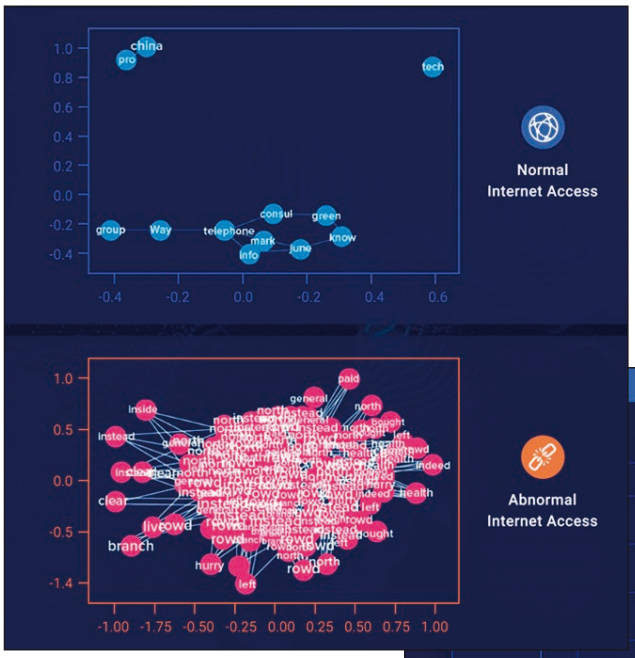
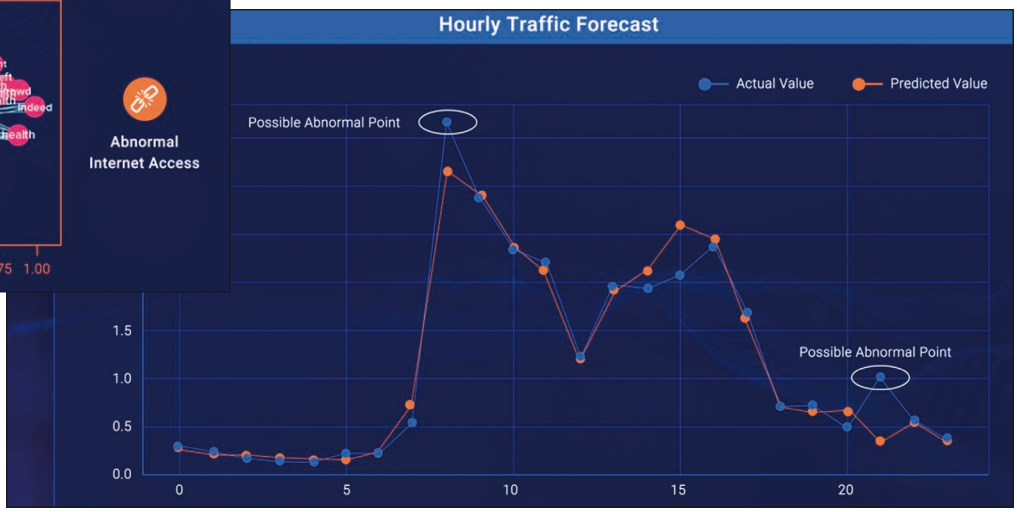
Kommunikation und Interaktion durch Information

Vier Fragen, die EDR und NDR für eine umfassende Cyberabwehr beantworten



Ein Beitrag der Network Detection and Response: KI erkennt den ungewöhnlichen Aufbau von Verbindungen nach außen



NDR erkennt die Exekution einer Datenexfiltration durch erhöhten Datenverkehr.

Cyberangriffe, die Datenverluste oder längere IT-Ausfallzeiten verursachen, beruhen auf der Kenntnis der Hacker über die Gegebenheiten und das Geschehen in der Opfer-IT. Wer diese komplexen Attacken abwehren will, benötigt eine gut informierte und tief gestaffelte IT-Sicherheit. Diese sollte den Datenverkehr, die Endpunkte sowie Informationen aus beiden Bereichen im Blick haben. Eine Network Detection and Response (NDR) und eine Endpoint Dectection and Response (EDR) entfalten einen wirklichen Schutz in ihrer Kombination. Mit Interaktion und Koordination beantworten beide Systeme vier zentrale Fragen für die Cyberabwehr.

Angriffstypen

Viele Angriffe starten meist immer noch mit einer einfachen Phishing-Mail. Nach einer Studie von ForeNova und Cyber Security Insiders aus dem Herbst 2022 starteten Ransomware in 58 % der Fälle durch eine Phishing-Mail, 52 % durch infizierte E-Mail-Attachements. Diese sorgen aber nur für die initiale Infektion eines Systems. Die Urheber gefährlicher Advanced Persistent Threats (APTs) suchen anschließend nach kritischen Systemen sowie nach Informationen als Ansatzpunkte effizienter Attacken. Ihr Ziel ist es bei einer Ransomware-Attacke zum Beispiel, die größtmögliche Drohkulisse aufzubauen, damit Opfer ein Lösegeld bezahlen.

Die Spuren gestaffelter Angriffe verteilen sich im ganzen Netzverkehr und auf verschiedene Endpunkte. Ihre Abwehr beruht vor allem auf Wissen und der kontinuierlicher Überwachung der gesamten IT. Eine Kombination aus NDR und EDR verbessert den notwendigen Wissensaustausch und beantwortet vier entscheidende Fragen:

1. Was befindet sich wo?

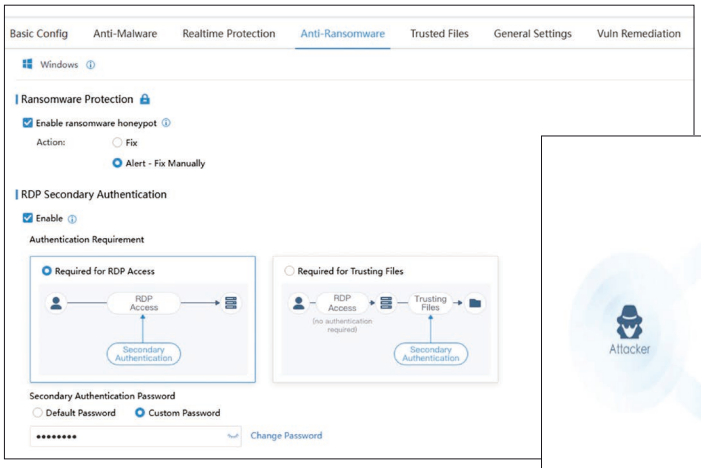
NDR sieht den Aufbau neuer Verbindungen mit bisher unbekannten IP-Adressen wie unbekannten externen Servern. Zudem erkennt sie, wenn Daten in unüblichen Mengen oder zu ungewöhnlichen Zeiten zwischen bekannten Systemen fließen. Ebenso zeigt sie unbekannte Assets im Netz – wie Schatten-IT oder einmal angelegte und eventuell wieder vergessene virtuelle Maschinen.

Eine EDR wiederum sieht alle zentral verwalteten Endpunkte mit einer IP-Adresse, wie einen Windows-PC- oder Mac-Systeme im Büro, remote im Home Office oder unterwegs. Auf einem zentral verwalteten Arbeitsnotebook installiert, erkennt ein EDR-Agent die Quelle gefährlicher Prozesse, wenn ein Mitarbeiter remote arbeitet: Ist das Notebook oder das WLAN im Hotel oder zuhause für ein Risiko verantwortlich? Auch eine angemietete Cloud-Server-Instanz lässt sich überwachen, indem Administratoren einen Agenten auf dieser Unternehmensressource in der angemieteten Cloud installierten.

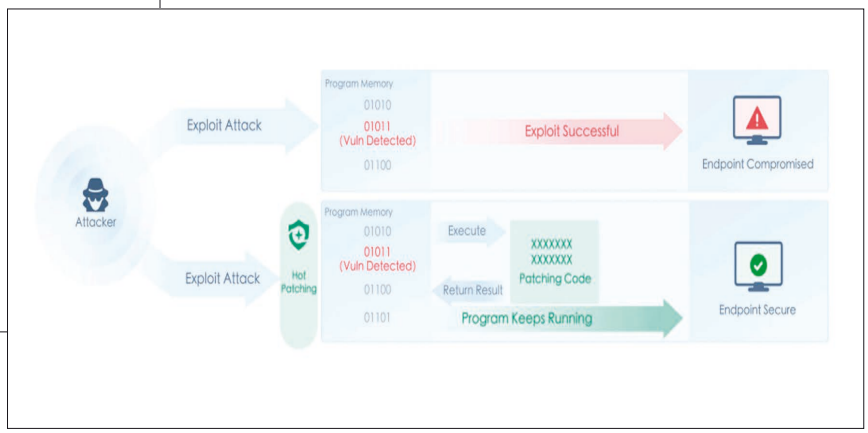
2. Was geschieht wo?

Menschliche Beobachter sind mit der Analyse der Aktivitäten im Netz und auf den Endpunkten überfordert. Künstliche Intelligenz (KI) unterstützt daher beim Monitoring und der Interpretation der IT-Vorgänge. Sie definiert die normalen und damit erlaubten Modelle des Datenverkehrs oder der Endpunktaktivitäten.

Autor:
Paul Smit
Director Professional Services
ForeNova Technologies B.V
www.forenova.com/de



Ein Endpunkt-Schutz kann eine zusätzliche Authentifizierung einführen.



EDR kann durch Hot Patching verdächtige Prozesse blocken und damit noch nicht gepatchte Schwachstellen schließen.

Daraus abgeleitet definiert sie zutreffend, schnell und effizient neue und damit eventuell illegitime Abläufe, die auf einen Angriff hindeuten. KI von EDR und von NDR beobachten komplementär die verschiedenen Bereiche.

Muster erkennen

NDR hilft, die Muster im Datenverkehr und damit die Wege der Hacker im System zu erkennen und als potenziell gefährlich einzustufen. Wichtig ist, auffällige Wege nachzuzeichnen. Denn Hacker tarnen ihre Aktivitäten und Seitwärtsbewegungen mit legitimen Tools, die ein Administrator nutzen würde. Trotzdem ziehen sie dabei durch ihr Verhalten verräterische Spuren. Geht ein Tool etwa einzelne Systeme der Reihe nach durch, deutet dies darauf hin, dass ein Unbekannter, der sich in der IT nicht auskennt, nach Schwachstellen oder Informationen sucht. Ein Administrator, der Probleme lösen will, würde gezielt einzelne Systeme ansteuern, die er untersuchen will.

Endpunktschutz

Ein Endpunktschutz hilft unmittelbar bei der Exekution einer Attacke auf den Endpunkt, unterbindet also die Datenexfiltration oder den Verschlüsselungsprozess. EDR bietet zudem eine bessere Aufsicht der Endpunkte. Die Analyse von Prozessen, Verbindungen sowie von Aktivitäten der Nutzer oder von Prozessen, die vielleicht noch keine unmittelbaren Folgen zeigen, lässt sich oft erst durch die KI am Endpunkt interpretieren. Eine intelligente EDR unterscheidet zum Beispiel legitime vown illegitimen Kompressionen oder Verschlüsselungen von Informationen.

3. Wann greift die Abwehr?

Wer Endpunkt und Netzwerk beobachtet, erkennt verschiedene Zeitpunkte und Notwendigkeiten, vielstufige Angriffe abzuwehren. Eine Threat Intelligence einer EDR wehrt eine bekannte Phishing-Website in einer Mail ebenso ab wie eine Malware, deren Signatur bekannt ist. Die Dunkelziffer, wie viele Ransomware-Attacken so schon im Keim erstickt wurden, ist erfreulich hoch.

Eine NDR erkennt sofort den Aufbau der Kommunikation zwischen einem infizierten System und einem bösartigen Command-and-Control-Server. Sie sieht langfristige Manöver der Hacker, die etwa auf eine weitere Schwachstellenanalyse oder eine Eskalation von Privilegien digitaler Identitäten hindeuten.

Honeypot

Von einer EDR als Honeypot-Lockvögel angelegte Dateien in Verzeichnissen veranlassen verräterische Prozesse wie ein Verschlüsseln oder ein Löschen dieser Köder-Dateien. EDR löst einen sich verratenden Angriff frühzeitig aus und stoppt ihn. Ebenso blockiert sie Systeme. Ein auf Grund der Analyse des Netzverkehrs durch NDR erstellter Notfallplan legt fest, welche Systeme eine EDR im Ernstfall blocken soll, um Infektionswege abzuschneiden.

4. Wer übernimmt welche Maßnahmen?

Eine NDR sieht durch die KI-gestützte Definition von Angriffsmustern Gefahren frühzeitig kommen, doch sie benötigt die konkrete Hilfe vor Ort am Endpunkt. NDR und EDR tauschen nicht nur Informationen aus, sie arbeiten Hand in Hand. Die NDR veranlasst eine effiziente Mikrosegmentierung durch ihre Kenntnis des Datenverkehrs, die der Endpunkt auch ohne Firewall umsetzt. Sie bemerkt eine Datenexfiltration am Datenverkehr, die EDR stoppt diese. Ebenso alarmiert sie eine Firewall, um den Datenverkehr zu stoppen. NDR zeigt Schwachstellen auf, deren Ausnutzen eine EDR dann blockt – auch bevor ein Patch des Softwareanbieters bereitsteht oder eingespielt wird.

Zusammenspiel erzeugt Sicherheit

Nur ein Zusammenspiel der beiden Abwehrkomponenten erzeugt umfassende Sicherheit – einschließlich der Interaktion mit anderen Abwehrtechnologien wie SIEM oder einer Firewall. Zusammengestellte und im Kontext interpretierte Informationen aus mehreren Quellen erfassen das Gesamtgeschehen in der IT-Infrastruktur. Eine gestaffelte Abwehr bedeutet mehr, als nur viele Auffangnetze zu spannen. Sie erweitert den Schutzbereich, verbessert die Analyse von Angriffen und das Schließen einmal ausgenutzter Schwachstellen gegen zukünftige Angriffe. Sie beschleunigt die Reaktionszeit der Cyberabwehr.

Abwehrhorizonte erweitern

Durch das Zusammenspiel von EDR und NDR werden auch die Randbereiche der IT-Unsicherheit – nicht verwaltete IOT- oder OT-Geräte – zumindest etwas kleiner. Indirekt reduzieren sich die Gefahren oder möglichen Angriffsfolgen durch das Überwachen des Netzverkehrs und durch den Schutz der Endpunkte. Ein intakter Endpunktschutz oder eine Firewall senken das Risiko etwa eines nicht verwaltbaren Routers im Homeoffice. Die wirkliche nahtlose Integration dieser Systeme bleibt aber noch eine gemeinsame Aufgabe der IT-, OT- und IoT-Architekten. EDR und NDR können Gefahren für die Systeme der IT senken: Durch das Erkennen ungewöhnlicher Prozesse auf dem Endpunkt und im Datenverkehr.

Wer schreibt

ForeNova Technologies B.V. ist ein Cybersicherheitsspezialist, der mittelständischen Unternehmen preiswerte und umfassende Network Detection and Response (NDR) anbietet, um Schäden durch Cyberbedrohungen effizient zu mindern und Geschäftsrisiken zu minimieren. ◄