

Door 5G komen cyberdreigingen nog sneller binnen

5G combineert razendsnelle draadloze prestaties en lage latency met verbeterde mobiliteit en schaalbaarheid. Daarmee is deze telecommunicatienorm geknipt voor het opschakelen van operationele technologie (OT) voor het automatiseren van productieprocessen. Het ondersteunt bovendien nieuwe toepassingen voor bedrijven in het industriële segment. 5G stelt OT- en IT-omgevingen en de telecomnetwerken waarmee die zijn verbonden echter ook bloot aan nieuwe cyberrisico's, waarschuwt Nick Onken van Fortinet.

De systemen van industriële bedrijven zijn extra gevoelig voor vertragingen. Automatisering mag er niet toe leiden dat sluisdeuren, telescopen, scheepsroeren en dergelijke zelfs maar een duizendste van een seconde te laat reageren op commando's. Industriële systemen die verbonden zijn met de IT-omgeving belasten de verbindingen echter enorm. Ze vragen niet alleen om de convergentie van communicatieverbindingen, maar ook om een grote capaciteit voor gegevensopslag en -analyse. Daarnaast vereist de toegang tot industriële besturingssystemen

en productieomgevingen hoogwaardige beveiliging. Cybercriminelen mogen tenslotte niet de touwtjes van operationele technologie in handen krijgen. Inbraken in IT-systemen bedreigen de bedrijfscontinuïteit, maar cybercriminelen met toegang tot OT zijn levensbedreigend. Het simpelweg toepassen van losstaande beveiligingsoplossingen voor netwerken en OT is niet voldoende. De inzet van 5G voor bedrijfskritieke toepassingen vraagt om integrale beveiliging.

Detecteren en verhelpen

Het 'slim' maken van industriële systemen of het 'industrial internet of things (IIoT)' betekent dat bedrijven sensoren, bewakingsystemen en de besturing van machines en andere apparatuur met het bedrijfsnetwerk verbinden. "Dat gebeurt vaak op afstand, zoals bij schepen op zee of bij een uitgebreid industrieterrein", zegt Nick Onken, major account manager service providers bij Fortinet. "Dat is mogelijk dankzij 5G, want dit biedt snelle verbindingen met een lage vertraging. 5G is snel, maar cyberdreigingen komen met dezelfde snelheid binnen en het is belangrijk om deze direct te kunnen detecteren en verhelpen."

Dat is uitdagend, want IIoT-omgevingen bestaan uit duizenden sensoren, sondes en actuatoren, weet Onken. "Die bieden allemaal



Nick Onken



5G is snel, maar cyberdreigingen komen met dezelfde snelheid binnen

LAN, WAN en cloudnetwerk. Dat is geen overbodige luxe als cyberbedreigingen met de snelheid van 5G te werk gaan.”

Showstopper: een onbeschermd aanvalsoppervlak

Door 5G ondersteunde draadloze IIoT-apparaten hebben vaak geen ingebouwde beveiliging. Cybercriminelen kunnen deze kwetsbare systemen gebruiken als springplank naar de productieomgeving. “Apparatuur en systemen met 5G-functionaliteit nemen een steeds belangrijkere rol in productieomgevingen in”, zegt Onken. “Dat zorgt voor een groeiend aanvalsoppervlak van onbeschermden apparaten.”

Succesfactor: netwerksegmentatie met een modulaire security-infrastructuur

De eerste stap voor de beveiliging van 5G- en IIoT-apparaten is deze onder te brengen in netwerksegmenten die zijn afgescheiden van het productienetwerk, stelt Onken. “Maar deze maatregel is op zichzelf niet voldoende. Het oplossen van de problemen die inherent zijn aan een gedistribueerd, hyperverbonden en razendsnel 5G-netwerk vraagt om de inzet van een beveiligingsarchitectuur die integrale bescherming biedt voor zowel de IT- als OT-omgeving. Dit zorgt voor het nodige overzicht op de complete infrastructuur. Dat helpt weer met de definitie en orchestration van beveiligingsregels. Door de beveiliging van edge computing en 5G te combineren met een consistent en geïntegreerd beveiligingsplatform kun je ervoor zorgen dat alle apparatuur, endpoints, processen en netwerken beschermd blijven, zelfs in uiterst dynamische omgevingen.” ■

toegang op afstand voor beheer, probleemoplossing en onderhoud. Ze vertegenwoordigen een hoog risico, omdat ze direct met de productieomgeving zijn verbonden. Cybercriminelen kunnen ze misbruiken om systemen uit de lucht te halen of om die op ongebruikelijke manieren te laten werken.”

Showstoppers en succesfactoren

De verantwoordelijken voor IIoT-middelen moeten de beveiligingseisen en -maatregelen opnieuw onder de loep nemen. Onken noemt een aantal potentiële showstoppers en succesfactoren waarmee beheerders van OT-systemen rekening moeten houden.

Showstopper: ontoereikende bescherming van de groeiende netwerkrand

Veel bedrijfsprocessen reageren vrijwel direct op veranderende omstandigheden. Het terugkoppelen van data naar een centraal systeem voor analyse en besluitvorming duurt voor sommige processen eenvoudig te lang. “Een edge computing-strategie biedt in dat geval uitkomst”, zegt Onken. “Die brengt applicaties naar de productievloer en maakt lokale, door 5G ondersteunde verzameling en analyse van data mogelijk.”

Onken wijst erop dat edge computing echter ook gevolgen heeft voor de beveiliging. “Hoe meer endpoints er met het netwerk verbonden zijn, hoe uitgebreider en moeilijker beheersbaar het aanvalsoppervlak. Cybercriminelen die het op apparaten aan de netwerkrand hebben gemunt worden vaak pas door een centraal beveiligingssysteem opgemerkt als het te laat is.”

Succesfactor: overzicht en automatisering

Edge computing-apparatuur moet volgens Onken worden beschermd door next-generation firewalls, antivirusplossingen en systemen voor intrusion prevention. “Hoogwaardige beveiliging betekent integratie met alle IIoT- en netwerkvoorzieningen en ondersteuning door artificial intelligence en endpoint detection & response (EDR). Dit is nodig voor realtime overzicht en geautomatiseerde incidentrespons. IT-teams kunnen zodoende effectiever cyberbedreigingen detecteren en analyseren en beveiligingsregels toepassen op het gedistribueerde OT-netwerk en de randen van het