**Anwenderzentrierte IT-Security**

# Endpunkte im Visier

Im Zuge hybrider Arbeitsszenarien kommen Unternehmen am Thema Endpoint Security nicht vorbei. Bei der Lösungsauswahl sollten IT-Verantwortliche auf mehrstufige Sicherheitsfunktionalität, den Einsatz künstlicher Intelligenz und das Zusammenspiel der Schutzmechanismen im Netzwerk und am Endpunkt achten.

Befeuert durch die Pandemie arbeiten immer mehr Angestellte von zu Hause aus. Dies eröffnet neue Angriffsvektoren, was Cyberkriminelle zu nutzen wissen. Aktuelle Auswertungen wie der WatchGuard Internet Security Report zeigen, dass endpunktgerichtete Angriffsvarianten seit Ausbruch der COVID-19-Pandemie stark zugenommen haben. Unter anderem stieg die Anzahl der versuchten Übergriffe in Form dateiloser Malware im Jahr 2020 gegenüber dem Vorjahr um eindrucksvolle 900 Prozent. Bösartige Cryptominer kamen zu 25 Prozent häufiger zum Einsatz, und auch Phishing steht weiterhin hoch im Kurs.

Insofern sollten Unternehmen ihre Sicherheitsvorkehrungen auf Herz und Nieren prüfen – gerade wenn sie dezentrale Arbeitsmodelle dauerhaft unterstützen. Fachwissen und entsprechende technische Ressourcen zur Abwehr moderner endpunkt- und benutzerorientierter Bedrohungen zählen mehr denn je. Tradierte EPP-Lösungen (Endpoint Protection Platform) allein sind vielfach gar nicht mehr in der Lage, die derzeitigen Bedrohungen abzuwehren, die im Hinblick auf Masse wie auch Klasse ganz neue Maßstäbe setzen.

Es braucht einen Perspektivwechsel: Unternehmen sind gut beraten, einen Zero-Trust-Ansatz zu verfolgen. Dieser impliziert, dass alle Endpunkte standardmäßig gefährdet und nicht vertrauenswürdig sind. Die Kernelemente solcher Sicherheitskonzepte sind die folgenden:

**Signatur- und heuristikbasierte Erkennung:** Das Zusammenwirken dieser Erkennungsmethoden bildet die Basis jeder effektiven Endpoint-Security-Strategie. Bei der signaturbasierten Erkennung gleicht Sicherheitssoftware Dateien mit Bedrohungsdatenbanken ab. Der heuristikbasierte Ansatz wiederum umfasst die Identifizierung von Code, der auf potenzielle Bedrohungen hinweist, auf Basis spezifischer Algorithmen.

**Kontextbezogene Analyse:** Im Fokus steht hier das Durchleuchten von Verhaltensweisen möglicher Gefahren und Hacking-Techniken über unterschiedliche Zielobjekte hinweg. Dazu zählen beispielsweise Browser, E-Mail-Anwendungen, Dateisysteme oder externe Devices, die mit den Endgeräten des Unternehmens verbunden sind. Auf diese Weise können Unternehmen neben den bekannten Varianten auch unbekannten Arten von Viren, Malware, Spyware und Phishing über verschiedene Angriffsvektoren auf die Spur kommen und diesen etwas entgegensetzen. Über den Abgleich von Signaturen und Heuristiken sowie den Hinweisen zu früheren Angriffsmustern lassen sich kontextbezogene Regeln zur Erkennung von Endpoint-Attacken ableiten.

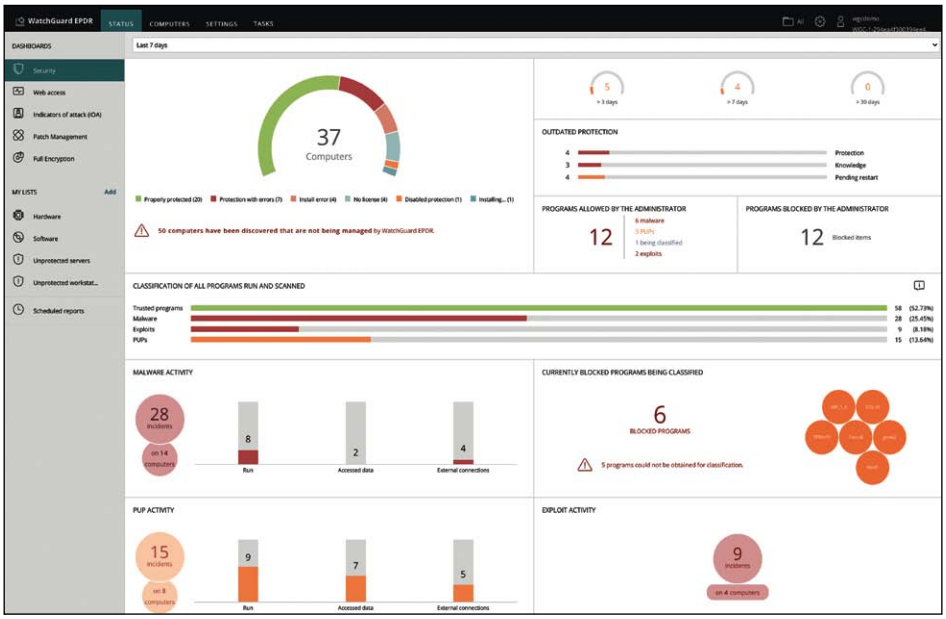
**Anti-Exploit-Technik:** Dies betrifft die permanente Überwachung und Abwehr im Hinblick auf Zero-Day Malware, datei- oder Malware-lose Bedrohungen, Ransomware, Phishing-Angriffe und weitere Gefahren am Endpunkt. Hochentwickelte Anti-Exploit-Technik kann alle auf den Endpunkten des Unternehmens laufenden Prozesse sowie Entwicklungen verfolgen und selbst fortschrittlichen Hacking-Techniken automatisiert den Garaus machen.

**Zero-Trust-Applikationsschutz**: Entsprechende Lösungen kontrollieren und klassifizieren auf Basis künstlicher Intelligenz (KI) und Deep Learning jegliche Aktivität am Endgerät. Sie unterbinden auch bisher unbekannte bösartige Prozesse, blockieren auffällige Anwendungen und stoppen die Fortbewegung von Angreifern im Netzwerk (Lateral Movement). Software prüft dabei jede einzelne Aktion und alle Daten und stuft sie in Echtzeit als legitim oder schadhaft ein.

**Threat Hunting:** Beim Threat Hunting sichern Echtzeitanalysen erfahrener Security-Experten die Erkennung und Abwehr moderner Bedrohungen zusätzlich ab. Dies umfasst beispielsweise den Einsatz von Profilanalyse und Korrelationstools, um anomales Endpunktverhalten zu untersuchen. So lassen sich Angriffe und Endpunktinfektionen in der Regel im Frühstadium erkennen und neue Hacking- und Umgehungstechniken aufdecken. Ein solcher Service stellt außerdem sicher, dass jede Endpunktaktion nachvollziehbar ist – inklusive detaillierter Sicht auf Angreifer und ihre Aktivitäten. Dies ebnet den Weg für forensische Untersuchungen über Anwendungen, Benutzer und Rechner hinweg. Zudem ermöglicht es die schnelle Anpassung der Sicherheitsrichtlinien im Hinblick auf zukünftige Bedrohungen.

## KI als Zünglein an der Waage

Auf jeder dieser Stufen bringt der Einsatz künstlicher Intelligenz spürbaren Mehrwert. Unabhängig davon, ob es darauf ankommt, in der Flut an Informationen nicht den Überblick zu verlieren oder IT-Teams, die in der Regel am Anschlag arbeiten, durch Abwehrautomatismen zu entlasten: Mit modernen, KI-fähigen Endpoint-Security-Techniken ergeben sich klare Vorteile. Entsprechende Lösungen übernehmen verlässlich das Monitoring und stufen ohne manuelles Zutun jede Code-Ausführung als böswillig oder legitim ein – und das selbst in Fällen, in denen ein Angreifer Software korrumpiert, die bereits als vertrauenswürdig bewertet ist. Administrationsteams sollten in dem Zusammenhang




**Kontrolle basiert nicht zuletzt auf Transparenz. Daher sollte ein Unternehmen bei der Auswahl einer Endpoint-Security-Lösung auch auf intuitive Visualisierungsmöglichkeiten achten.**

Bild: WatchGuard Technologies

jedoch darauf achten, dass die Leistung der eingesetzten Endpoint-Security-Produkte nicht mit der Einordnung nach „gut“ oder „schlecht“ entsprechend des Abgleichs mit Listen bekannter Malware endet. Stattdessen sind vor allem die weiterführenden Analysen wichtig. KI- und ML-Algorithmen (maschinelles Lernen) können vor dem Hintergrund noch unbekannter Prozesse nicht zuletzt dafür Sorge tragen, dass sich Telemetrieattribute weiter extrahieren und Auffälligkeiten im Einklang mit den Informationen zusätzlicher Sandbox-Systeme wirklich abschließend und zuverlässig charakterisieren lassen.

Aufgrund der Komplexität der Angriffe sollten Unternehmen zudem auf das Zusammenwirken der Sicherheitsfunktionalität am Endpunkt und im Netzwerk achten. Denn die von Übergriffen ausgehenden Schäden sind bei Weitem nicht mehr nur auf den ursprünglichen Infektionskanal beschränkt. Bedrohungen auf dem Endgerät eines Beschäftigten oder im Kernnetzwerk haben es inzwischen immer öfter auch darauf abgesehen, sich „versteckt“ zu verbreiten und an anderer Stelle Unheil anzurichten.

Die folgenden Beispiele zeigen, wie wichtig die Kombination von Technologien zum Endgeräte- und Netzwerkschutz ist.

**Rootkits:** Damit sind Angriffswerkzeuge oder spezifische Malware-Eigenschaften gemeint, die Funktionen des Endgeräte-Betriebssystems ausnutzen, um unentdeckt zu bleiben. Trojaner oder Botnet-Clients, die den OS- und Endpoint-Security-Kontrollmechanismen entgehen, sind keine Seltenheit mehr. Aber selbst wenn Angreifer solche Dateien, Registry-Einträge und Netzwerkverbindungen am Endpunkt noch verbergen können, sollten sie spätestens dann auffliegen, wenn die initiale Malware eine Verbindung zur Command-and-Control-Infrastruktur herstellt.

**Techniken zur Umgehung von Netzwerk-IPS:** Dass die Verschleierung auch andersherum geht, zeigt die zunehmende Anzahl von „Mogelpackungen“ im Netzwerk. Die Fragmentierung des Datenverkehrs, das ausgeklügelte Umschiffen von Protokollen oder Anwendungen, zeitbezogene Angriffe sowie einfache Verschlüsselungen sind alles Maßnahmen, mit denen Kriminelle Netzwerk-Sicherheitskontrollen auszutricksen versuchen. Als Gegenmittel fungieren Endpunktkontrollen, die das Scanning im Netzwerk flankieren.

**Dateilose Malware und „Living off the Land“-Angriffe:** Im Gegensatz zu den meisten herkömmlichen Malware-Varianten hinterlassen solche Angriffe keine ausführbare Datei oder Registry-Einträge auf dem Zielsystem. Insofern erfordert die Suche nach solcher Malware eine andere Art von EDR-Lösung (Endpoint Detection and Response), die neben Dateien und Registry-Einträgen weitere Indikatoren berücksichtigt – zum Beispiel, welches Verhalten ein legitimer oder unbekannter Prozess an den Tag legt, welche Art von Netzwerkverkehr der Prozess erzeugt oder ob Hinweise auf Speicherinjektion oder DLL-Hijacking erkennbar sind. In diesem Fall ist der Blick in Richtung Netzwerk wie auch Endpunkt extrem hilfreich.

**Zero-Day Malware:** Der bloße Abgleich von Datenbanken zu bekannten Malware-Signaturen reicht hier nicht mehr aus. Stattdessen helfen nur fortschrittliche, verhaltensbasierte Anti-Malware-Dienste, die in der Lage sind, potenzielle Bedrohungen in Netzwerken und auf Endgeräten auf der Grundlage ihrer Prozesse und Eigenschaften zu bewerten. Einmal mehr kommt es darauf an, Indikatoren von vielen Sicherheitskontrollen – sowohl am Endpunkt als auch im Netzwerk – gemeinsam zu betrachten und zu korrelieren, um verdächtige Verhaltensweisen zu erkennen.

## Mehrschichtige Strategie erforderlich

Am Ende lässt sich festhalten, dass die zunehmend raffinierten Bedrohungen eine mehrschichtige, stringente Sicherheitsstrategie erfordern, die Netzwerke, Endpunkte und Benutzer schützt. Keine einzelne Sicherheitskontrolle ist unschlagbar, aber die enge Integration von Netzwerk- und Endgeräte-Sicherheitsdiensten minimiert das Risiko deutlich.

Es zählen Lösungen, die Endpunkt- und Netzwerkindikatoren miteinander in Beziehung setzen, um selbst Bedrohungen zu finden, die ein einzelner Kontrollmechanismus allein möglicherweise nicht erkannt hätte. Gerade die Zusammenführung der kritischen Sicherheitsmechanismen auf einer Cloud-verwalteten Plattform birgt hier einen klaren Mehrwert.

Jonas Spieckermann/wg

Jonas Spieckermann ist Manager Sales Engineering Central Europe bei WatchGuard Technologies.