DARKTRACE INDUSTRIAL

BRANCHENFOKUS

Cyberabwehr für Produktionsunternehmen

Die jüngsten Angriffe auf Produktionsunternehmen haben deutlich gemacht, wie stark diese Branche gefährdet ist. Von automatisierten Produktionsanlagen bis hin zu vernetzten Lieferketten – das moderne Produktionswerk profitiert von der starken Vernetzung von OT- und IT-Systemen, die reibungslose Abläufe und Echtzeitanalysen von Daten und Prozessen ermöglicht.

> Durch die Konvergenz von OT und IT ist allerdings auch die Angriffsfläche größer geworden und hat neue Wege für raffinierte und heimtückische Cyberangriffe und Insiderbedrohungen eröffnet.

In diesem Zusammenhang ist der TRITON-Angriff 2017 auf einen Hersteller petrochemischer Erzeugnisse in Saudi-Arabien zu nennen, bei dem die Angreifer in das Sicherheitssystem des Werks eindrangen. Hätte es keinen Fehler im Code der Malware gegeben, hätten die Angreifer schweren Schaden anrichten können, indem sie einen Mechanismus umgangen hätten, der verhindert, dass automatisierte Anlagen über die sicheren Betriebsbedingungen hinaus betrieben werden.

Da solche Angriffe immer raffinierter werden, ist es für Produktionsunternehmen wichtiger denn je, ihre kritischen Geschäftsprozesse vor ressourcenstarken Cyberkriminellen zu schützen, die mit neuartigen Bedrohungen die Abläufe stören und anderen Schaden anrichten.

Bedrohungen in Zahlen

48% der Produktionsunternehmen waren schon einmal Opfer eines Cybersicherheitsvorfalls

Einer von The Manufacturers' Organisation (EEF) in Auftrag gegebenen Studie zufolge haben von den 48 % der Produktionsunternehmen, die schon einmal Opfer eines Cybersicherheitsvorfalls waren, 24 % finanzielle Verluste erlitten oder wurden durch Störungen ihres Geschäftsbetriebs beeinträchtigt. Diese Zahlen machen deutlich, dass die Reife von Unternehmen des produzierenden Gewerbes im Hinblick auf Cybersicherheit sehr unterschiedlich ist und die Unternehmen Maßnahmen ergreifen müssen, damit ihnen nicht ein ähnliches Schicksal widerfährt.

45% der Produktionsunternehmen sind nicht überzeugt, dass sie auf einen Cyberangriff vorbereitet sind

Die Studie von EEF hat auch gezeigt, dass 45 % der Produktionsunternehmen nicht überzeugt sind, dass sie auf einen Cyberangriff vorbereitet sind. Die Herausforderungen in puncto Cybersicherheit sind für das produzierende Gewerbe sehr komplex und vielfältig – daher braucht es hochentwickelte Cyberabwehr-Mechanismen, die in der Lage sind, ihre OT-, IT- und IIoT-Umgebungen wirksam zu schützen.

Manufacturing is the third most attacked sector

Nach öffentlichen Einrichtungen und Finanzwesen ist das produzierende Gewerbe der The Manufacturers' Organisation zufolge die am dritthäufigsten angegriffene Branche. Die Angriffe konzentrieren sich auf die Entwendung von geistigem Eigentum oder internen Informationen über Betriebsverfahren. Dabei nutzen Cyberkriminelle Sicherheitslücken in Betriebssystemen und industriellen Steuerungssystemen.

Darktrace Industrial

Darktrace Industrial ist die weltweit führende Cyber-KI-Technologie für OT- und IT-Umgebungen. Dabei wird in Echtzeit ein „Immunsystem" aufgebaut, um vernetzte Geräte vor dem gesamten Spektrum an Cyberbedrohungen zu schützen – von ultraschneller Ransomware bis hin zu verborgenen Cyberkampagnen, die ungesehen in industriellen Steuerungssystemen lauern.

Darktrace Industrial nutzt künstliche Intelligenz, um die Verhaltensmuster jedes Controllers und jeder Workstation im Steuerungsnetzwerk sowie jedes Benutzers und Geräts im Unternehmensnetzwerk zu lernen und sich nach und nach ein Bild von der normalen Funktionsweise der gesamten Umgebung zu machen. So ist Darktrace Industrial in der Lage, die ersten Anzeichen einer sich entwickelnden Bedrohung zu erkennen – und das ganz ohne Regeln, Signaturen oder Annahmen.

> Die bahnbrechende Self-Learning-Technologie von Darktrace Industrial verändert grundlegend die Art und Weise, wie Industrieumgebungen umfassend geschützt werden, unabhängig von der Art des Geräts.

Das Industrial Immune System schützt einige der komplexesten Produktionsanlagen der Welt, darunter FMCG- Konzerne und führende Pharma-, Chemie- und Automobilunternehmen.

Darktrace Industrial implementiert Software sowohl in ICS- als auch in Geschäftsnetzwerken und führt Analysen zentral zusammen. So können Sicherheitsteams die gesamte Netzwerkaktivität zentral überwachen, von ständigem PLC-Datenverkehr bis hin zu verteilten IIoT-Sensor-Grids.

Darktrace Industrial in Aktion

Kompromittierung eines biometrischen Kontrollsystems

In einem großen Produktionsunternehmen mit mehreren High-Priority-Standorten erkannte Darktrace eine schwerwiegende Bedrohung in Verbindung mit einem Fingerabdruckscanner. Die Angreifer nutzten Sicherheitslücken in der Scanner-Software aus und verschafften sich auf diese Weise Zugriff auf sensible Benutzerdaten im Unternehmensnetzwerk. Mit diesen Informationen war ein unbefugter Zugang zu den Räumlichkeiten des Unternehmen möglich, was eine große Bedrohung für das Unternehmen darstellte.

Darktrace erkannte diese Bedrohung, weil verdächtige abnormale Verbindungen zu neuen Geräten außerhalb des Netzwerks aufgebaut wurden, und informierte sofort das IT-Team, bevor Schaden entstehen konnte.

Datenspeicher gefährdet geistiges Eigentum

Darktrace erkannte im Netzwerk eines großen europäischen Produktionsunternehmens, das sein geistiges Eigentum in der Cloud speichert, dass mit einer einfachen Kombination aus Benutzername und Kennwort – ohne weitere Beschränkungen oder Verschlüsselung – auf kritische Daten zugegriffen werden konnte. Das bedeutete, dass ein Benutzer mit bösen Absichten relativ leicht durch Belauschen der Netzwerkkommunikation sensible Informationen hätte abgreifen können.

Darktrace erkannte diese Sicherheitslücke, weil der Technologie anormale Aktivität im Netzwerk aufgefallen war: Abruf einer ungewöhnlichen zip-Datei aus einem externen Verzeichnis. Darktrace konnte dem Unternehmen das Risiko sofort melden, sodass keine sensiblen Daten zum geistigen Eigentum ausgeschleust werden konnten und das Risiko für Produkt und Umsätze begrenzt werden konnte.

> Maschinelles Lernen erkennt Dinge, die wir selbst nicht vorhersagen und definieren können. Das ist wie die Suche nach der Nadel im Heuhaufen.
>
> **Stuart Berman, Information Security Architect, Steelcase**

Kontakt

Nordamerika: +1 415 229 9100
Europa: +44 (0) 1223 394 100
Asien/Pazifik: +65 6804 5010
Lateinamerika: +55 11 97 242 2011

info@darktraceindustrial.com
darktrace.com/industrial