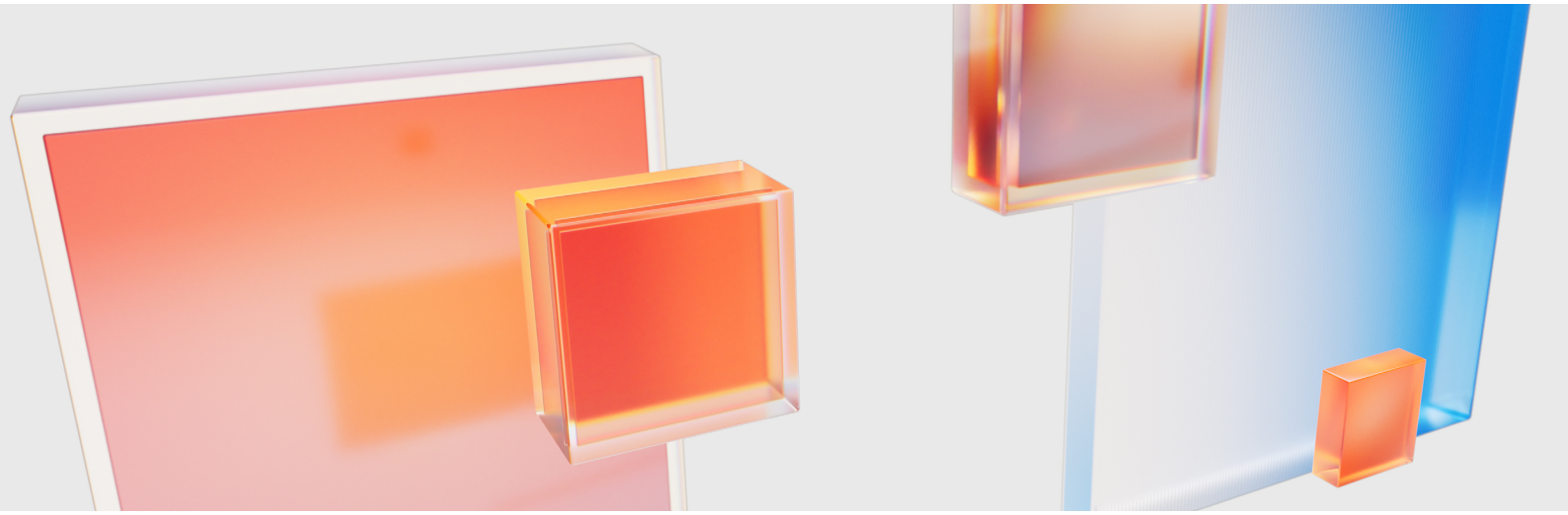
SONICWALL



Über den bloßen Schutz hinaus: Verbessern Sie die Cyberversicherungs-Compliance mit EDR

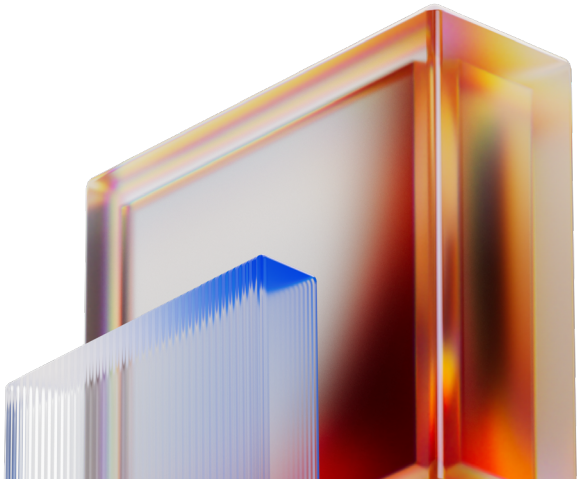
Einführung

In den ersten Monaten 2024 ist die Zahl der bekannt gewordenen Cyberangriffe um erschreckende 96 % gestiegen. Als wäre das nicht genug, dürfte sich dieser Trend in naher Zukunft aller Voraussagen nach fortsetzen.[1] Parallel zu den rasanten Entwicklungen in der Bedrohungslandschaft hat sich auch das regulatorische Umfeld schnell verändert. Besonderes Augenmerk lag dabei auf den wirtschaftlichen Auswirkungen von Cyberangriffen und den Methoden zur Risikominderung für Verbraucher und Unternehmen. So hat die SEC im Jahr 2023 neue Regeln eingeführt, die Unternehmen zur Offenlegung von Cybersicherheitsvorfällen verpflichten.[2] Diese neuen Vorschriften erhöhen den Druck, da sie ohne Zweifel erhebliche Auswirkungen auf die zahlreichen Ransomware-Angriffe und Datenlecks haben werden, die in letzter Zeit zu hohen Geldstrafen und Anwaltskosten geführt haben. Die Implementierung geeigneter Instrumente und Praktiken ist wichtig, um Bedrohungen zu verhindern und den von Cyberkriminellen verursachten Schaden zu minimieren. Neben diesen Maßnahmen haben viele Unternehmen damit begonnen, Cyberversicherungen und Garantien abzuschließen, um die Kosten für die Wiederherstellung zu decken und die Haftung im Falle eines Angriffs zu begrenzen.

Obwohl es nicht so aussieht, sind kleine und mittlere Unternehmen (KMUs) genauso anfällig für Cyberangriffe wie große Organisationen, wenn nicht sogar noch mehr. Ein Cyberangriff kann für Kleinunternehmen verheerende finanzielle Folgen haben und den Betrieb empfindlich stören, was in einigen Fällen sogar zur Schließung führen kann. Künftig sollten sowohl große Unternehmen als auch KMUs darüber nachdenken, eine Cyberversicherung als Teil ihrer Gesamtstrategie abzuschließen, um sich vor finanziellen Schäden durch Cyberangriffe zu schützen.

WHITEPAPER

Eine Cyberversicherung kann helfen, die Auswirkungen einer Sicherheitsverletzung oder eines Ransomware-Angriffs abzumildern. Um eine Cyberversicherung in Anspruch nehmen zu können, müssen Unternehmen jedoch bestimmte Cybersicherheitsstandards und -vorschriften einhalten (z. B. die Nutzung bestimmter Cybersecurity-Tools). So fordern viele Versicherer den Einsatz eines EDR-Tools (Endpoint Detection and Response). Trends wie Telearbeit und Bring-your-own-Device(BYOD)-Modelle haben die Anfälligkeit von Endgeräten erhöht. Daher setzen Cyberversicherungen oft die Nutzung angemessener Endpoint-Security-Produkte explizit voraus. Wichtig zu wissen: Ansprüche können trotz abgeschlossener Versicherung abgelehnt werden, wenn die Sicherheitsmaßnahmen einer Organisation als unzureichend bewertet werden. Um ihre Risiken zu minimieren, brauchen kleine wie große Organisationen heute unbedingt eine Cyberversicherung. Was viele nicht wissen: EDR-Lösungen sind mindestens genauso wichtig, da sie die Einhaltung aller Vorgaben von Cyberversicherungspolicen gewährleisten.



Die Cyberversicherungslandschaft verstehen

Je weiter sich der Markt für Cyberversicherungen entwickelt, desto wichtiger ist es, die steigende Nachfrage zu befriedigen und die zunehmend komplexere Bedrohungslandschaft sowie die damit verbundenen Risiken in den Griff zu bekommen. Hier finden Sie ein paar wichtige Trends, die sich auf die Risikoprofile von Unternehmen auswirken:

Technologische Fortschritte bei der generativen künstlichen Intelligenz (KI)

Generative KI-Tools werden immer besser und leichter zugänglich. Daher wird es auch für Bedrohungsakteure einfacher, raffinierte Angriffe zu entwickeln. Um Datenverluste und andere Risiken zu vermeiden, müssen Unternehmen eine sichere KI-Nutzung gewährleisten.

Migration zu Cloud-Technologien/Software-as-a-Service(SaaS)-Anwendungen

Immer mehr Organisationen setzen auf Cloud-Technologien und wechseln von lokalen Netzwerken zu SaaS-Anwendungen. Diese Umstellung kann Netzwerkadministratoren vor neue Herausforderungen stellen und die Angriffsfläche des Unternehmens vergrößern.

Zunehmende Abhängigkeit vom Internet der Dinge (IoT)

Industrie- und Unternehmenstechnologien sind zunehmend vernetzt. Viele dieser Technologien sind wichtige Bestandteile der Lieferkette und schaffen neue Möglichkeiten für Angreifer, in Netzwerke einzudringen, wenn diese nicht angemessen geschützt sind.

Geopolitische Konflikte

Aufgrund geopolitischer Spannungen ist das Risiko gestiegen, dass staatliche Akteure kritische Infrastrukturen in verschiedenen Branchen ins Visier nehmen. Cyberangriffe werden heute in vielen Konflikten als Waffe eingesetzt, und wir können davon ausgehen, dass die Zahl komplexer Angriffe steigen wird.

Das ewige Katz-und-Maus-Spiel zwischen Cybersicherheitsteams und Bedrohungsakteuren entwickelt sich angesichts neuer, alter und akuter Bedrohungen weiter. In unserer digitalisierten und vernetzten Welt spielen Cyberversicherer eine entscheidende Rolle, wenn es darum geht, Unternehmen gegen signifikante Cyberrisiken abzusichern. Diese Versicherungsunternehmen wissen: Obwohl die globale Wirtschaft in hohem Maße von digitalen Ressourcen abhängig ist, reichen die derzeitigen Möglichkeiten, Risiken zu mindern und Bedrohungen abzuwehren, immer noch nicht aus. Cyberversicherungen waren noch nie so wichtig wie heute – insbesondere für KMUs, von denen 75 % ihren Betrieb nach einem Ransomware-Angriff nicht fortführen könnten.[3] In der aktuellen Cyberversicherungslandschaft müssen Organisationen die richtigen Instrumente und Services nutzen, um ihre Cyberrisikovorsorge zu verbessern und die erforderlichen Sicherheitsmaßnahmen umzusetzen.

Welche Rolle spielt EDR?

EDR (Endpoint Detection and Response) ist eine Sicherheitslösung, die erstmals 2013 von einem Gartner-Analysten beschrieben wurde. EDR-Lösungen überwachen und analysieren kontinuierlich die Aktivitäten auf Endgeräten, um Bedrohungen zu erkennen und angemessene Gegenmaßnahmen einzuleiten. In der Zwischenzeit haben sich EDR-Tools weiterentwickelt. Sie umfassen jetzt eine zunehmende Zahl von Funktionen, die nicht nur proaktiv Bedrohungen und ihre Quellen analysieren, sondern auch Angriffe untersuchen können, nachdem sie bereits stattgefunden haben.

In der Vergangenheit waren Antiviren(AV)-Produkte die primäre Methode zum Schutz von Endpunkten. Weil sie allerdings größtenteils auf statischen Bedrohungssignaturen und -mustern basieren, können sie nur bekannte Bedrohungen erkennen, die sich bereits in ihrer Datenbank befinden. Fakt ist aber: Die raffinierten Bedrohungen von heute, insbesondere Zero-Day-Angriffe, erfordern andere Erkennungsmethoden. EDR-Lösungen sind verhaltensbasiert und schlagen bei verdächtigen oder bösartigen Aktivitäten auf Endgeräten Alarm. So können sie sowohl bekannte als auch unbekannte Bedrohungen aktiv in Echtzeit überwachen und identifizieren.

Hier die wichtigsten Funktionen von EDR:

Erkennung und Meldung von Bedrohungen

Erkennung ungewöhnlicher Aktivitäten und verdächtiger Prozesse auf Endgeräten, die auf einen beginnenden Angriff hindeuten können. Das EDR-System alarmiert daraufhin die Sicherheitsteams.

Threat-Hunting

Da alle Sicherheitsereignisse über sämtliche Endgeräte einer Organisation hinweg aufgelistet werden, können Sicherheitsteams potenzielle Angriffe und Eindringversuche proaktiv untersuchen.

Abwehr/Isolierung von Bedrohungen

Sicherheitsteams können mithilfe eines EDR-Tools Hosts auf einem Netzwerk während ihrer Untersuchungen isolieren – ein wichtiger Schritt, um eine seitliche Ausbreitung zu verhindern.

Reaktion auf Vorfälle

Nach einer Sicherheitsverletzung oder einem Angriff können Sicherheitsteams mittels Rollback-Funktionen den Zustand des Endgeräts vor der Infektion wiederherstellen. Außerdem können Administratoren infizierte Endpunkte isolieren, um zu verhindern, dass Bedrohungsakteure Zugang zu anderen Netzwerkbereichen erhalten.

Problembehebung

Ist die anfängliche Infektion unter Kontrolle, müssen die Sicherheitsteams bestimmte Maßnahmen einleiten, um die betroffenen Endgeräte zu resetten. Sie können die Geräte entweder vollständig löschen oder auf den letzten bekannten sicheren Zustand zurücksetzen.

EDR-Lösungen sind aufgrund ihrer vielfältigen Funktionen für die Erkennung von Bedrohungen und die Reaktion auf Vorfälle von entscheidender Bedeutung und daher für das Risikomanagement und die Bedrohungsabwehr – sowohl für Unternehmen als auch für Versicherer – wichtig. Da 90 % der erfolgreichen Cyberangriffe und 70 % der Datenschutzverletzungen vom Endgerät ausgehen, sind EDR-Lösungen entscheidend für eine starke Sicherheitsstrategie.[4]

Warum EDR für den Zugang zu einer Cyberversicherung unerlässlich ist

Eine angemessene Endpoint-Security ist so wichtig, dass ohne eine funktionierende EDR-Lösung oft kein Versicherungsschutz gewährt wird. EDR-Lösungen können nach einem Vorfall relevante Informationen bereitstellen und so Aufschluss darüber geben, ob ein Unternehmen über ein angemessenes Sicherheitskonzept verfügt. Ein proaktives Risikomanagement mit einem Echtzeiteinblick in die Endgeräte hilft Unternehmen, Cybervorfälle schnell zu erkennen und darauf zu reagieren, Endpunkte zu schützen und Sicherheitsverletzungen schnell zu unterbinden. Versicherer konzentrieren sich nicht nur auf die finanzielle Absicherung ihrer Kunden, sondern auch auf das gemeinsame Risikomanagement.

Beim Abschluss einer Cyberversicherungspolice können Versicherer folgende Aspekte berücksichtigen:[5]

- Branche
- Größe/Umsatz
- Implementierte Cybersecurity-Maßnahmen und -Protokolle
- Einhaltung gesetzlicher Vorgaben (z. B. DSGVO, HIPAA)
- Bisherige Cybervorfälle
- Geografischer Umfang der Geschäftstätigkeit
- Abhängigkeit von Dritten

Während Versicherer die oben genannten Aspekte auf mittlere und große Unternehmen anwenden können, ist das für KMUs nicht immer der Fall, da sie als eigene Risikokategorie mit individuellen Kriterien und Anforderungen betrachtet werden können.

Unabhängig von der Unternehmensgröße kann sich der Einsatz einer EDR-Lösung positiv auf diese Kriterien auswirken und möglicherweise die Versicherungsprämien senken. Angesichts der wachsenden Remote-Work- und BYOD-Trends ist die Fähigkeit einer EDR-Lösung, Geräte sowohl im Netzwerk als auch außerhalb zu schützen, von entscheidender Bedeutung. Neben EDR fordern Cyberversicherer zunehmend auch den Einsatz von MDR-Services (Managed Detection and Response). MDR kombiniert Technologie und menschliche Expertise, um Bedrohungen und Warnmeldungen rund um die Uhr zu überwachen und sicherzustellen, dass Netzwerke optimal geschützt sind und Meldungen schnell bearbeitet werden. Dies minimiert letzten Endes die Auswirkungen von Bedrohungen. MDR-Lösungen von Managed-Services-Anbietern umfassen oft auch EDR-Tools, die beide wichtige Bestandteile einer robusten Cyberversicherungsstrategie sind.

Fazit

Wirksame Cybersicherheitsmaßnahmen sind angesichts der zunehmenden Weiterentwicklung, Häufigkeit und Raffinesse von Cyberbedrohungen wichtiger denn je. Die rasant steigende Zahl von Cyberangriffen und strengere Vorschriften machen deutlich, dass Unternehmen ihre Sicherheit dringend verbessern müssen. Die Cyberversicherung ist zu einem wichtigen Bestandteil einer soliden Cybersicherheitsstrategie geworden, da sie großen wie kleinen Unternehmen finanziellen Schutz und eine Möglichkeit zur Risikominimierung bietet.

Für Unternehmen, die eine Cyberversicherung abschließen möchten, spielen EDR-Lösungen eine wesentliche Rolle. Sie ermöglichen eine kontinuierliche Überwachung, die Erkennung von Bedrohungen in Echtzeit und eine wirksame Reaktion auf Vorfälle, sodass Unternehmen schnell und effektiv gegen Cyberbedrohungen vorgehen können. Versicherer wissen, wie wertvoll EDR-Funktionen zur Risikominderung sind, und setzen sie daher häufig als Bedingung für die Gewährung von Versicherungsschutz voraus.

Darüber hinaus können Organisationen durch die Integration von EDR mit MDR-Diensten die Anforderungen der Cyberversicherung besser erfüllen und sich niedrigere Prämien sichern. Dieser kombinierte Ansatz trägt nicht nur zum Schutz der Endgeräte bei, sondern bietet auch einen umfassenden und transparenten Einblick in die Sicherheitslandschaft des Unternehmens. Das Ergebnis ist ein ganzheitlicher Schutz.

Da sich der Cyberversicherungsmarkt weiterentwickelt und die Bedrohungslandschaft immer komplexer wird, müssen Unternehmen hoch entwickelte Sicherheitslösungen wie EDR priorisieren. Auf diese Weise können sie sich nicht nur für die Cyberversicherung qualifizieren, sondern auch ihre Cybersicherheit insgesamt stärken. So sind sie bestens für die Herausforderungen einer zunehmend cloudbasierten und mobilen Welt gewappnet.

Interessieren Sie sich für das EDR-Lösungsangebot von SonicWall?

Capture Client kombiniert einen erstklassigen Enterprise-Class-Schutz für Endgeräte mit weiteren wichtigen, leistungsstarken Funktionen wie Content-Filterung, für die andere Anbieter oft einen Aufpreis verlangen. Capture Client bietet eine kosteneffiziente Endpunktlösung, die Tools konsolidiert und ein wichtiger Bestandteil einer mehrschichtigen Cybersicherheitsstrategie und einer starken Bedrohungsabwehr ist.

Wenn Sie mehr über die zentralisierte Dual-Engine-Endpoint-Security-Lösung und die Content-Filtering-Funktionen von SonicWall Capture Client erfahren möchten, starten Sie eine kostenlose Testversion oder sprechen Sie mit unserem Team.

Sie möchten mehr über das MDR-Angebot von SonicWall wissen?

Der MDR-Service von SonicWall kombiniert leistungsstarke Cybersecurity-Lösungen mit der Expertise eines Security-Operations-Centers (SOC), das rund um die Uhr Warnmeldungen überwacht, Vorfälle untersucht und Bedrohungen bekämpft, die bestehende Abwehrmechanismen umgehen. SonicWall MDR arbeitet eng mit Capture Client zusammen und lässt sich außerdem mit verschiedenen EDR-Tools Ihrer Wahl kombinieren.

Organisationen, die über kein eigenes Sicherheitsteam verfügen, ihre Teams unterstützen möchten oder ihre bestehenden Tools erweitern wollen, können hier weiterführende Infos finden oder mit unserem Team sprechen.

Weitere Informationen erhalten Sie unter www.sonicwall.de.

E-Mail: sales@sonicwall.com

Quellen

[1] https://www.canalys.com/insights/cyber-insurance-partnerships

[2] https://www.sec.gov/news/press-release/2023-139

[3] https://www.strongdm.com/blog/small-business-cyber-security-statistics

[4] https://www.ibm.com/topics/edr

[5] https://www.crowdstrike.com/cybersecurity-101/cyber-insurance/

Über SonicWall

Mit über 30 Jahren Erfahrung stellt der Cybersecurity-Pionier SonicWall seine Partner in den Mittelpunkt. Als führender Sicherheitsanbieter kann SonicWall schnell und kostengünstig maßgeschneiderte Sicherheitslösungen für jedes Unternehmen weltweit in Echtzeit bereitstellen, skalieren und verwalten – egal ob in der Cloud oder in hybriden und herkömmlichen Umgebungen. Basierend auf den Daten seines eigenen Threat-Research-Centers bietet SonicWall nahtlosen Schutz vor den ausgefeiltesten Cyberangriffen und versorgt Partner, Kunden und die Cybersecurity-Community mit aussagekräftigen Bedrohungsdaten.

SonicWall, Inc.
1033 McCarthy Boulevard | Milpitas, Kalifornien 95035, USA
Weitere Informationen erhalten Sie auf unserer Website.
www.sonicwall.com

221.24 - Whitepaper - EDR Cyberinsurance