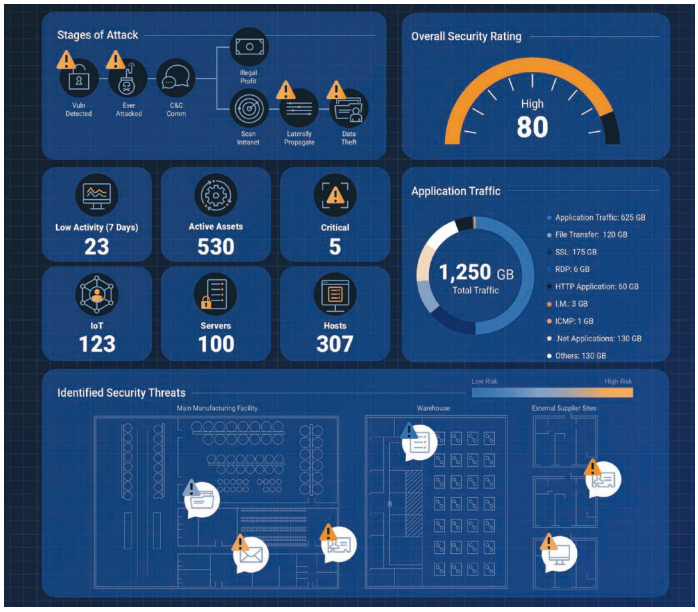
Cybersicherheit im Internet der Dinge



Schematische Darstellung der Sicherheitsbedrohungen für produzierende Unternehmen. Alle Bilder © ForeNova

Hardware, die mit dem Internet of Things (IoT) verbunden ist, sendet Informationen an die zentrale IT oder unerwünscht nach außen. Unter den Datenpaketen können sich Hacker-Befehle, Malware-Codes sowie auch vertrauliche Informationen befinden. Auffälligkeiten im Netzverkehr und am Endpunkt machen solche Vorgänge sichtbar. Für den Schutz von IT-Infrastrukturen mit einer Konnektivität über Internet-of-Things-Hardware ist eine Network Detection and Response (NDR) daher ein wichtiger Bestandteil einer umfassenden Cyberabwehr. Eine damit interagierende Endpoint Detection and Response (EDR), die die Effekte eines Angriffs über das Internet der Dinge auf Endpunkte in der Unternehmens-IT zeigt, ergänzt den Schutz um eine wichtige Komponente.

Zahl der Verbindungen steigt stark an

Die Angriffsfläche von Unternehmen wächst kontinuierlich durch das IoT. Laut Schätzungen der Experten von IoT-Analytics wird konnektive Hardware im Jahr 2025 über 27 Milliarden Verbindungen knüpfen. Aus verschiedenen Gründen ist das Internet der Dinge aber zugleich ein attraktives Ziel für Hacker: Sie übernehmen etwa die Kontrolle über IP-Kameras mit Anschluss ans Unternehmensnetz für Botnetze, um über sie eine Denial-of-Service-Attacke zu starten. Angriffe über Thermostate sind zurzeit noch keine alltägliche Praxis, aber die prinzipielle Vorgehensweise dafür haben Experten bereits beschrieben. Ein weiterer Gefahrenbereich sind, verstärkt durch die Pandemie, die privaten Router oder andere IoT-Geräte im Homeoffice der Mitarbeiter. Sie können ein Zugangstor für Angreifer in die Unternehmens-IT werden. Letztlich stehen bereits bei kleinen Lücken die Türen und Tore für weitreichende Hackeraktivitäten offen.

Fehlende Sichtbarkeit als Sicherheitslücke

Dass Sensoren und IoT-Hardware zu einer Achillesferse der IT-Abwehr werden können, hat verschiedene Gründe: Viele Administratoren haben nicht einmal einen Überblick, ganz zu schweigen von einem vollständigen Wissen, welche konnektiven Geräte Teil ihres Netzwerks sind. Zudem werden mit dieser Hardware oft Sicherheitsmängel mit eingekauft, die der Hersteller aus mangelhafter Entwicklungssorgfalt eingebaut hat: Authentifikationsprozesse, die sich umgehen lassen können, das sprichwörtliche Default-Passwort „1234“ oder unbekannte Nutzerkonten, die ein Entwickler aus Programmierungsgründen anlegt, aber nicht dokumentiert.

Doch auch die Anwender machen Fehler: Unternehmen und Mitarbeiter nutzen die Geräte so lange, wie sie nur irgendwie ihren Dienst tun – und damit über die Lebensdauer hinaus, die die Anbieter etwa für einen Sensor vorgesehen haben. Unterstützen die Hersteller diese Hardware dann nicht mehr, wird sie zu einer Sicherheitslücke. Eine weitere Flanke in der Abwehr öffnet die fehlende Update-Disziplin in Unternehmen, die verschiedene Gründe hat: IT-Administratoren haben oft keine Zeit, die zahlreichen Geräte zu aktualisieren. Außerdem unterstützen gerade manche billige Anbieter ihre IoT-Geräte von vornherein nicht.

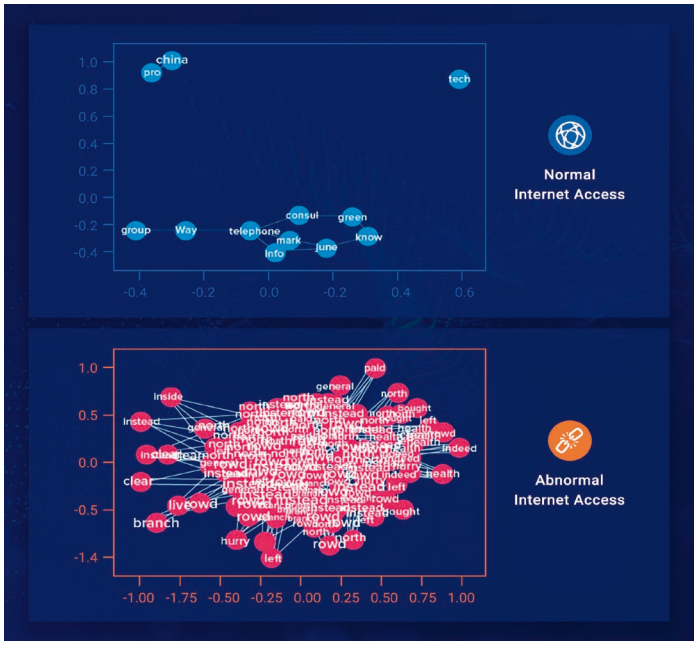
Auf den Spuren der Anomalien

Wer den etwa durch den Austausch von Befehlen zwischen Sensor und Command-and-Control-Server bedingten Datenverkehr früh erkennen und unterbinden will, benötigt dazu den unmittelbaren Zugriff auf IoT-Geräte. Haben Geräte eine IP-Adresse und sind ein Teil des Unternehmensnetzes, kann eine Network Detection and Response (NDR) den Datenverkehr der IP-Videokamera, des Sensors in der Produktion oder des intelligenten Türschlosses auswerten.

Oft haben aber Sensoren keine eigene IP-Adresse oder sind nicht direkt zentral verwaltet. Vom Standpunkt der IT-Sicherheit ist das ein sehr unbefriedigender Zustand. In einer idealen Welt müsste ein Schutz am Endpunkt durch eine EDR implementiert sein. Oft ist auch dies nicht der Fall, weil kein Agent installiert werden kann oder ein solches Vorgehen zu aufwändig ist. NDR und EDR erkennen aber die Effekte einer IoT-Attacke, etwa wenn ein System eine ungewöhnlich große Menge an Daten zu einem unbekannten Ziel versendet.

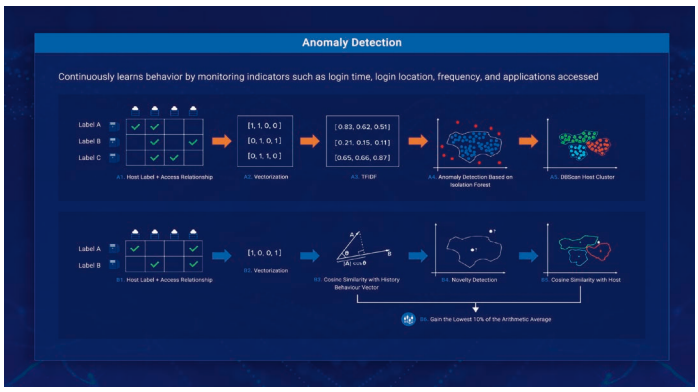
Wie sieht eine Anomalie aus?

Die Spuren einer anomalen Kommunikation verwalteter IoT-Geräte mit einer IP-Adresse werden in diesem Fall sichtbar. Wie sieht aber eine solche Anomalie aus? Sensoren in der Produktion etwa liefern im legitimen Standardbetrieb regelmäßig kleine Pakete an zentrale Systeme und Applikation, erhalten aber so gut wie nie Datenpakete zurück

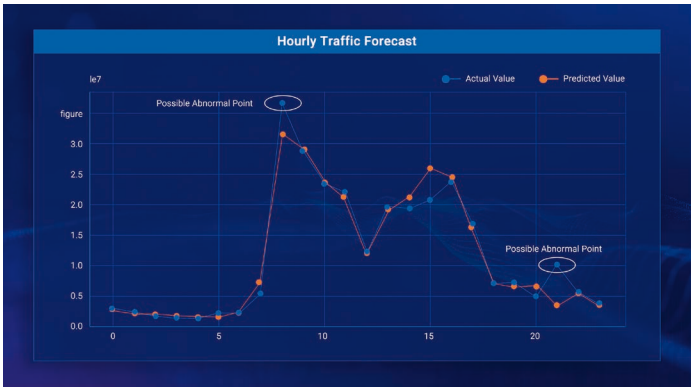


Die Überwachung des Netzwerkverkehrs zeigt anomale Kommunikation mit dem Internet an – der auf Angriffe hindeutet

Autor:
Paul Smit, Director Professional Services
ForeNova
www.forenova.com/de



Künstliche Intelligenz erkennt Anomalien im Netzverkehr – wie Zeit, Ort und Häufigkeit eines Logins oder den atypischen Zugriff auf Dateien



Ein erhöhtes Datenvolumen kann Symptom für eine Exfiltration von Daten sein

– von einem eventuellen Update abgesehen. Nach außen dürften über IoT keine Daten übertragen werden. Dies sollte über andere zusätzlich kontrollierte Schnittstellen erfolgen. Ein von einem solchen durch künstliche Intelligenz erlernten Modells eines legitimen Netzverkehrs abweichender Sendeverkehr ist verdächtig und als außergewöhnliches Muster im Datenverkehr recht einfach anhand der Metadaten zu erkennen. Eine durch künstliche Intelligenz und maschinelles Lernen geschulte Analyse des Netzverkehrs durch NDR in Verbindung mit einer Überwachung des Verhaltens der Endpunkte durch EDR erkennt aus der Internet-Konnektivität entstehende abweichende Vorgänge und schlägt Alarm.

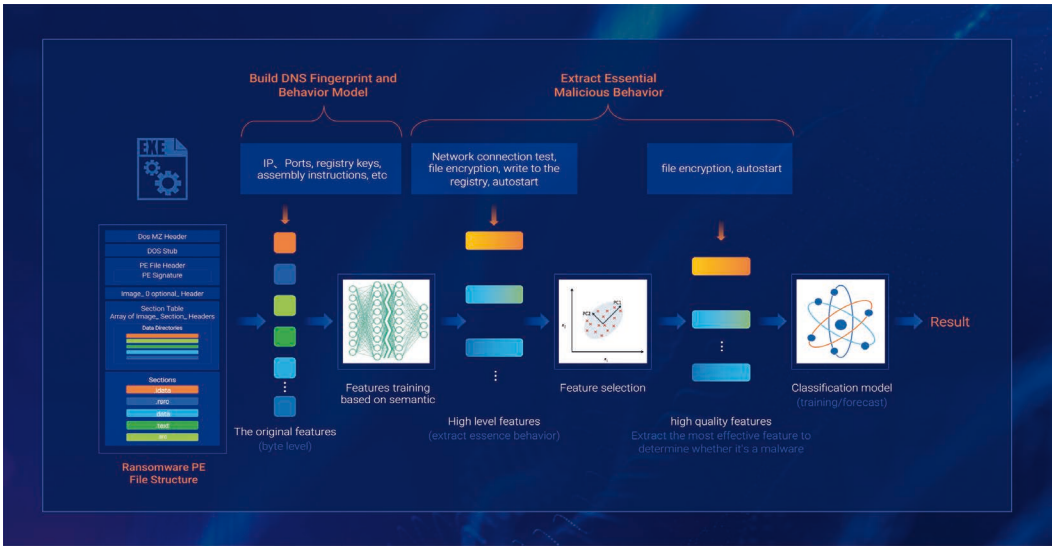
Neue IoT-Sicherheitspolitik

Wie können sich Industrie-Unternehmen gegen die Gefahren aus dem Internet schützen? IT-Administratoren sollten folgende Ratschläge befolgen, um Attacken aus dem Internet of Things abzuwehren:

1. Unternehmensnetzwerke segmentieren: IoT-Geräte sollten zunächst nur in einem Gastnetz ihre Daten weitergeben. Der Datenverkehr zwischen IoT- und zentralem Netz lässt sich effizient überwachen.
2. Zero Trust als Sicherheitsgrundlage: Administratoren sollten jede Kontaktaufnahme aus dem Netz zunächst überprüfen, bevor sie diese zulassen. Eine Kontrolle per Default stoppt zugleich einen Wildwuchs von IoT-Hardware mit Zugriff aufs Netzwerk. Denn nun wird jeder Sensor oder jede Hardware sichtbar, sobald sie Kontakt ihm Netz sucht.
3. Virtuelles Patchen schließt Schwachstellen nicht aktualisierbarer oder verwaltbarer IoT-Geräte auf Application-Firewall-Ebene.
4. Sofortmaßnahmen festlegen: Ein anomaler Datenverkehr muss Abwehrmaßnahmen durch Firewalls, Antivirus, Endpoint Detection and Response oder Identitätsmanagement auslösen. Das Blocken von Systemen und Netzsegmenten oder ein automatisches Snapshot Backup zum Sichern von Daten bei ungewöhnlichen Ereignissen kann einem Schaden vorbeugen.
5. Ganzheitliche IT-Sicherheit: Nicht zentral verwaltete IT-Systeme sind eine potenzielle Sicherheitslücke, da Administratoren auf sie nicht zugreifen können und sie nur den von ihnen ausgehenden Datenverkehr sehen. Ein EDR-Client sorgt im Idealfall für den unmittelbaren Schutz dieser Endpunkte. Ist dies nicht möglich, greift die NDR, die durch auffälligen Datenverkehr Hinweise auf sicherheitsrelevante Vorfälle erhält.
6. Ereignisse analysieren, um die Angriffe von morgen zu verhindern: Haben NDR und EDR mit Hilfe anderer Technologien einen Angriff abgewehrt, spielt die Analyse des Vorfalls eine wichtige Rolle, um die Lücke zu schließen und Folgeangriffe zu verhindern. Die Wege einer Attacke, die eine NDR in einer Timeline der Metadaten von und nach außen sowie innerhalb des Systems in einem Spiegel des gesamten Datenverkehrs aufzeichnet, bleiben sichtbar. Künstliche Intelligenz und maschinelles Lernen erstellen zudem neue Übertragungsmuster des Datenverkehrs, die auf einen IoT-Angriff hindeuten können. Sie helfen damit, ähnliche Angriffe in der Zukunft abzuwehren. Ebenso überwacht auch eine EDR in Echtzeit anomales Verhalten der Endpunkte: Wie etwa das Versenden von Daten nach außen, um Industriespionage zu betreiben oder um eine Ransomware-Erpressung voranzutreiben.

Auch für den Mittelstand in der Industrie sinnvoll

Selbst kleine aber digital affine Produktionsunternehmen öffnen sich immer mehr dem Internet – oft ungeordnet und ohne die neue Netztopographie in die bestehende IT-Sicherheitsstruktur einzubinden. Die Sicherheit dieser neuen Konnektivität muss aber auf einer starken Basis stehen. NDR überprüft dabei den gesamten ein- und ausgehenden sowie den internen Datenverkehr und erkennt atypische Muster in Echtzeit. Gemeinsam sorgen EDR und NDR für einen Schutz der unternehmenseigenen Endpunkte gegen die Gefahren aus dem Internet. ◀



Künstliche Intelligenz erkennt Verhaltensmuster von Malware: Aus grundlegenden Eigenschaften und erweiterten Funktionalitäten komplexer Angriffe entsteht das Verhaltensprofil zum Beispiel einer Ransomware-Attacke