KANTOOR-ICT IS NIET TE VERGELIJKEN MET ICT OP DE WERKVLOER

Technische installaties MKB gevoelig voor cybercrime

Handig: je koppelt je productiemachines aan het kantoornetwerk zodat je de bedrijfsuren kunt registreren. Maar je vergeet dat de beveiligingscamera's ook aan dat netwerken hangen. En laat dat nou net een belangrijke bron van lekken zijn. Voor je het weet liggen de bedrijfsgegevens op straat.

Tekst **Evi Husson**

Bedrijven die bijvoorbeeld water, elektriciteit of energie leveren, hebben hun cybersecurity doorgaans goed op orde. Zij eisen ook steeds vaker van hun toeleveranciers dat de geleverde systemen of instrumentatie cybersecure zijn. Niet alleen de systemen, maar ook de bedrijven zelf moeten goed beveiligd zijn. Bij het MKB is dit nog niet altijd het geval, stelt Marcel Jutte, managing director van Hudson Cybertec, gespecialiseerd in cyber security in technische omgevingen.

Hoge automatiseringsgraad

'De complexiteit en automatiseringsgraad van technische installaties neemt steeds verder toe waardoor organisaties steeds afhankelijker worden van hun technische systemen. Ontwikkelingen zoals Internet of Things en LoRa zorgen voor grotere blootstelling aan cyberdreigingen. Steeds meer grote bedrijven – bijvoorbeeld bedrijven uit de olie- en gassector – zijn zich bewust van cybersecurity en de complexiteit van Internet of Things en zorgen niet alleen dat hun eigen bedrijven goed zijn beveiligd, maar beginnen ook eisen te stellen aan hun toeleveranciers. Ze screenen hun toeleveranciers door middel van een scan of assessment om na te gaan of de instrumenten of systemen die ze in hun assets implementeren voldoende zijn beschermd tegen cybercrime', zegt Marcel Jutte.

Bij zo'n security scan wordt gekeken naar de cyberweerbaarheid volgens de IEC 62443, de wereldwijd geaccepteerde standaard om cybersecurity in te regelen. 'Er wordt nagegaan in welke mate de drie pijlers - mens, organisatie en techniek – op orde zijn. Zijn werknemers zich bewust van de problematiek en potentiele risico's? Welk opleidingsniveau hebben de werknemers? (mens, red.) Zijn alle technische voorzieningen cybersecure? Wat moet er verder nog worden ingericht om het risico zoveel mogelijk te elimineren? (techniek, red.) En zijn er procedures, protocollen en beleidsmaatregelen opgesteld die ook worden nageleefd? (organisatie, red.)? Aan de hand van een vragenlijst en de antwoorden die worden gegeven, is het mogelijk het risico in te schatten en kunnen trainingen op maat worden gegeven.'

De trend dat bedrijven ook een bepaald niveau van cybersecurity verwachten van hun toeleveranciers is te zien in de tenders die op de markt worden geplaatst. Cybersecurity wordt steeds concreter benoemd. 'Inkoopafdelingen specificeren steeds beter waaraan moet worden voldaan op het gebied van OT (operationele technologie, red.) en IT. Daar zal ook het MKB geleidelijk aan mee worden geconfronteerd. Niet meteen morgen, maar de vraag gaat wel komen.'

IT en OT

Bij het MKB moet vooral het bewustzijn rond cybersecurity nog toenemen, stelt Jutte. 'Kleine ondernemingen zijn voornamelijk, logischerwijze, bezig met hun core business. Willen ze er toch mee aan de slag, dan vragen ze vaak hun IT-specialist om ondersteuning. Dat IT en OT niet hetzelfde is en niet op dezelfde manier mag worden behandeld, wordt wel eens vergeten.'

Operationele Technologie (OT) is primair ontworpen om zo betrouwbaar mogelijk te opereren met een zo hoog mogelijke beschikbaarheid. Als het besturingssysteem uitvalt of er zijn andere calamiteiten, dan zou het proces moeten kunnen blijven draaien, *no matter what*. Bij IT is daarentegen snelheid, connectiviteit, rekenkracht en communicatie veel belangrijker. 'Bedrijven die menen dat de beveiliging van de IT dezelfde aanpak heeft als de beveiliging van de industriële automatisering en control systems hebben het mis. Het gaat om twee totaal andere werelden die op een hele andere manier zijn opgebouwd.'

Jutte geeft een concreet voorbeeld. 'In de IT-wereld worden regelmatig updates van software gedaan om de security te verbeteren. Als servers daardoor korte tijd uit bedrijf zijn, zorgt dit doorgaans niet voor grote problemen. In de industriële automatisering of bij gebouwgebonden besturingen is dit veel lastiger. Er is doorgaans geen mogelijkheid om een systeem een half uur buiten bedrijf te stellen om softwareupdates te doen. Daarnaast brengen updates mogelijk ook onverwachte risico's met zich mee die besturingssystemen volledig in de war kunnen sturen, met alle gevolgen van

dien. IT en OT zijn twee aparte werelden en zijn wat cybersecurity betreft ook op een andere manier te benaderen.'

Overzicht

Ook het overzicht moet worden bewaard. Het moet duidelijk zijn op welke wijze systemen in het netwerk aan elkaar zijn gekoppeld. Door dit in kaart te brengen wordt het mogelijk je netwerk te segmenteren. Er kan worden bepaald welke segmenten met elkaar mogen communiceren en hoe/of er mag worden gecommuniceerd met bijvoorbeeld de kantoorautomatisering dat op een heel andere manier is ingericht. Dit is slechts één voorbeeld van een maatregel die een bedrijf kan nemen om cybersecure te worden. 'Belangrijk bij het MKB is vooral dat de bewustwording groeit. Met een MKB Cybersecurity scan kan bijvoorbeeld worden nagegaan wat de cyberweerbaarheid is van de organisatie. Soms is dit confronterend. Maar wellicht minder confronterend dan een lek.'

In de praktijk

Jutte geeft een concreet voorbeeld wanneer kennis of bewustzijn rond cybersecurity ontbreekt. 'Een klein niet nader te noemen familiebedrijf had twee productiemachines aangekocht. Het was mogelijk de machines te koppelen aan het algemene netwerk. Iemand met IT-kennis koppelt alles aan elkaar waardoor ook via de computer van de kantooradministratie die is gekoppeld aan het internet, al de productiegegevens kon worden ingekeken, net als het aantal bedrijfsuren en wanneer onderhoud moet worden gepleegd. Het leek hen erg handig om dit op deze manier te doen, maar over de mogelijke gevolgen ervan werd niet nagedacht. Aan hetzelfde netwerk bleken ook een aantal beveiligingscamera's van inferieure kwaliteit te zijn gekoppeld. Er hoeft maar één klein lek te zijn en alle bedrijfsgegevens liggen op straat.'

'Steeds meer grote bedrijven screenen hun toeleveranciers om na te gaan of ze voldoende zijn beschermd tegen cybercrime.'

Andere voorbeelden zijn het aan elkaar koppelen van systemen om op één centrale printer te kunnen printen, een memory stick, extra device of laptop even op het systeem inpluggen,... Dergelijke voorbeelden komen meer voor dan je denkt. Belangrijk is om eerst bewustzijn te creëren. Alles is vast goed bedoeld, maar werknemers moeten bewust zijn van de risico's. Is er geen bewustzijn, dan kan het wel eens heel fout lopen.'

Tijdens WoTS gehouden van 2 t/m 5 oktober in de Jaarbeurs in Utrecht zal ook veel aandacht worden besteed aan cybersecurity. Meer info: www.wots.nl