung Ihres EDR-Projekts berücksichtigen müssen.

Die top fünf Herausforderungen zu Beginn eines EDR-Projekts

Es gibt immer neue Herausforderungen für Organisationen, die sich mit neuen Technologien oder unbekannten Prozessen beschäftigen. Und da EDR-Lösungen teurer sind als herkömmliche EPP-Lösungen, kann es schwierig sein, Ihre Investition in EDR in Bezug auf den Mehrwert zu rechtfertigen, wenn man sie mit den Kosten eines SIEM- oder forensischen Tools vergleicht.

Die Kernfunktion eines unternehmenstauglichen EDR-Systems ist **die Fähigkeit, das Sicherheitsteam bei fragebasierten Untersuchungen zu unterstützen:** Threat-Hunting-Tipps sind iterativ und beginnen mit Fragen oder Hypothesen, um Transparenz zu schaffen. Eine erste Frage oder Hypothese könnte auf den Schritten der Cyber-Kill-Chain beruhen und etwa wie folgt lauten: „Findet Datenexfiltration oder schädliche Kommunikation statt?“ oder „Wenn es eine verdächtige Verbindung zu einer externen Domain gibt, läuft sie höchstwahrscheinlich durch diesen Teil des Netzwerks, aber von welchem Endpoint und von welchem Prozess aus?“.

Um diese Fähigkeiten bereitstellen zu können, muss die EDR-Lösung über **Funktionen zur Unterstützung von Untersuchungen** sowie über **Funktionen zur Datenerfassung** und **-speicherung** verfügen. Die **Vorfallserkennung** sollte außerdem sowohl automatisierte als auch manuelle Elemente enthalten. Nicht zuletzt sollten das Sicherheits- und das Incident Response, sobald der erste Vorfall erkannt wird, in der Lage sein, die Bedrohung **auf einfache Weise einzudämmen**, die Endpoints **wiederherzustellen** und zu **verhindern**, dass sich diese konkrete Aktivität wiederholt.

Werfen wir einen Blick auf fünf gängige Herausforderungen, die Unternehmen berücksichtigen sollten, wenn sie sich für hoch entwickelte EDR-Lösungen entscheiden oder ihren aktuellen Endpoint-Schutz in Bezug auf Erkennung und Reaktion verbessern möchten.

Endpoint-Daten: zu viel Transparenz

Endpoint-Schutz beginnt in jeder Form mit der Erfassung neuer Daten sowie ihrer Speicherung und Analyse. Theoretisch gilt: Je mehr Daten Sie sammeln können, desto größer ist der Nutzen. Dieselbe Theorie wurde früher auch auf SIEM-Systeme angewandt. Um große Mengen gesammelter Daten zu interpretieren, benötigt der EDR-Betreiber aber auch den entsprechenden Kontext. Beispielsweise ist das schnelle Auffinden einer Verbindung zu einer schädlichen Domain von wesentlich geringerem Wert, wenn man nicht weiß, von welchem Endpoint diese stammt, wie der Prozess gestartet wurde, was die Ursache dafür war und welche Ressourcen möglicherweise bereits betroffen sind.

Unausgereifte EDR-Lösungen auf dem Markt sammeln zwar Daten, liefern aber nicht den richtigen Kontext. Mit ihnen kann der Bediener unter Umständen beispielsweise erkennen, auf welchen Rechnern eine Datei mit einer bestimmten Hash-Summe gespeichert ist, ohne Informationen darüber zu erhalten, wie die Datei auf diese Rechner gelangt ist. Eine Liste der generierten Prozesse kann für das Objekt und die Aktivitäten zur Verfügung gestellt werden, jedoch ohne Visualisierung. Oder es können komplexe Warnmeldungen über atypische Verhaltensweisen oder Abweichungen ausgegeben werden, jedoch ohne grundlegende Scans und Ergebnisse.

Einige Lösungen sammeln alle Daten von den Endpoints und präsentieren sie dann direkt auf der Benutzeroberfläche, um quasi direkten Einblick in die Datenbank zu gewähren. Wenn der Betreiber kein Datenwissenschaftler oder Big-Data-Experte und darüber hinaus kein Sicherheitsexperte ist, kann er auf der Grundlage dieser Rohdaten keine fundierte Entscheidung treffen.

Oftmals erzeugen solche Systeme Tausende von Nachrichten und buchstäblich Millionen von Warnmeldungen, die alle von jemandem überprüft werden müssen. Selbst in den größten Organisationen ist es unwahrscheinlich, dass das Überwachungs- und Reaktionsteam in der Lage ist, mehr als 50–60 mittlere bis sehr kritische Vorfälle gleichzeitig zu bewältigen. Man verfügt also zwar über eine Lösung, die alle Bedrohungen findet; es kann jedoch wenig bis gar nichts gegen die gefundenen Bedrohungen unternommen werden, da man einerseits zu viel und andererseits zu wenig erfährt.

Ein Kompromiss kann hier die Weiterleitung von Alarmen Ihres eigenen Sicherheitsteams an einen externen MSSP sein. Hierfür müssen Sie jedoch einen Anbieter mit der richtigen Ausbildung und dem richtigen Fachwissen finden. Und ohne eine Priorisierung der Vorfälle könnte dies eine enorme Investition und Verschwendung von Ressourcen für nicht kritische Warnmeldungen bedeuten. Ein weiterer kritischer Punkt, der jeden MSSP betrifft, ist die Frage des Vertrauens, des Datenschutzes und der Compliance-Beschränkungen.

Empfehlungen:

- Suchen Sie nach Lösungen, mit denen Sie nicht nur Risiken automatisch durch Warnmeldungen erkennen können, sondern die auch eine tief greifende Anpassung ermöglichen – die Konfiguration verschiedener Benutzerrollen, die Zuweisung von VIP-Gruppen und die schnelle Einrichtung von Whitelists. Auf diese Weise können Sie Wichtiges entsprechend hervorheben, Unnötiges aussortieren und sicherstellen, dass nur kritische Informationen für externe MSSPs sichtbar sind.
- Denken Sie darüber nach, inwieweit Sie Datenanalysen innerhalb des Unternehmens durchführen wollen und wie viele Daten Sie speichern und verarbeiten möchten. Der Umgang mit ganzen Terabyte von internen Daten kann zu erheblichen zusätzlichen Hardwarekosten führen.

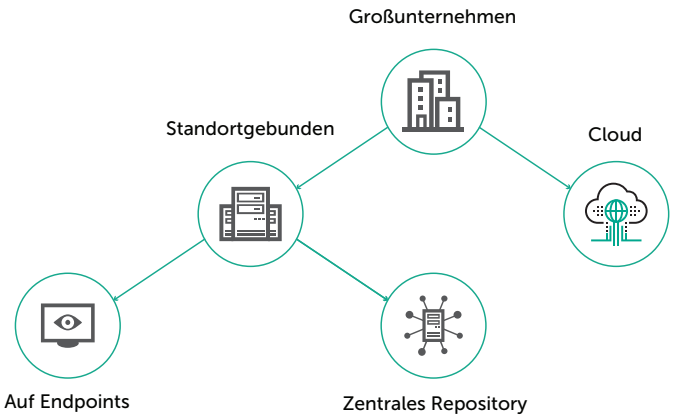
2

Verantwortung für gesammelte und gespeicherte Daten

Ein weiterer wichtiger Punkt im Zusammenhang mit Daten ist die Art und Weise, wie diese gesammelt und gespeichert werden. Sie sollten einem EDR-Anbieter hierbei folgende Fragen stellen:

- Wie viele Daten werden gespeichert und warum?
- Welche Daten werden gespeichert?
- Wo werden sie gespeichert?

Es gibt mehrere mögliche Ansätze für die Speicherung:



Sehen wir uns diese näher an:

Cloud

Viele Anbieter bieten Cloud-Lösungen zur Datenspeicherung oder sogar zur Verwaltung von EDR-Agenten (sogenannte MDR) an. Diese sind praktisch, aber durch die Menge der Daten beschränkt, die sie gleichzeitig hochladen können. Dazu gehört auch eine offene Leitung, die Daten der Organisation nach außen überträgt, was in manchen Umgebungen problematisch sein kann. Wenn Sie diese Option in Betracht ziehen, sollten Sie unter anderem folgende Fragen stellen:

- Sind wir dazu bereit, Sicherheitsdaten in eine öffentliche Cloud zu senden? Wie viel Kontrolle haben wir?
- Ist der Anbieter oder Cloud-Anbieter (u. U. ein Drittanbieter), der meine Daten speichert, vertrauenswürdig? Wie gut sind seine eigenen Cybersicherheitsvorkehrungen?
- Könnte die Nutzung dieses Services gegen die Einhaltung interner Sicherheitsstandards und/oder gesetzlicher Vorschriften verstoßen?
- Wenn nur kleine Mengen unkritischer Daten in die Cloud gesendet werden, wie effektiv kann dann die Lösung sein?

Agentenbasiert

Ein lokaler Cache auf jedem Gerät stellt einen Kompromiss zwischen umfassender Speicherung und der Cloud dar. Dieser Ansatz schont die Netzwerkressourcen und erlaubt die parallele Unterstützung einer großen Anzahl von Agenten. Wichtige Informationen werden im Endpoint-Cache selbst gespeichert, und alle Analysen erfolgen in Echtzeit durch Abfragen. Dezentrale Speicherung ist jedoch nicht immer der schnellste und effektivste Weg, um Informationen zu analysieren und auf diese zu reagieren. Wenn z. B. ein Teilsegment des Netzes nicht verfügbar ist, können Daten der betroffenen Maschinen nicht in die Gesamtanalyse einbezogen werden.

Zentrales Repository „on premise“

Alle wesentlichen Informationen werden gesammelt und von einem dedizierten Server mit einem Repository analysiert. Eine lokale Datenbank und Analysetools (z. B. eine Sandbox) erledigen dann die ganze Arbeit. Dieser Ansatz hat eine Reihe von Vorteilen: Daten werden nicht auf potentiell gefährdeten Geräten gespeichert, wie es theoretisch bei agentenbasierter Speicherung der Fall sein kann. Die Ressourcen des Computers werden nicht belastet, und Sie können in Echtzeit Endpoint-Abfragen und schnelle Suchen über die Datenbank selbst durchführen. Solche lokalen Lösungen sind besonders dann nützlich, wenn Vorschriften oder Sicherheitsstandards verlangen, dass keine Daten außerhalb der Organisation gelangen dürfen.

Empfehlungen:

- Prüfen Sie beim Thema Cloud-Speicher Ihren Cloud EDR-Anbieter im Hinblick auf Datenschutz und -kontrolle.
- In sensiblen Umgebungen, in denen die Einhaltung gesetzlicher Vorschriften die externe Datenübertragung potentiell einschränken kann, müssen Sie unter Umständen Optionen für eine lokale, vollständig isolierte Implementierung und die private Bereitstellung von Threat Intelligence prüfen.
- Überprüfen Sie bei agentenbasierter Datenspeicherung, was geschieht, wenn ein Endpoint nicht verfügbar ist oder befallen wurde (wie der Agent selbst, der PC und die Daten geschützt werden).
- Bei On Premise-Lösungen sollten Sie die interne Datenspeicherkapazität und die Menge der von jedem Gerät gesendeten Daten überprüfen.

Die Anzahl der Agenten diktiert die Hardware-Anforderungen: Wenn eine EDR-Lösung nur einen kleinen Server benötigt, um Hunderttausende von Agenten zu unterstützen, kann etwas nicht stimmen. Im Durchschnitt generiert ein Endpoint pro Tag etwa 10 Megabyte an nützlicher Telemetrie. Wenn Sie also 10 000 Knoten haben, geht es um 100 Gigabyte Daten pro Tag – oder 3 TB bei einer einmonatigen retrospektiven Datenbank.

3

Erkennung: manuelles Aufspüren vs. automatisierte Engines

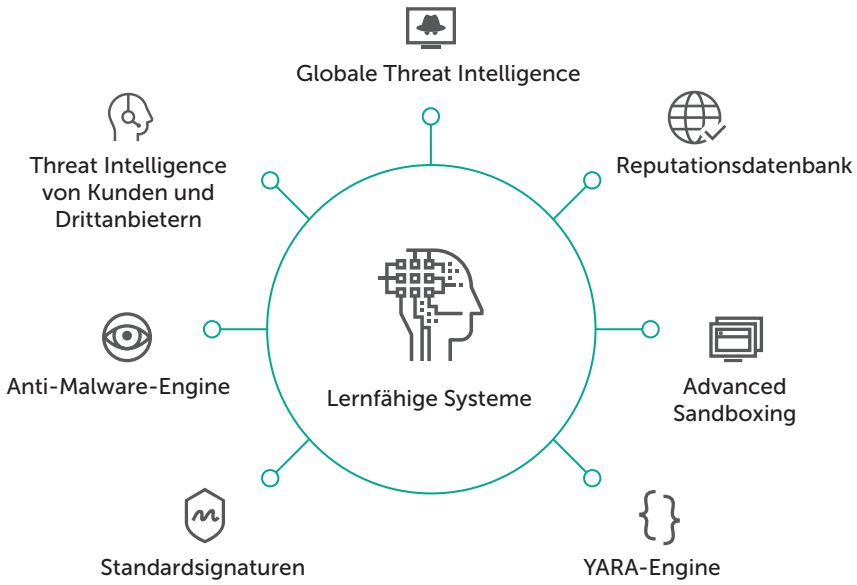
Das Thema Daten und Speicher wäre soweit erledigt. Kommen wir nun zur Datenanalyse – der Bedrohungssuche und -überwachung, die manuell mit den Toolkits, Datenbanken und Ressourcen Ihres Anbieters und automatisch über das EDR-System selbst durchgeführt wird. Je früher ein Angriff erkannt wird, desto geringer sind die finanziellen Verluste und desto weniger Störungen treten auf. Die Geschwindigkeit und Effektivität der Erkennung sind also von größter Bedeutung – und manuelle Erkennungstechniken allein sind in der Regel nicht der schnellste und effizienteste Ansatz. Viele Anbieter bieten sogenannte „moderne Erkennungstechniken“ an – IoC-Scanning von Endpoints in Echtzeit oder die schnelle Suche über Datenbanken mit zentral gespeicherten forensischen Daten – und bereichern die Vorfallserkennung so um ein automatisiertes Element.

Um Ihre aggregierten Daten optimal nutzen zu können, benötigen Sie leistungsstarke automatisierte Datenanalyseverfahren, die Ihren Analysten helfen, die über das Netzwerk auftretenden Risiken und Bedrohungen aufzuspüren. Mehrdimensionale und mehrstufige Analysen sollten nicht nur kontinuierlich neue Sicherheitsvorfälle, sondern auch verwertbare Informationen liefern, um Ihrem Sicherheitsteam dabei zu helfen, die richtigen Entscheidungen zu treffen und unnötige Zeit für unkritische Ereignisse zu sparen.

Solche hoch entwickelten Erkennungs- und Bedrohungsentdeckungs-Technologien sollten nicht nur gewöhnliche schädliche Aktivitäten zutage fördern, sondern auch über Malware hinaus komplexere Sicherheitsverletzungen aufdecken. Hier geht es nicht um die Filterebenen von Präventionstechnologien, die die Grundlage der meisten EPP-Lösungen bilden, sondern um hoch entwickelte Analysesysteme.

Sicherheitslösungen, die mehrere Erkennungstechnologien verwenden, können Angriffe und Eindringlinge schneller erkennen, bevor der Organisation ernsthafter Schaden zugefügt wird. EDR-Lösungen sollten integrierte Erkennungs-Engines für hochentwickelte Bedrohungserkennung beinhalten, die statische, verhaltensbasierte und dynamische Analysen mit Echtzeitzugriff auf globale Threat Intelligence und lernfähige Technologien kombiniert.

Das Hauptziel besteht also darin, möglichst viele verschiedene Erkennungs-Engines zu nutzen, um intern „Virenanalyselabor"-Funktionen bereitzustellen und damit Prognosen zu prüfen, neue Untersuchungen zu starten oder bereits laufende Untersuchungen zu unterstützen.



Je nach Anbieter werden die verwendeten Erkennungstechniken und -Engines mit hoher Wahrscheinlichkeit aus einem manuellen Toolkit und automatisierten Systemen bestehen:

Manuelle Erkennungshilfen

- Upload von Gefährdungsindikatoren und automatisierte/manuelle Suche
- Schnelle Suche über retrospektive Daten
- Sandboxing (die Möglichkeit, ein bestimmtes Objekt an eine dedizierte oder Cloud-basierte Sandbox zu senden)
- Zugang zu den Threat Intelligence-Quellen des Anbieters

Automatisierte Erkennung

- Malware-Schutz
- YARA-Regeln (anpassbar durch den Anbieter und/oder Ihr Sicherheitsteam)
- Threat Intelligence (automatisch vom Anbieter bereitgestellt)
- Reputationsdienste (Dateien und/oder Domains)
- Automatisierte Sandbox-Analyse der verdächtigen Objekte
- Lernfähige Systeme
  - Deep Learning (ohne Signatur – neuronales Netz)
  - Künstliche Intelligenz (Baselining, Verhaltensanalyse)

Empfehlungen:

- Erkundigen Sie sich bei Ihrem EDR-Anbieter, welche Erkennungstechnologien verfügbar sind und zum Einsatz kommen.
- Finden Sie heraus, ob interne, OEM- oder Open-Source-Erkennungs-Engines verwendet werden.
- Verschaffen Sie sich einen Überblick über die Qualität und Aktualität der Threat Intelligence, die diese Engines nutzen.
- Wenn mehrere Erkennungstechnologien genutzt werden, wie werden diese integriert und korreliert? (Es sollte nicht vorkommen, dass separate Vorfälle für dasselbe Ereignis in verschiedenen Engines protokolliert werden.)

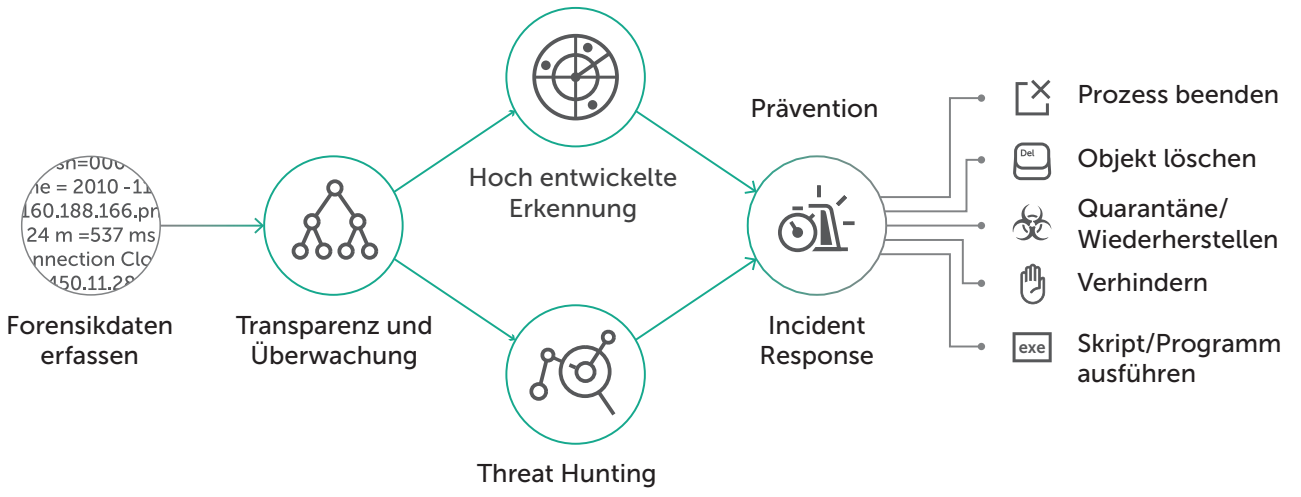
4

Effektives Reagieren

Das Reagieren auf einen Vorfall führt nur dann zu einer Lösung, wenn es effektiv gestaltet wird. Der Reaktionsprozess wird aktiviert, sobald ein Sicherheitsvorfall durch erste Einschätzungen und Untersuchungen bestätigt wurde. Sobald bestätigt ist, dass es sich nicht um einen Fehlalarm handelt, ist eine schnelle und präzise Reaktion erforderlich.

Der Vorfallsreaktionsprozess hängt von der Schwere des Vorfalls ab. Die meisten Vorfälle haben eine relativ geringe Auswirkung auf das Unternehmen (und werden sofort beim versuchten Eindringen erkannt). Aber es wird auch solche geben, die zu einer ernsten Situation führen können – eine schwerwiegende Datenschutzverletzung, Finanzkriminalität, Spionage oder noch schlimmer. Dies sind die kritischen Situationen, die eine Notfallreaktion und Untersuchungen erfordern.

Wenn Sie über die Sicherheitslösung eines Drittanbieters oder Ihr EDR-Produkt manuell eine potentielle Bedrohung entdeckt oder eine Sicherheitswarnung davor erhalten haben, was passiert dann als Nächstes? Haben Sie die Ersteinschätzungs-, Untersuchungs- und Antwortprozesse für Ihr Unternehmen festgelegt? Ohne diese kann Ihr Sicherheitsteam schnell vom Workflow rund um eine EDR-Lösung überfordert sein.



Das Aufspüren einer aktiven Bedrohung ist der entscheidende erste Schritt zur Abwehr eines Angriffs. Nachdem Sie die Bedrohung erkannt haben, müssen Sie möglicherweise schnell auf Tausenden von Endpoints reagieren. Eine wirksame EDR-Lösung ermöglicht die zentrale Verwaltung von Vorfällen über alle Endpoints des Unternehmensnetzwerks hinweg – mit einem nahtlosen Workflow. Darüber hinaus hilft Ihnen eine große Anzahl automatisierter Reaktionen, herkömmliche Beseitigungsmechanismen – wie z. B. Löschung und Re-Imaging – und damit einhergehende kostspielige Ausfallzeiten und Produktivitätsverluste zu vermeiden.

Die Kernfunktionalität der Reaktion hängt vom Ansatz des Anbieters ab, der Fokus sollte aber auf diesen gängigen Vorgehensweisen liegen:

- Verbot der Ausführung von PE-Dateien, Office-Dokumenten und Skripten
- Fähigkeit zur Remote-Löschung der Datei auf der jeweiligen Workstation
- Verschieben der Datei von der Workstation in die Quarantäne sowie Wiederherstellung bei Bedarf
- Abrufen der Datei und Durchführen einer Analyse während der Untersuchung (z. B. erzwungene Sandbox-Ausführung)
- Erzwungenes Herunterfahren des Prozesses
- Starten des Programms/Skripts an der jeweiligen Workstation

Einige Anbieter geben unter Umständen zusätzliche Szenarien für detailliertere Reaktionen an. Dazu gehören beispielsweise Szenarien zur Netzwerkisolierung, Prozessisolierung, Benutzerdeaktivierung, Rollback und Behebung.

Empfehlungen:

Halten Sie Ausschau nach:

- Anbietern, die in der Lage sind, leistungsstarke, umfassende Threat Intelligence-Datenbanken zu verwalten und Ihnen bei Bedarf fachkundigen Support und Beratung zu bieten
- EDR-Lösungen, die durch hilfreiche Schulungskurse unterstützt werden, in denen Ihr Sicherheitsteam lernt, effektive Prozesse zu implementieren und das Beste aus Ihrer Investition herauszuholen
- Einem nahtlosen Workflow zwischen Erkennung, manuellem Threat Hunting, IOC- und Vorfallsreaktionsprozessen von Drittanbietern, ohne dass zwischen verschiedenen Konsolen oder Lösungen gewechselt werden muss
- Agenten, die für den Endbenutzer auch während Untersuchungen im Hintergrund laufen, das Benutzerverhalten nicht beeinflussen und nicht zu Ausfallzeiten beitragen

5

Prävention – EDR oder EPP?

In EDR-Lösungen werden vermehrt Präventionselemente integriert, um eine „All-in-one"-Lösung anbieten zu können. Mit zunehmend ausgereiften Präventionsfunktionen werden die Funktionen für Endpoint-Prävention, -Transparenz, -Erkennung und -Reaktion möglicherweise zu einem einzigen Endpoint-Produkt zusammenwachsen.

So weit sind wir allerdings noch nicht. Auch wenn es vielversprechend klingt, nach einer Lösung zu suchen, die neben Erkennung und Reaktion auch Prävention umfasst, empfehlen wir Ihnen, diesem Aspekt zum jetzigen Zeitpunkt nicht allzu viel Beachtung zu schenken. Wählen Sie Ihr Produkt in erster Linie anhand der Transparenz-, Erkennungs- und Reaktionsfunktionalität. Wenn die Lösung auch Präventionselemente enthält, ist das ein Bonus. Seien Sie jedoch vorsichtig bei Next-Generation-EDR-Lösungen mit unausgereiften Präventionsfunktionen. Wenn Sie versuchen, Ihre herkömmliche EPP-Lösung durch eine EDR-Lösung zu ersetzen, werden Sie wahrscheinlich nicht die gleichen Präventionskapazitäten erreichen.

Allerdings kaufen oder entwickeln viele EPP-Anbieter inzwischen eigene EDRs. Wenn Sie mit Ihrem derzeitigen EPP zufrieden sind und Ihr EPP-Anbieter eine EDR-Lösung anbietet, ist es sinnvoll zu prüfen, wie beide interagieren und wie sie in Ihrem Sinne zusammenarbeiten könnten – insbesondere, wenn dies bedeutet, dass Sie keinen zweiten Agenten für EDR installieren müssen.

Empfehlungen:

- Sehen Sie sich die Roadmap des EDR-Produkts an, und prüfen Sie, wie sich das Produkt im Laufe der Zeit weiterentwickeln kann, um zusätzliche Präventionsfunktionen bereitzustellen.
- Wenn Ihnen die Idee der Integration von Endpoint-Schutz, Erkennung und Vorfallsreaktion gefällt, prüfen Sie das EPP-Angebot Ihres aktuellen EDR-Anbieters und vergleichen Sie es mit den EPP-Funktionen anderer EDR-Anbieter.
- Informieren Sie sich über die Architektur des EDR-Produkts und insbesondere über die Möglichkeit, einen einzigen Agenten sowohl für EPP als auch für EDR zu verwenden.

Die Zukunft der Endpoint-Sicherheit in Unternehmen

Die Marktführer werden versuchen, neue Technologien einzuführen und die interne Entwicklung zu nutzen, um ihre EDR-Kompetenz zu verbessern.

Für Sicherheitsexperten ist der Endpoint-Sicherheitsmarkt derzeit mit verschiedenen Anbietern stark übersättigt. Allmählich wird deutlich, dass das nicht so bleiben wird. Große Anbieter werden letztlich kleinere Unternehmen übernehmen und deren Produkte einsetzen, um Portfoliolücken zu schließen und ihre Marken zu verbessern. Die Marktführer werden versuchen, neue Technologien einzuführen und die interne Entwicklung zu nutzen, um ihre EDR-Kompetenz zu verbessern.

Die Next-Generation-Endpoint-Sicherheit, die sowohl traditionelle Kontroll- und Schutzmethoden als auch hoch entwickelte Technologien bietet, wird sich durch die Bemühungen der wichtigsten Akteure auf dem EPP-Markt weiterentwickeln. Die aktuelle Generation hoch entwickelter Endpoint-Sicherheits-Agenten, wie z. B. EDR, bietet lediglich Elemente echter EPP-Funktionalität – sie zielen derzeit nicht darauf ab, die Rolle einer voll funktionsfähigen Endpoint-Schutz-Suite einzunehmen.

Endpoint-Sicherheit rückt immer mehr in den Fokus des Unternehmens und wird in Zukunft ein immer stärker beachteter Aspekt sein. Zukünftige Kunden werden ihre Sicherheitsstrategien anpassen und weiterentwickeln und sich dabei auf fortschrittliche Technologien für den Endpoint-Schutz sowie die Überwachung der Endpoint-Aktivität konzentrieren.

Technologisch gesehen werden solche hoch entwickelten Lösungen einen anpassungsfähigen Ansatz für Schutzlösungen darstellen, dabei aber gleichzeitig Systeme stärken, schädliche Aktivitäten verhindern und hoch entwickelte Erkennung bieten. Cloud-basierte Threat Intelligence, maschinelles Lernen im lokalen System, Threat Hunting einschließlich aktiver Reaktion und rascher Untersuchung sowie tiefgreifende Verhaltens- und Bedrohungsanalyse werden ebenfalls eine Rolle spielen.

Direkte Empfehlungen

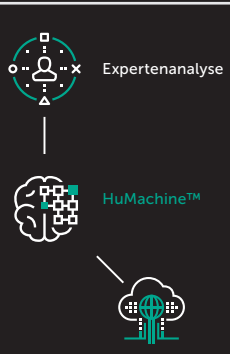
Sicherheitsexperten erkennen den steigenden Bedarf an tieferer Endpoint-Analyse und Endpoint-Schutz und sind nun bei begrenztem Budget mit einer langen Liste von Anforderungen konfrontiert, die es zu erfüllen gilt. Aber auch ohne Budget ist es sinnvoll, aktuelle Technologien und mögliche zukünftige Entwicklungen dahingehend zu bewerten, wie sie sich mit Ihren Geschäftszielen und internen Möglichkeiten vereinbaren lassen. Durch ganzheitliche Betrachtungen und Testen der Optionen lenken Sie die Aufmerksamkeit der Entscheidungsträger in Ihrem Unternehmen auf die Möglichkeiten und Chancen neuer Technologien. Sie können künftigere IT-Sicherheitsbudgets präziser planen und wissen, dass Sie fundierte Entscheidungen über anstehende Investitionen treffen können.

Sofort zu ergreifende Maßnahmen

1. Bewerten Sie Ihre Sicherheitsfunktionen als Ganzes. Wie schnell und wie einheitlich ist Ihr aktueller Prozess der Vorfallsreaktion? Nutzen Sie derzeit – von EDR-Überlegungen einmal abgesehen – die für Sie optimalen Lösungen aus? Wie sehen Sie das Ganze im Verhältnis zu Ihrer Branche und Ihren Mitbewerbern?
2. Verschaffen Sie sich einen Überblick über Ihre aktuellen Erkennungsmöglichkeiten bei Endpoints. Nutzen Sie Analysen durch und testen Sie zusätzliche Informationsquellen – zum Beispiel die Verwendung von Threat Data Feeds mit Ihrem SIEM.
3. Denken Sie darüber nach, wie Sie beginnen können, Ihre Expertise im Bereich der Vorfallsreaktion intern zu erweitern. Bewerten Sie die Fähigkeiten Ihres Teams und eruieren Sie effektive Schulungsmöglichkeiten.
4. Bestimmen Sie Ihren tatsächlichen bzw. zukünftigen Bedarf, und prüfen Sie die EDR-Lösungen, die in dieser Hinsicht in die engere Wahl kommen.

Nützliche Links

1. Richtlinien zur Vorfallsreaktion: https://cdn.securelist.com/files/2017/08/Incident_Response_Guide_eng.pdf
2. Bewerten Sie Ihre Sicherheit mit diesem IT-Sicherheitskalkulator, und laden Sie den Global Enterprise Report herunter: https://calculator.kaspersky.com/de/



Kaspersky Lab
Enterprise Cybersecurity: www.kaspersky.de/enterprise
Neues über Cyberbedrohungen: de.securelist.com
IT-Sicherheitsnachrichten: https://www.kaspersky.de/blog/b2b/

#truecybersecurity
#HuMachine

www.kaspersky.de