VOORTSCHRIJDENDE KETENINTEGRATIE EN AUTOMATISERING STELT HOGERE EISEN AAN IT-BEVEILIGING

DUBBEL OPLETTEN

De recente cyberaanval WannaCry maakte ruim 200.000 slachtoffers in 150 landen. Voor een optimale beveiliging is het essentieel dat bedrijven inzicht hebben in de activiteiten op hun netwerk en snel potentiële gevaren weten te ontdekken. Het Eindhovense KMWE nam al de nodige voorzorgsmaatregelen.

DOOR WILMA SCHREIBER

Internet of things mag dan populair zijn, bij KMWE – toeleverancier voor de hightech machinebouw en aerospace – is het minder aan de orde, stelt Arthur van Hout, manager TQM & ICT. 'Er is geen intensieve communicatie tussen de machines van verschillende afdelingen. Wel zijn afdelingen afhankelijk van eenzelfde netwerk waar data worden opgehaald en weggeschreven. Bij *ransomware* zouden we snel in de problemen komen als bestanden beschadigd of onbetrouwbaar blijken. Als we dan programma's in machines laden, kan dit een machinebotsing tot gevolg hebben. Dan kun je het product weggooien en waarschijnlijk heeft de machine ook schade.' Het machinepark is gedeeltelijk geautomatiseerd met robots, maar dan is er alleen communicatie tussen robot en machine.

MACHINESTILSTAND

De risico's van een aanval met ransomware zijn groot. 'Allereerst natuurlijk financieel, maar het kan ook leiden tot machinestilstand omdat een programma onbetrouwbaar is geworden. Als in korte tijd veel of zelfs alle bestanden beschadigd zijn, kan het lang duren voor je de back-ups hebt teruggezet en weer *up and running* bent', aldus Van Hout. 'Daar komt bij dat we richting klanten onze processen kwalificeren. Als de processen wijzigen, is herkwalificatie noodzakelijk. Een tijdrovende aangelegenheid en dus iets waar je je tegen wilt beschermen.'

Zelf heeft KMWE op kleine schaal te maken gehad met ransomware. Van Hout: 'Iemand had op de zaak zijn webmail geopend en zo ransomware binnengehaald waardoor bestanden werden versleuteld. Gelukkig hebben we dit in de kiem weten te smoren.' Om de risico's te beperken, werkt KMWE samen met it-dienstverlener IP4Sure en zijn naast de gebruikelijke spamfilters en firewalls de nodige maatregelen genomen. 'We hebben ons netwerk afgebakend, de machines draaien op een ander deel dan de meeste gebruikers. Verder hebben we de internettoegang beperkt, goksites en social media zijn bijvoorbeeld afgesloten, net als het gebruik van webmail. Ook bepalen wij de vrijgave van applicaties; als een gebruiker of een server een niet toegestane applicatie probeert te openen, wordt het programma gestopt. Tot slot zijn we behoudend met het verstrekken van ict-bevoegdheden aan gebruikers.' KMWE werkt tevens actief aan bewustwording van medewerkers. 'Regelmatig worden intern berichten verstuurd om personeel alert te houden. Zo is ook na de WannaCry-uitbraak een mailtje de organisatie ingegaan dat ze dubbel moeten opletten wat ze doen.'

CONTINUÏTEIT IN GEVAAR

Klanten zijn zich steeds meer bewust van de it-risico's van samenwerking in de keten, merkt Van Hout. 'Voor ons als *first tier supplier* is er vaak sprake van intensieve samenwerking en ook dat je bij elkaar op het netwerk moet kunnen. Oem'-ers vragen nadrukkelijker hoe we de beveiliging en het management erop hebben geregeld. Gezien de verdere automatisering en integratie van systemen is dit ook noodzakelijk. Want bij gekoppelde netwerken is de impact en reikwijdte van een ransom-aanval groter en kan deze direct de continuïteit in gevaar brengen.' ●

www.kmwe.com
www.ip4sure.nl

WANNACRY-UITBRAAK: DE MENS ZWAKSTE SCHAKEL

Marcel van Oirschot, commercieel directeur van Fox-IT, stelt dat het bij it-beveiliging zeker niet alleen gaat om kantoorautomatisering, maar ook om gekoppelde zaken als bewerkingsmachines, productielijnen, robots, et cetera. 'Deze gebruiken soms andere netwerken en connecties, maar heel vaak eindigt het toch op een standaard Windows-pc of server. Stilstand van machines is uitermate kostbaar en heeft een serieuze impact op de continuïteit van een bedrijf.' Hij noemt het verstandig om netwerken te scheiden en rechten van gebruikers te beperken zonder dat het impact heeft op hun functioneren. 'Realiseer je wel dat firewalls, virusscanner en dergelijke noodzakelijk zijn maar verre van afdoende. Het informeren van medewerkers is essentieel en kun je ook zelf organiseren.' Van Oirschot wijst erop dat bij de WannaCry-uitbraak de zwakste schakel in de keten, de mens, niet hoefde te klikken. 'Wil je je optimaal beveiligen, dan is het cruciaal dat je inzicht hebt in wat er op je netwerk gebeurt en dat je potentiële gevaren heel snel ontdekt. Dat kan veel ellende voorkomen. Het merendeel van de productiebedrijven heeft dit echter niet of slecht geregeld.'

www.fox-it.com

LEREN OVER LOSGELDSOFTWARE

Ransomware is ongrijpbaar – en potentieel desastreus voor bedrijven. Bent u geïnteresseerd in een bijeenkomst over dit actuele onderwerp, georganiseerd door Link Magazine en specialisten zoals Fox-IT, laat het weten aan de uitgever.

john.vanginkel@linkmagazine.nl