WARUM SIE EDR BRAUCHEN

Ein Leitfaden für kleine und mittlere Unternehmen

F-Secure

INHALT

WARUM SIE EDR BRAUCHEN

Ihr Netzwerk wird gerade angegriffen. Oder nicht?

Trotz steigender Investitionen in Cybersicherheit können die meisten IT-Verantwortlichen diese Frage nicht zu 100 % beantworten, da sie so vieles ständig im Auge behalten müssen: Nutzer, Geräte, Anwendungen, Alarme, Schwachstellen, Patches u. v. m. IT-Teams, besonders in kleineren Unternehmen, haben schlicht nicht die Zeit, ihre Netzwerke rund um die Uhr zu überwachen.

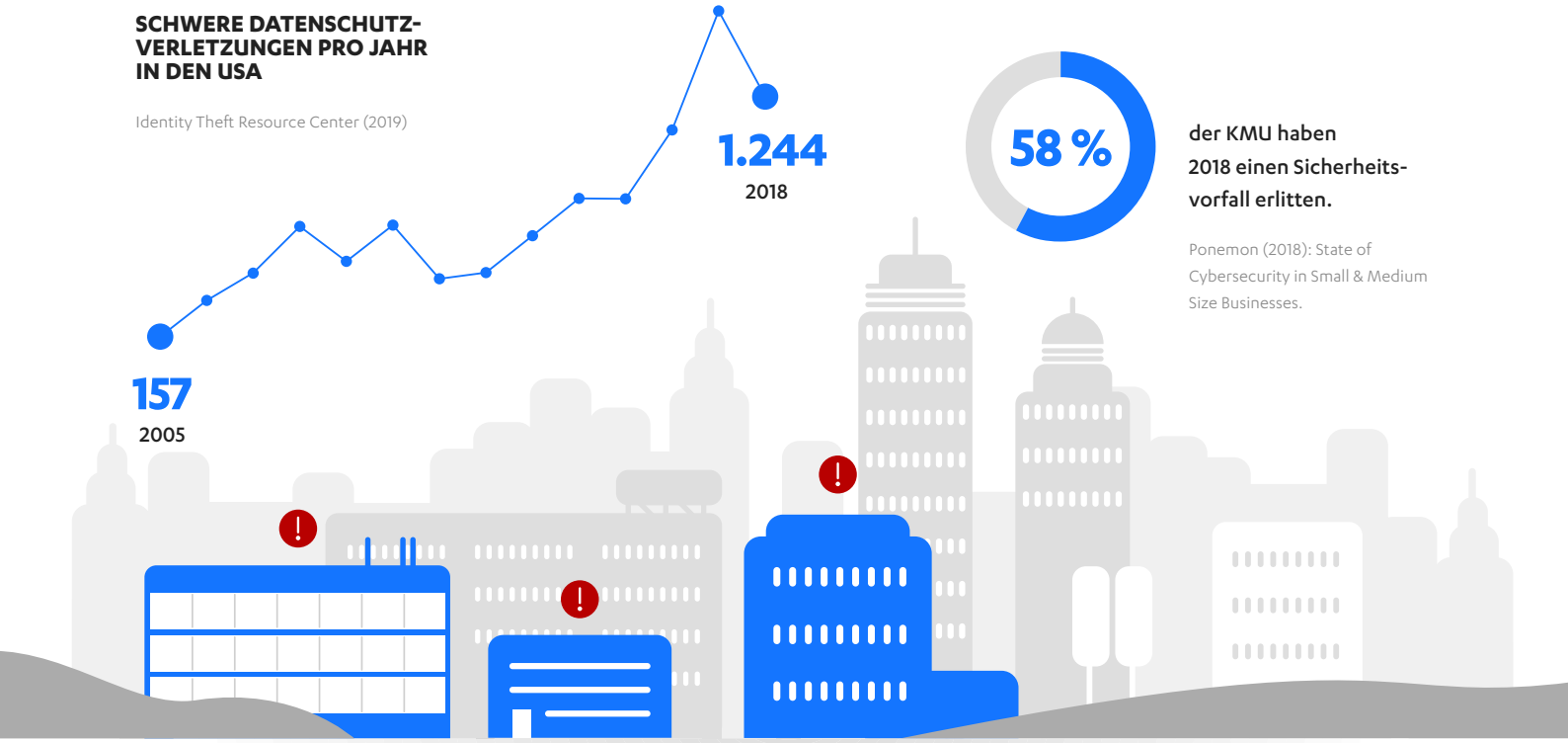
Bis jetzt ist es bei fast zwei Dritteln der global operierenden Organisationen zu Sicherheitsverletzungen gekommen[1], wobei 56 % dieser Vorfälle monatelang oder noch länger nicht entdeckt wurden[2]. Und je länger sie unentdeckt bleiben, desto teurer wird das Ganze. Die Kosten für Gegenmaßnahmen können schnell mehrere tausend Euro pro Tag erreichen.

Die Angriffe zielen genauso auf kleinere Unternehmen: Fast 58 % der KMU haben 2018 einen Sicherheitsvorfall erlebt[3]. In dieser Unternehmensgröße sind die Folgen sogar noch ernster: Die National Cyber Security Alliance schätzt, dass 60 % der betroffenen KMU innerhalb von sechs Monaten nach dem Vorfall schließen mussten[4].

Die Lage sieht düster aus: Angreifer überwinden links und rechts die Verteidigungslinien. Was können Sie als IT-Verantwortlicher mit beschränkten Ressourcen, aber endlosen Pflichten überhaupt tun?

Entdecken Sie **Endpoint Detection and Response,** häufig abgekürzt als **EDR.** EDR-Lösungen stärken den **Endgeräteschutz** (Anti-Malware, Spamfilter usw. Ihres Unternehmens) und verbessern Ihre Entdeckungs- und Reaktionsfähigkeiten gewaltig. Der Endgeräteschutz ist wie eine Mauer, und EDR ist das Sicherheitsteam, das patrouilliert und aufpasst, dass keiner drüberklettert. Es ist die nächste Linie, wenn Ihre Präventivmaßnahmen einen Angriff übersehen oder einem Ihrer Geräte ein wichtiger Patch fehlt. Selbst wenn es ein Angreifer schafft, ins System zu gelangen, können Sie die Bedrohung immer noch aufspüren und stoppen.

EDR wird immer wichtiger. Dennoch tun sich viele IT-Fachleute schwer, die Vorteile für ihr Unternehmen zu quantifizieren. Um Ihnen dabei zu helfen, haben wir diesen Leitfaden erstellt. Er erklärt, wie EDR funktioniert, warum EDR so wichtig ist und wie Sie sich mit EDR optimal aufstellen. Dazu gibt es noch praktische Infos und Tipps zur Beurteilung von EDR-Anbietern.



WIE EDR FUNKTIONIERT

EDR sammelt mithilfe von schlanken Sensoren eine Unmenge von Verhaltensdaten (Prozesse, Netzwerkverbindungen, Dateiausführungen etc.) der PCs und Server. Diese Daten sind äußerst hilfreich, um Angriffe zu entdecken, aber in der Masse für menschliche Analysten nicht mehr durchschaubar. Wir sprechen hier von Millionen, gar Milliarden von Informationsschnipseln, in denen sich einige echte Bedrohungen verbergen: die sprichwörtliche Nadel im Heuhaufen.

Mit fortschrittlichen Analysetechniken und maschinellem Lernen kann EDR diese Daten durchforsten und Angriffsindikatoren ausmachen, sodass sowohl bereits bekannte als auch neue Bedrohungen entdeckt werden. Das geschieht vor allem dadurch, dass EDR akzeptiertes Nutzerverhalten mit den Sensordaten abgleicht und so ungewöhnliche Ereignisse identifiziert. Einige Beispiele:

- Erkennung dateiloser Malware-Angriffe, die über Webseiten, PDF-Dokumente im Browser oder Makros in MS-Office-Dateien verbreitet werden.
- Identifizierung von ungewöhnlichen und unüblichen Prozessen, die von Arbeitsplatzrechnern ausgehen.
- Erkennung völlig neuer Arten von Malware, auch wenn es dazu noch keine Signaturen gibt.
- Warnung, wenn Mitarbeiter unbekannte oder schädliche Anwendungen einsetzen.
- Isolation kompromittierter Computer und Server, sodass sich ein Angriff nicht weiter ausbreiten kann.

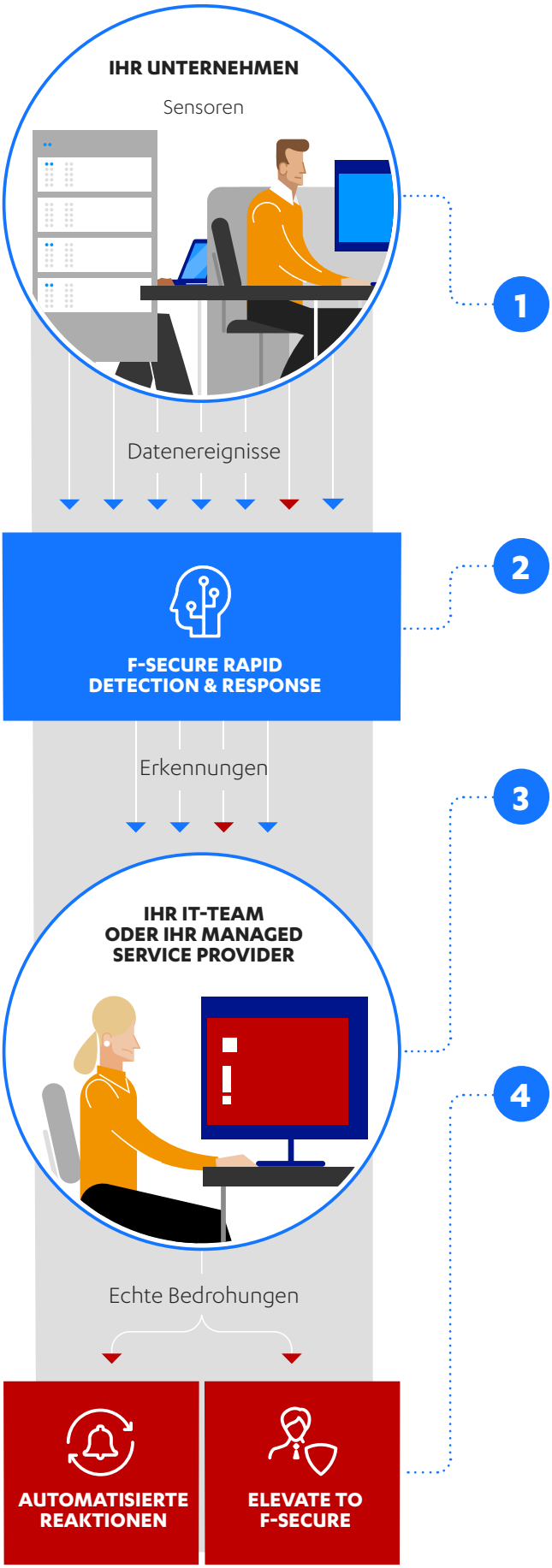
Anstatt Sie mit Fehlalarmen zu überschütten, grenzt EDR die Liste schnell und genau auf die Dinge ein, die wichtig sind. Bei einem Kunden hat die EDR-Lösung von F-Secure in einem Monat über zwei Milliarden Ereignisse erfasst, von denen 15 echte Bedrohungen waren.

Sind die Bedrohungen identifiziert, hilft Ihnen EDR mit automatisierten Aktionen und Vorschlägen dabei, die Vorfälle zu untersuchen und darauf zu reagieren. Dies ist für kleinere Unternehmen enorm wichtig, da sie meist nicht über die Ressourcen und das Fachwissen verfügen, um sich bei komplizierten Attacken selbst zu helfen. Mit einer EDR-Lösung wie F-Secure Rapid Detection & Response erfahren Sie nicht nur, welche Probleme Ihre IT hat, Sie erhalten auch konkrete Lösungshilfe.

EIN BEISPIEL

Ein Notebook, das einem jungen Marketing-Mitarbeiter gehört, lädt Daten auf einen unbekannten Server im Internet hoch. EDR entdeckt dieses verdächtige Verhalten innerhalb von Minuten, isoliert den Computer automatisch vom restlichen Netzwerk und alarmiert Ihr IT-Team. Mit der Hilfe von EDR erkennt Ihr Team schnell, dass es sich um einen Angriff handelt (der Computer des Mitarbeiters wurde kompromittiert), und untersucht dessen Ursprung. Sie finden heraus, dass ein schädlicher E-Mail-Anhang den Prozess gestartet hat. Ihr IT-Team bereinigt dann das kompromittierte Gerät, passt die Einstellungen Ihres Spamfilters an, um zu verhindern, dass Mitarbeiter zukünftig solche E-Mail-Anhänge erhalten, passt die Firewall-Regeln an, um Verbindungen zu dieser Domain zu blockieren, und informiert die Nutzer über die aktuellen Risiken.

In diesem Beispiel wurde keine traditionelle Malware gefunden – also gab es auch nichts, was Ihr Endgeräteschutz hätte blockieren können. Ohne EDR hätten Sie gegen einen unsichtbaren Feind kämpfen müssen.



So funktioniert unsere EDR-Lösung F-Secure Rapid Detection & Response:

Sensoren auf Ihren Windows-PCs, Macs und Servern zeichnen das Nutzungsverhalten in Ihrer Organisation auf. Die gesammelten Datenereignisse werden zur Echtzeitanalyse an unsere Cloud-Datenbank gestreamt. Die Sensoren sind für die Endanwender unsichtbar, und Ihr IT-Team muss keine zusätzlichen Anstrengungen unternehmen, um Ihre IT-Umgebung zu überwachen.

Unser Cloud-Backend untersucht die gesammelten Daten und trennt verdächtige Ereignisse von normalem Nutzerverhalten. Dies geschieht durch Verhaltens-, Reputations- und Big-Data-Analysen in Echtzeit sowie mit maschinellem Lernen. Die Analyse läuft selbstständig ab, Eingriffe seitens Ihres IT-Teams sind nicht nötig.

Eine gefilterte Liste von Alarmen erscheint auf Ihrem Dashboard, mit klaren Visuals und Infos zu Angriffen. Sie können schnell und einfach alle betroffenen Hosts und die damit verbundenen Ereignisse auf einer Timeline erkennen. Die Vorfälle werden auch in Kontext gesetzt, sprich: Sie erfassen die Relevanz der betroffenen Hosts, die derzeitige Bedrohungslandschaft und aktuelle Risiko-Level. So wissen Sie auf einen Blick, was jetzt Priorität hat.

Echte Bedrohungen werden vom Netzwerk isoliert. Sie haben nun zwei Möglichkeiten:

a) Sie können dieses Problem mit Ihrem eigenen IT-Team untersuchen und darauf reagieren, indem sie die automatisierten Reaktionen und Anleitungen nutzen, die unsere Lösung bereitstellt. Falls sich ein zertifizierter F-Secure-Dienstleister um Ihre Sicherheit kümmert, wird er die nötigen Schritte für Sie unternehmen.

b) Sie können das Problem per **Elevate to F-Secure** an die Incident-Response-Experten von F-Secure weiterleiten. Diese werden dann die Bedrohung untersuchen und Ihnen Ratschläge geben, wie Sie die Bedrohung eliminieren, bevor Ihr Unternehmen Schaden nimmt.

WIE FORTSCHRITTLICHE ANGRIFFE ABLAUFEN

Um zu verstehen, wie EDR Ihre Organisation vor gezielten und fortschrittlichen Angriffen schützt, müssen wir uns ansehen, wie die Angreifer vorgehen. Um Ihre präventiven Schutzmaßnahmen zu überwinden, fangen Cyberkriminelle meist mit einer dieser Taktiken an:

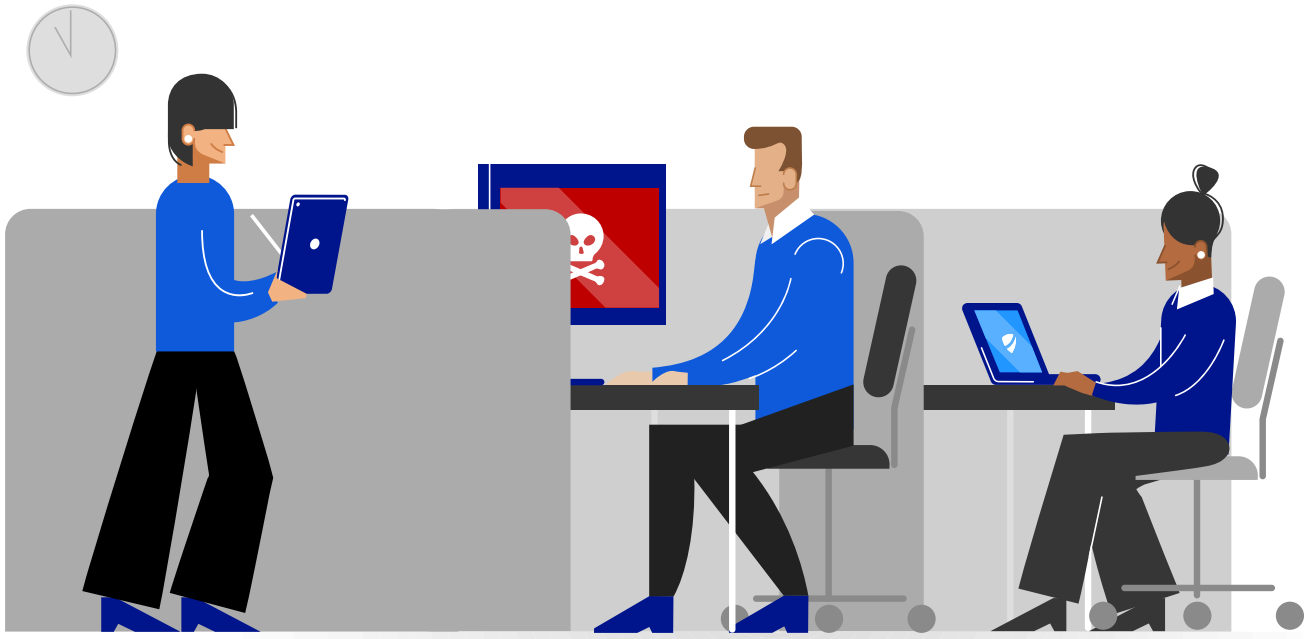
1. **Ausnutzen einer Schwachstelle:** Bekannte Schwachstellen in Ihren öffentlich zugänglichen Systemen sind ein attraktives Ziel: 57 % der Sicherheitsverletzungen haben mit solchen Schwachstellen zu tun, die man hätte patchen können[5]. Bei über 16.000 neuen Sicherheitslücken pro Jahr fällt es den meisten Unternehmen sehr schwer, ihre Infrastruktur stets aktuell zu halten[6]. Mit automatischen Tools durchkämmen opportunistische Angreifer das Internet nach diesen Schwachstellen und spüren eventuell tausende nicht gepatchter Geräte auf.

2. **Spear Phishing:** Gezielt irreführende Kommunikation führt Mitarbeiter aufs Glatteis, sodass sie vertrauliche Informationen preisgeben oder eine ausführbare Datei öffnen. Spear Phishing ist weit verbreitet und sehr effektiv: Der jährliche Verizon Data Breach Investigations Report schätzt, dass 32 % der Sicherheitsverletzungen mit dieser Art von Angriffstaktik zu tun haben[2].

3. **Watering Hole:** Der Angreifer sucht nach Schwachstellen in Webseiten, die von Ihren Mitarbeitern oft angesteuert werden. Er fügt dann einen Schadcode in JavaScript oder HTML auf diesen Seiten ein, der die Opfer auf eine andere, und zwar eine kompromittierte Seite leitet, wo die Malware schon lauert. Wenn jemand in Ihrer Organisation nun diese Webseite besucht, schnappt die Falle zu.

4. **Man in the Middle:** Der Angreifer fängt Ihre Kommunikation ab und analysiert oder verändert sie, bevor er sie weiterleitet – und er lässt Sie im Glauben, dass Sie weiter vertrauenswürdig kommunizieren. Man-in-the-Middle-Angriffe werden aus der Nähe durch unverschlüsselte WLAN-Netzwerke oder aus der Ferne über Malware durchgeführt.

5. **Zugang erkaufen:** Kriminelle Organisationen crowdsourcen Unmengen von Angriffen auf so viele Systeme, dass immer ein gewisser Anteil davon einen Treffer landet. In vielen Fällen können sich Angreifer Zeit und Mühe sparen, indem sie sich den Zugang zu einem Unternehmen, das bereits kompromittiert wurde, einfach erkaufen. Wurde Ihr Unternehmen früher schon einmal kompromittiert? Falls ja, gibt es den Zugang zu Ihren Systemen vielleicht schon irgendwo günstig zu kaufen.



Wenn ein Angreifer erst einmal durch die Tür ist, wird er als Nächstes ausspähen, was es zu holen gibt. Er könnte neue Nutzer hinzufügen oder bestehende Nutzerkonten so verändern, dass sie mehr Rechte bekommen. Er könnte mit einem Memory-Scraping-Tool nach Domain-Admin-Passwörtern suchen oder ein System nach dem anderen nach irgendwas Interessantem durchforsten.

Natürlich möchten Angreifer dabei nicht erwischt werden. Gewiefte Kriminelle werden aus diesem Grund oft legitime Betriebssystem-Komponenten verwenden, um sich in Ihrem Unternehmen einzunisten und sich im normalen Traffic zu verbergen. Firewalls und die üblichen Produkte zum Endgeräteschutz sind nicht in der Lage, den Angreifer in dieser Phase zu entdecken.

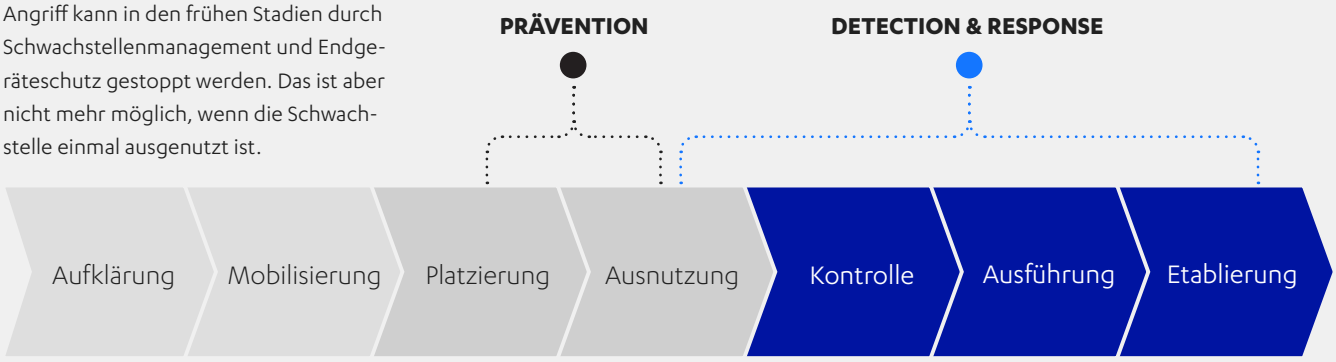
Zuletzt wird der Angreifer Ihre eigenen IT-Admin-Tools gegen Sie verwenden und sich PowerShell, Service Commands oder Windows Remote Management zunutze machen, um sich zu holen, was er sucht, etwa Kundendaten oder geistiges Eigentum. Und wenn er diese Daten ausschleust, wird er den Prozess so gestalten, dass er aussieht wie normales Nutzerverhalten. So landen Ihre Kronjuwelen auf dem Schwarzmarkt und werden an den Höchstbietenden verkauft.

Ausgeklügelte Angriffe wie dieser sind mit statischen Verteidigungsmethoden allein nicht zu stoppen, und keine Organisation sollte sich dagegen immun wähnen. Tatsächlich suchen sich die meisten Cyberkriminellen lieber kleinere bis mittlere Unternehmen aus, da diese häufig weniger Verteidigungsmechanismen und weniger IT-Sicherheitspersonal haben. KMU sind außerdem oft Teil der Lieferkette von Großunternehmen, weshalb sie ein attraktives Primärziel darstellen.

Mit EDR drehen Sie den Spieß um: Selbst wenn ein Widersacher es schaffen sollte, Ihre präventiven Sicherheitsmechanismen auszuhebeln, ist es für ihn nun sehr viel schwieriger, sich im normalen Netzwerkverkehr zu verstecken. Sie können jegliches ungewöhnliche Verhalten erkennen, bevor Ihr Unternehmen Schaden nimmt. Meist wirkt schon der Einsatz einer EDR-Lösung abschreckend auf opportunistische Cyberkriminelle.

LEBENSZYKLUS VON CYBERANGRIFFEN

Dieser schematische Ablauf zeichnet Schritt für Schritt nach, wie ein Angreifer versucht, ins Netzwerk zu gelangen. Ein Angriff kann in den frühen Stadien durch Schwachstellenmanagement und Endgeräteschutz gestoppt werden. Das ist aber nicht mehr möglich, wenn die Schwachstelle einmal ausgenutzt ist.



WAS EDR FÜR IT-VERANTWORTLICHE LEISTET

Wer für die Cybersicherheit eines Unternehmens zuständig ist, profitiert von EDR in vielfältiger Weise:

1 **Falls Sie jemand zu Ihrer Sicherheitssituation befragt, können Sie eine klare, selbstsichere und konkrete Antwort geben:** Cybersicherheit hat sich von einem IT-Nischenthema zu einem Pflichtpunkt im Risikomanagement entwickelt. IT-Manager stehen unter immer größerem Druck, den Sicherheitsstatus an das Topmanagement zu berichten. Auf die unausweichliche Frage „Wie steht es aktuell um unsere Sicherheit?" können Sie dank EDR eine umfassende, ehrliche Antwort geben. Zusammen mit Daten aus Ihren Schwachstellenmanagement- und Endgeräteschutz-Plattformen zeigen Sie klar und deutlich auf, wie gut Sie geschützt sind, welchen Angriffen das System ausgesetzt war, ob die IT-Sicherheitsrichtlinien befolgt werden usw.

2 **Sie können beruhigt sein, weil Sie wissen, dass alle Angriffe schnell aufgespürt und gemeldet werden – ohne dass Sie Ihr ganzes IT-Sicherheitsbudget aufbrauchen müssen:** Wir haben in diesem Leitfaden schon wiederholt darauf hingewiesen, dass Angriffsprävention alleine nicht mehr reicht. Effektive Erkennungs- und Reaktionsfähigkeiten zu entwickeln, ist aber nicht einfach – geschweige denn günstig –, wenn Sie bei null anfangen müssen. Eine schlüsselfertige EDR-Lösung ist dann eine hervorragende Möglichkeit für KMU, denn damit bekommen Sie alle Kernfunktionen zur Erkennung und Reaktion, zahlen aber längst nicht so viel wie Sie für vollständig gemanagte Services ausgeben müssten. Dabei geben Ihnen Lösungen wie F-Secure Rapid Detection & Response sogar einen Draht zu Sicherheitsfachleuten, der sonst meist Premium-Lösungen vorbehalten ist: Mit unserem Feature **Elevate to F-Secure** können Sie erkannte ernsthafte oder komplexe Bedrohungen direkt an die Experten unseres Incident Response Centers weiterleiten – das sind dieselben Leute, die tagtäglich die Cybersicherheit unserer Firmenkunden betreuen.

3 **Wenn eine Bedrohung entdeckt wird, können Sie sehr viel schneller reagieren und sich schützen:** Zusätzlich zur Erkennung gibt Ihnen EDR Tools und praktische Empfehlungen zum Umgang mit Sicherheitsproblemen an die Hand. Host-Isolierung, direkte Nutzerkommunikation, Gegenmaßnahmen aus der Ferne: Ihre EDR-Lösung zeigt Ihnen, wie Sie Sicherheitsvorkommnisse so schnell wie möglich lösen. Angriffe von vornherein zu unterbinden, ist zwar am besten; wenn aber doch eine aktive Bedrohung vorliegt, sind diese Tools Gold wert.

4 **Im Fall einer Sicherheitsverletzung sind Sie in der Lage, genau nachzuvollziehen, was passiert ist – und zu verhindern, dass so etwas noch einmal passiert:** Angriffe zu erkennen und zu stoppen ist das Eine – aber genauso wichtig ist es, zu verstehen, wie sie geschehen konnten. Wer die Sicherheit seiner Organisation sinnvoll stärken will, muss zurückblicken und sich die Angriffsmethoden ansehen, die erfolgreich waren. EDR sammelt alle relevanten forensischen Daten, sodass Sie den Angriff analysieren, daraus lernen und Ihre Security gegen ähnliche Versuche aufrüsten können. Ebenso wichtig sind Daten zu erfolglosen Angriffsversuchen – sie könnten darauf hindeuten, dass Sie das Ziel eines hartnäckigen Cyberkriminellen sind.

5 **Gemäß der europäischen Datenschutz-Grundverordnung (EU-DSGVO) sind Unternehmen verpflichtet, Datenschutzverletzungen innerhalb von 72 Stunden zu melden. Statt sich Sorgen um Compliance zu machen, können Sie sich sicher sein, dass Ihr Unternehmen die folgenden Voraussetzungen erfüllt:** Es ist bereits vorgekommen, dass Unternehmen, die einen Sicherheitsvorfall hatten, Strafe zahlen mussten. EDR hilft Ihnen bei der DSGVO-Compliance an zwei Fronten: Erstens können Sie den EU-Behörden zeigen, dass Sie grundlegende Maßnahmen zum Schutz Ihrer Daten ergriffen haben, indem Sie Ihre IT-Umgebung überwachen. Zweitens können Sie, falls ein Angreifer Ihre Verteidigung überwindet, genug Informationen sammeln, um dies den Behörden innerhalb der Frist von 72 Stunden zu melden.

WIE MAN EDR-ANBIETER BEURTEILT

Sie haben jetzt hoffentlich eine bessere Vorstellung von den wichtigsten EDR-Funktionsweisen und -Vorteilen. Aber woher wissen Sie, welche Lösung für Sie richtig ist?

Immerhin ist das Feld bei EDR-Anbietern gut überschaubar: Es gibt hierfür die Evaluierung durch die Non-Profit-Organisation MITRE. Sie vergleicht EDR-Lösungen mit dem ATT&CK Framework, einer laufend aktualisierten Sammlung an Taktiken, Techniken und Verfahren, die von Cyberkriminellen verwendet werden. Das gibt Unternehmen neutrale Ergebnisse zum Vergleich der Leistungen verschiedener EDR-Anbieter, außerdem Informationen zu Telemetrien, Alarmen, Schnittstellen und Outputs der jeweiligen Lösungen. Die Beurteilungen von MITRE werden von vielen Branchenführern wie Gartner und Forrester verwendet.

Im Sommer 2019 hat MITRE die EDR-Erkennung von F-Secure unter die Lupe genommen. Wir haben hervorragende Ergebnisse erzielt – sie zeigen, dass F-Secure selbst die fortschrittlichsten staatlich durchgeführten Angriffe aufspüren kann. Die Beurteilung von MITRE ist zwar kein Produktvergleich, doch Forrester hat systematisch getestet; die Ergebnisse wurden aufgeführt, bewertet und es wurde versucht, die Leistung der einzelnen Anbieter zu quantifizieren. In dieser Metrik hat F-Secure die höchste Punktzahl erreicht. Mit anderen Worten: Bei F-Secure können Sie sicher sein, dass Sie die beste EDR-Technologie bekommen. Nehmen Sie Kontakt mit uns auf, wenn Sie mehr über das MITRE ATT&CK Framework wissen möchten und darüber, wie die Testergebnisse zu lesen sind.

Die MITRE-Evaluation ist ein guter Start, aber Sie sollten noch weitere Faktoren einbeziehen. Ein EDR-Anbieter muss Ihnen mindestens Antworten auf die folgenden Fragen geben können. Wir haben unsere Antworten einmal mitgeliefert, um Ihnen ein Beispiel zu geben.

FRAGEN ZUR BEURTEILUNG VON EDR-ANBIETERN

Wie schwierig und zeitaufwendig ist Ihre EDR-Lösung in der Anwendung? F-Secure Rapid Detection & Response ist so konzipiert, dass selbst unerfahrene IT-Analysten damit klarkommen, mit übersichtlicher Nutzeroberfläche und Dashboards. Weil alle Aktivitäten der Endgeräte visualisiert werden, ist es einfach zu erkennen, wann und wie ein Angriff stattfindet. Mit unseren automatisierten Gegenmaßnahmen und eingebauter Unterstützung können Sie reagieren, auch wenn Sie kein umfassend zertifizierter Incident-Response-Experte sind.

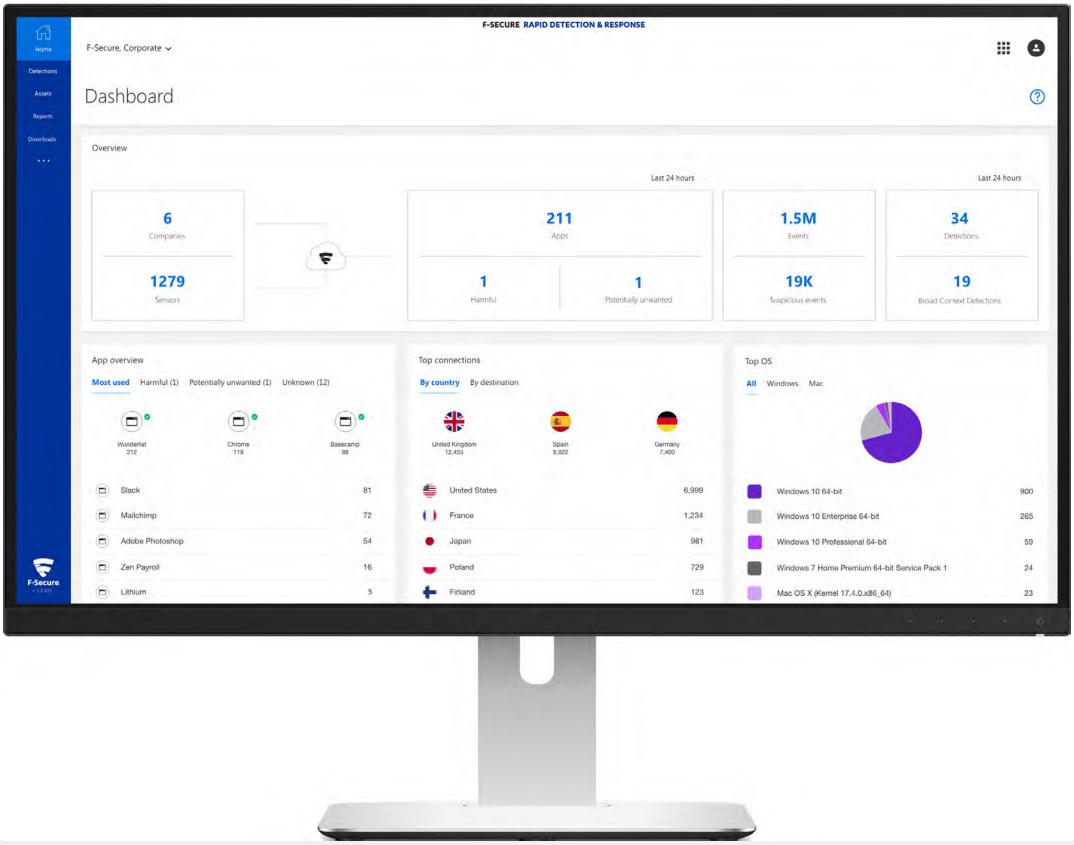
Kann die Lösung in Ihre anderen Sicherheitsprodukte integriert werden? F-Secure Rapid Detection & Response ist mit allen Endgeräteschutz-Plattformen kompatibel. Mehr noch: Sie ist komplett in unsere eigene preisgekrönte Sicherheitslösung F-Secure Protection Service for Business integriert. Mit diesem Endgeräteschutzpaket sind Sie gegen alle Bedrohungen optimal aufgestellt. Zudem können Sie beide Lösungen im selben Nutzerportal verwalten.

Wie wirkt sich die Lösung auf die Leistung der Endgeräte aus? Die Endgerätesensoren von F-Secure Rapid Detection & Response arbeiten sparsam im Hintergrund und verbrauchen nur minimale Ressourcen. Kunden berichten, dass sie für die Endnutzer praktisch unsichtbar sind – und so soll es auch sein.

Wie spürt die Lösung Bedrohungen auf? F-Secure Rapid Detection & Response verwendet zur Erkennung unsere patentierte Broad-Context-Detection-Technologie. Sie nutzt Verhaltens-, Reputations- und Big-Data-Analysen in Echtzeit zusammen mit maschinellem Lernen, sodass sie erkannte Angriffe automatisch im Kontext einordnet. Diese Erkennungen werden zudem nach Risikostufen, der Relevanz des betroffenen Hosts und vor der aktuellen Bedrohungslandschaft klassifiziert.

Welche Unterstützung bietet der Anbieter? Falls Ihr Unternehmen eine komplexe Bedrohung erlebt, bietet unsere Lösung die Option „Elevate to F-Secure“: Mit nur einem Klick erhalten Sie Hilfe von unseren geschulten Incident-Response-Experten. Außerdem können Sie F-Secure Rapid Detection & Response auch als Managed Service von unseren zertifizierten Partnern einsetzen: Sie konzentrieren sich auf Ihre IT-Kernaufgaben, während sich Experten um die Sicherheit kümmern.

Für große Unternehmen, die häufig Angriffen ausgesetzt sind, ist darüber hinaus der komplett gemanagte Threat Hunting Service interessant. Er unterbindet selbst anspruchsvollste nationalstaatliche Angriffe innerhalb von Minuten und bietet Rund-um-die-Uhr-Support unserer Bedrohungsermittler und Incident Response-Experten.



F-SECURE RAPID DETECTION & RESPONSE

- Sofort umfassende Transparenz Ihrer IT-Umgebung
- Automatisierte und unterstützte Bedrohungsabwehr
- Erkennung von Angriffen und IT-Problemen binnen Minuten
- Direkte Hilfe von F-Secure bei komplexen Ereignissen

Kostenlose Demo anfordern

QUELLEN

1 IDC (2019): Thales Data Threat Report: The Changing Face of Data Security.

2 Verizon (2019): Data Breach Investigations Report.

3 Ponemon (2018): State of Cybersecurity in Small & Medium Size Businesses.

4 Vistage (2018): Cyberthreats and solutions for small and midsize businesses.

5 Ponemon (2018): Cost of a Data Breach Report.

6 CVE Details (2019): Vulnerabilities by Date [neue Schwachstellen und Risiken pro Jahr].

ÜBER F-SECURE

Niemand hat einen besseren Einblick in echte Cyberangriffe als F-Secure. Wir schließen die Lücke zwischen Erkennung und Reaktion. Zu diesem Zweck nutzen wir die unübertroffene Bedrohungsdatenerkennung von Hunderten der besten technischen Berater unserer Branche, aus Millionen von Geräten, die unsere preisgekrönte Software nutzen, sowie durch fortlaufende Innovationen im Bereich künstlicher Intelligenz. Führende Banken, Fluggesellschaften und Unternehmen vertrauen auf unser Engagement bei der Bekämpfung der gefährlichsten Bedrohungen der Welt.

Zusammen mit unserem Netzwerk an Top-Channel-Partnern und über 200 Serviceanbietern ist es unsere Mission, all unseren Kunden maßgeschneiderte unternehmensfähige Cybersicherheit zur Verfügung zu stellen. F-Secure wurde 1988 gegründet und ist an der NASDAQ OMX Helsinki Ltd gelistet.

f-secure.com/business | twitter.com/fsecure | linkedin.com/f-secure

F-Secure