Wanneer hackers de koelcellen overnemen: waar zit de blinde vlek in uw cyberbeveiliging?

De hack van koelinstallaties in supermarkten toont aan hoe kwetsbaar onze economie is in een geconnecteerde digitale maatschappij. Door de kracht van AI hebben bedrijven steeds minder tijd om zich daartegen te wapenen. ‘We zitten in een perfecte storm.’

Een ontwrichtende cyberaanval op kritieke infrastructuur leek lange tijd een theoretisch risico of een probleem dat beperkt bleef tot landen in conflictgebieden als Oekraïne of Iran. Maar de cyberaanval op de koelsystemen van verschillende Belgische supermarkten brengt het nu toch griezelig dichtbij. Niet alleen in ons land, overigens. Ook al onze buurlanden hadden ermee te maken, net als bedrijven in Zweden, Finland, Estland en Ierland.

De aanvallen bleven niet beperkt tot supermarkten. Nog deze week werden in Frankrijk verschillende koelcellen met donorbloed van een afstand ontregeld, gelukkig zonder schade. Vorige week zei het Pentagon dat het een onderzoek heeft ingesteld naar mogelijke sabotage van vrieskasten op verschillende basissen van het Amerikaanse leger.

En het zijn lang niet alleen koelinstallaties die gevaar lopen. Eind 2024 veranderden aanvallers de waterdruk bij een Deense waterinstallatie, waardoor leidingen sprongen en zo’n 500 huishoudens tijdelijk zonder water zaten. In Noorwegen opende een aanvaller vorig jaar van een afstand een klep van een kleine dam. In Polen kregen hackers toegang tot vijf waterzuiveringsstations, en enkele maanden later ook tot wind- en zonneparken en energiecentrales. Het zijn pure sabotageacties zonder duidelijk financieel motief, waarbij Rusland door experts vaak wordt aangewezen als vermoedelijke dader - al is dat moeilijk zwart op wit te bewijzen.

Complexe IT, snelle AI

Specialisten waarschuwen wel al jaren dat geconnecteerde industriële systemen kwetsbaar zijn voor hackers. Hoe kan het dan dat zelfs grote ketens als Ahold Delhaize of Carrefour onvoldoende op zo’n scenario waren voorbereid? ‘Dat is een terechte vraag’, zegt Erik Van Buggenhout, partner managed security services bij de Brusselse cyberbeveiliger Nviso. ‘In de zomer heeft een securityresearcher in een artikel nog gewaarschuwd voor kwetsbaarheden in die specifieke koelsystemen, en in oktober waren in Frankrijk al verschillende ketens het slachtoffer. Dus men kende de risico’s.’

Dat bedrijven zich toch nog laten verrassen, wijt hij aan twee factoren: ‘Enerzijds is hun IT-omgeving zo complex dat ze geen zicht meer hebben op hun kwetsbaarheden. Anderzijds zijn er

bij zo'n aanval ook vaak derde partijen gemoeid, zoals de installateur of de onderhoudsfirma. Daardoor is het niet altijd duidelijk wie verantwoordelijk is voor het updaten van die systemen.'

"Als je een fysieke controller moet vervangen, heb je die niet zomaar op het schap liggen." - Mathias Caluwaerts (Strategisch adviseur bij Orange Cyberdefense)

Tijd is een andere factor waaraan het vaak ontbreekt, zeker nu aanvallen als gevolg van AI sneller en frequenter plaatsvinden. 'Als je een fysieke controller moet vervangen, heb je die niet zomaar op het schap liggen', zegt Mathias Caluwaerts, strategisch adviseur bij het beveiligingsbedrijf Orange Cyberdefense. 'En een software-update uitvoeren klinkt misschien eenvoudig, maar wat als je daarvoor je hele koelinstallatie tijdelijk moet uitzetten?'

'In afwachting van een update of vervanging kunnen bedrijven wel al maatregelen nemen, zoals de directe toegang tot systemen via het internet afsluiten', zegt Caluwaerts. Op die manier vermijden ze dan wel gehackt te worden, maar de hinder is er niet noodzakelijk minder door. Kijk maar naar de miljoenen websites die enkele weken geleden op zwart gingen, omdat een veiligheidslek was ontdekt in de veelgebruikte software PHP.

De Belgische cyberwaakhond CCB registreerde vorig jaar 58 procent meer cyberincidenten dan in 2024, en dit jaar is alweer een nieuw record in de maak. De beveiligingsbedrijven komen handen te kort. 'We hebben een incident response team dat snel bijstand kan bieden aan bedrijven. Sinds de zomer zijn zij constant in de weer, zelfs met tien dossiers tegelijk. Dat hebben we niet eerder gezien', zegt Van Buggenhout.

'Het aantal security patches (beveiligingsupdates, red.) dat Microsoft verstuurt, ligt zowat tien keer hoger dan een jaar geleden. Wat nu gebeurt, is precies wat voorspeld werd toen Mythos werd gelanceerd', zegt Caluwaerts. Hij verwijst naar Claude Mythos, een AI-model dat in april werd uitgebracht door het AI-bedrijf Anthropic. Het veroorzaakte wereldwijd commotie, omdat Anthropic zelf waarschuwde dat het model zeer sterk was in het opsporen van kwetsbaarheden in software.

Meer verzekeringspolissen

Ook de verzekeringsmakelaar Vanbreda Risk & Benefits merkt een duidelijke toename van de vraag naar cyberverzekeringen. 'We hadden sinds begin dit jaar al een toename van het aantal afgesloten polissen met 10 procent. De jongste dagen zijn de vragen van bedrijven - zowel bestaande klanten als nieuwe klanten - nog sterk toegenomen', zegt Tom Van Britsom, expert cyberverzekeringen en -veiligheid. 'Ik verwacht dat de premies op termijn zullen stijgen, al zal dat ook afhangen van het aantal aanvallen dat we bij ons nog gaan krijgen, en de schade die ze veroorzaken.'

Dat er nog meer onheil op komst is, daar twijfelt niemand aan. De kracht van AI, in handen van politiek gestuurde groepen die vooral schade willen veroorzaken, brengt ons 'in een perfecte storm', zegt Van Buggenhout.

Veel bedrijven beseffen plots dat niet alleen hun IT-netwerk, maar ook hun fysieke systemen - experts spreken van OT (operational technology) - gevaar lopen. Dat komt deels omdat hackers op zoek gaan naar de zwakste plek in een systeem. ‘Bedrijven hebben de jongste jaren al enorme inspanningen gedaan om de beveiliging van hun IT-park te verbeteren. OT is nog een inhaalbeweging aan het maken, maar in de overgangsperiode gaan we nog meer aanvallen zien gebeuren’, zegt Caluwaerts.

Eeuwigheid

Een groot verschil met klassieke IT-beveiliging is dat OT-systemen allemaal anders zijn, zegt hij. ‘De controller van een windturbine is niet dezelfde als die van een koeltoeren of een koelcel. Vroeger moest je een specialist zijn om een aanval te bedenken voor één specifiek systeem. Nu hebben hackers een AI-model dat hen daar continu bij kan helpen. En de aanvallen komen in een tempo dat we nooit eerder gezien hebben. Daar komt nog bij dat veel OT-systemen gemaakt zijn om 10 of 20 jaar mee te gaan. In cybersecuritytermen is dat een eeuwigheid.’

Een goede beveiliging begint met een goede diagnose, zeggen de experts. ‘Bedrijven weten vaak niet eens welke systemen allemaal aan hun netwerk hangen. Begin met dat in kaart te brengen. Het volstaat ook niet om één keer per jaar een foto te nemen van je systemen. IT-beveiliging is geen foto, maar een film: je moet het continu bewaken’, zegt Van Buggenhout.

‘Als een bedrijf bij ons een verzekering wil afsluiten, moet het aan verschillende voorwaarden voldoen’, zegt Van Britsom. ‘Dat gaat niet alleen over technische zaken zoals multifactorauthenticatie of het maken van back-ups. Ze moeten bijvoorbeeld ook een goed overzicht hebben van wat online geconnecteerd is, procedures opstellen voor als het fout gaat, en medewerkers trainen in het herkennen van phishing (aanvalsmethode die gebruikmaakt van fake mails en websites, red.).’

"Menselijke fouten kunnen altijd gebeuren. Bij ons is 90 procent van de schadegevallen daaraan te wijten. " - Tom Van Britsom (Cyber insurance & security expert Vanbreda Risk & Benefits)

De makelaar waarschuwde in maart vorig jaar al in een artikel over het groeiende risico van aanvallen op de voedingsindustrie en noemde onder meer ‘het manipuleren van de temperatuur van koelcellen’ als mogelijk scenario. ‘Doordat we met veel bedrijven gaan praten, begrijpen we beter wat hun risico’s zijn, dat is onze rol’, zegt Van Britsom. ‘Maar menselijke fouten kunnen ook altijd gebeuren. We zien dat 90 procent van de schadegevallen daaraan te wijten is. Precies daarvoor dient een cyberverzekering.’

Leveranciers

Een veelgemaakte denkfout is dat cyberbeveiliging ophoudt aan de muren van het eigen bedrijf. ‘Kijk je naar de cyberincidenten van de jongste jaren, dan komt meer dan 90 procent van buitenaf, via de toeleveringsketen’, zegt Kurt Gielen, de IT-directeur van Ziekenhuis Oost-

Limburg (ZOL). ‘Dat gaat over leveranciers die hun systemen niet opzetten of beschermen zoals het hoort. Ook bij die koelinstallaties hebben we dat gezien: dat zijn vaak systemen die door technische diensten met 4G-antennetjes op het dak geconnecteerd worden en volledig naast de IT-infrastructuur worden geplaatst.’

Wie zijn OT in kaart brengt, moet daarom ook naar die leveranciers kijken, klinkt het. Van Buggenhout: ‘Wie heeft het systeem opgezet? Wie is verantwoordelijk voor de software-updates en hoe snel gebeurt dat? Maakt dat deel uit van je contract? Dat zijn allemaal zaken die je in kaart moet brengen.’

Nog een stap verder is te kijken hoe je kritische bedrijfsprocessen geconnecteerd zijn met de buitenwereld. ‘In onze economie zijn bedrijven verbonden met leveranciers, klanten, externe dienstverleners en nutsbedrijven', zegt Caluwaerts. 'Weerbaarheid is daardoor veel meer geworden dan een loutere IT-kwestie. Het betekent ook dat je tijdens crisisoefeningen test hoe je je eigen activiteiten kan voortzetten wanneer een van die partijen uitvalt.'

Brandoefening

Een draaiboek met duidelijke procedures, protocollen en back-upsystemen kan veel chaos helpen voorkomen. ‘Zie het als de digitale versie van een brandoefening’, zegt Van Britsom. ‘Bedrijven zijn daar nog veel te weinig mee bezig. Een deel van die oefening is ook om duidelijk de contractuele aansprakelijkheden met leveranciers in kaart te brengen.’

‘Een incident kan altijd gebeuren', besluit Van Buggenhout. 'Daarom is het van belang dat je als organisatie een scenario klaar hebt liggen. Wie is verantwoordelijk voor wat? Hoe communiceren we? Dat zijn dingen die je niet wil improviseren wanneer er iets gebeurt.’

Wim De Preter, Tom Michielsen

Bron: De Tijd
Publicatiedatum: 7/11/2026