MDR benutten om de productie te beveiligen

Dreigingsactoren die snel winst willen maken, hebben de productie al lange tijd als doelwit. Door het gebruik van vaak verouderde systemen vormt deze sector een gemakkelijk aan te vallen doelwit. Beveilig jouw operationele technologie (OT) met Managed Detection & Response (MDR) voor maximale bescherming.

De productie: het kloppende hart van de economie

De productie, die verantwoordelijk is voor de productie van transportmiddelen, chemische producten, energie-infrastructuur en meer, houdt de wereldeconomie draaiende. Binnen deze sector zijn er echter kritieke schakels die door veel landen worden aangemerkt als essentieel voor de vitale infrastructuur. Denk hierbij aan de productie van primaire metalen, machines, elektrische apparatuur en componenten, en transportmiddelen. Het beschermen van deze sectoren is een fundamenteel aspect van nationale veiligheid en stabiliteit.

Een automatisch doelwit

Voor fabrikanten is digitale transformatie een tweesnijdend zwaard. Hoewel het zorgt voor verbeterde productiviteit en efficiëntie, opent het ook de deur naar cyberdreigingen. Veel industriële omgevingen maken gebruik van cyberfysieke systemen die afhankelijk zijn van OT en IT-netwerken. Dit kan leiden tot cyberaanvallen die productielijnen stilleggen en de bedrijfscontinuïteit bedreigen.

Een goed voorbeeld van deze kwetsbaarheid is de toename van supply-chain-aanvallen. In 2021 werd een grote Amerikaanse brandstofpijpleiding, die dagelijks 2,5 miljoen vaten vervoerde, stilgelegd na een ransomware-aanval door de cybercriminelen van DarkSide. De aanval, die mogelijk werd gemaakt via een gelekte VPN-wachtwoord, dwong de Amerikaanse overheid om regelgeving rond landtransport te versoepelen, wat resulteerde in een stijging van brandstofprijzen met ongeveer 6%. Uiteindelijk betaalde het getroffen bedrijf een losgeld van ongeveer 5 miljoen dollar om de systemen te herstellen.

Maar ransomware is niet de enige dreiging voor de maakindustrie. In 2017 ontdekten onderzoekers van ESET Industroyer, één van de meest geavanceerde dreigingen voor industriële controlesystemen. Deze malware kon schakelaars en stroomonderbrekers in elektriciteitsstations direct aansturen door industriële communicatieprotocollen te misbruiken. Dit soort aanvallen kan leiden tot grootschalige schade en systeemuitval.

Vertrouwen op verouderde systemen

Door de nauwe onderlinge verbondenheid van leveranciers, aannemers, distributeurs en externe dienstverleners ontstaat een uitgebreide aanvalsoppervlakte. Als één schakel valt, kunnen anderen snel volgen. Dit gold ook voor de verspreiding van de Petya-malware, die toegang kreeg via de boekhoudsoftware M.E.Doc en via een geïnfecteerde update een grootschalige ransomwarecampagne lanceerde.

Vooral kritieke fabrikanten die afhankelijk zijn van verouderde systemen lopen groot risico. In tegenstelling tot andere sectoren, waar systemen eenvoudiger kunnen worden geüpdatet, is de maakindustrie sterk afhankelijk van dure, gespecialiseerde apparatuur. Veel van deze systemen draaien op verouderde software. Wanneer een fabriek wordt getroffen door ransomware zoals

LockerGoga, kan een hele operatie plotseling handmatig moeten worden uitgevoerd, met miljoenenverliezen als gevolg.

Toch worden cybersecurity-investeringen en systeemupdates vaak uitgesteld omdat het bijwerken van industriële systemen gepaard gaat met lange stilstandperiodes, wat leidt tot operationele achterstanden en financiële verliezen. Dit creëert zwakke plekken in de beveiliging die vroeg of laat worden uitgebuit.

Een leiderschapskwestie?

De grote vraag is wie verantwoordelijk is voor beveiligingsfouten veroorzaakt door verouderde of onveilige systemen. Zijn dat de beveiligingsprofessionals die 24/7 hun best doen om een bedrijf te beschermen? Of is het de leiding van het bedrijf, die korte onderhoudsgerelateerde stilstand soms opoffert in ruil voor het risico op losgeldbetalingen en wereldwijde verstoringen?

Met een gemiddelde kostenpost van 5,56 miljoen dollar per datalek in de industriële sector is het essentieel dat bedrijven cybersecurity als een strategische prioriteit behandelen. Leidinggevenden en managers spelen hierin een cruciale rol. Cyberbeveiliging moet niet langer worden gezien als een IT-aangelegenheid, maar als een fundamenteel bedrijfsdoel. Dit betekent dat er budgetten moeten worden vrijgemaakt voor beveiligingstools, training en personeel. Wanneer cybersecurity wordt gecombineerd met procesoptimalisatie, kan dit op lange termijn leiden tot verbeterde productiviteit en concurrentievoordelen.

Vergeet de medewerkers niet

Naast strategische investeringen in cybersecurity moeten leiders ook aandacht besteden aan hun medewerkers. Dit geldt met name voor werknemers met toegang tot kritieke netwerksystemen, die per ongeluk malware kunnen introduceren.

Uit het Verizon Data Breach Investigations Report van 2024 blijkt dat 83% van de cyberincidenten in de maakindustrie het gevolg was van systeeminbraken, social engineering en aanvallen op webapplicaties. Cybercriminelen maken vaak gebruik van social engineering-technieken zoals phishing, of verspreiden malware via kwaadaardige bijlagen en downloads.

Regelmatige cybersecuritytrainingen zijn daarom essentieel en moeten onderwerpen behandelen zoals phishingherkenning, wachtwoordbeheer en veilig omgaan met gegevens. Werknemers moeten worden aangemoedigd om verdachte activiteiten direct te melden zonder angst voor represailles, zodat een open en preventiegerichte beveiligingscultuur ontstaat.

Daarnaast zijn geavanceerde cybersecurity-oplossingen, zoals endpoint security en extended detection & response (XDR), onmisbaar voor fabrikanten. Deze technologieën bieden realtime inzicht in netwerken en helpen dreigingen te detecteren en te neutraliseren voordat ze escaleren. Door gebruik te maken van een beheerde dienst kunnen organisaties profiteren van 24/7 bescherming zonder te hoeven investeren in uitgebreide interne beveiligingscapaciteiten.

ESET beschermt de productie

Managed services zoals ESET MDR bieden continue beveiliging en verlichten risico's die voortkomen uit oplossingen zoals endpoint detection & response (EDR), vooral wanneer een fabrikant te weinig of onvoldoende gekwalificeerd beveiligingspersoneel heeft. Dit gebeurt zonder zware investeringen in interne middelen, terwijl productie-efficiëntie behouden blijft.

ESET's MDR-aanbod omvat ook **ESET Detection & Response Ultimate**, een zeer gespecialiseerde service die fungeert als een verlengstuk van de beveiligingsteams van klanten. De dienst biedt toegang tot door onderzoek ondersteunde professionals die detecties binnen slechts 20 minuten kunnen afhandelen.

Altijd aanwezige compliance-standaarden

Naast externe dreigingen moeten fabrikanten ook rekening houden met regelgeving en compliance-verplichtingen. De Europese **NIS2-richtlijn** en de **Machinerichtlijn 2023/1230** stellen eisen aan kritieke sectoren, waaronder de maakindustrie. Dit omvat verbeterde beveiliging van de supply chain, risicobeheer en rapportageverplichtingen.

Ook internationale standaarden zoals **ISA/IEC 62443** bepalen richtlijnen voor de beveiliging van industriële automatiserings- en controlesystemen. Voor fabrikanten van medische apparatuur vereist de **Consolidated Appropriations Act, 2023 (sectie 524B)** een grondige beoordeling van verbonden apparaten om te garanderen dat ze voldoen aan cybersecuritynormen.

Gezien de toenemende focus van overheden op cyberweerbaarheid, is het waarschijnlijk dat er in de toekomst nog strengere regelgeving voor kritieke industrieën zal volgen.

Praktische oplossingen voor fabrikanten

Om risico's die voortkomen uit verouderde systemen te beperken, moeten fabrikanten robuuste beveiligingsmaatregelen implementeren, zoals **air gapping** en **netwerksegmentatie**.

- **Air gapping** betekent dat kritieke systemen volledig worden geïsoleerd van het netwerk, waardoor ongeautoriseerde toegang wordt voorkomen.
- **Netwerksegmentatie** verdeelt het netwerk in kleinere, geïsoleerde zones, zodat een eventuele inbraak zich niet door het hele systeem kan verspreiden.

Door deze maatregelen te combineren met een beheerde detectie- en responsdienst zoals **ESET MDR**, kunnen fabrikanten geavanceerde dreigingen proactief bestrijden en operationele verstoringen minimaliseren.