De grootste cyberdreiging voor de energiesector? Een basis die niet op orde is

Hackers uit Iran zijn erin geslaagd om een Britse energiecentrale vier dagen stil te leggen. Dat blijkt uit berichtgeving van *The Telegraph*. Over de precieze toedracht is vooralsnog weinig bekend.

Het is niet de eerste keer dat de Europese energiesector doelwit is van een serieus cyberincident. Zo werd vorig jaar in Polen een aanval uitgevoerd op de energie-infrastructuur. Hoewel die aanval niet tot een stroomstoring leidde, onderstreepte het incident opnieuw hoe kwetsbaar de energiesector kan zijn voor cyberaanvallen.

Voor bestuurders is het daarom weinig zinvol om nu al conclusies te trekken over wat er precies in Engeland is gebeurd. Interessanter is de bredere ontwikkeling: aanvallers beschikken over steeds meer mogelijkheden om vitale infrastructuur daadwerkelijk te ontregelen. Wat betekent dat voor de weerbaarheid van de eigen organisatie?

Volgens Godfried Boshuizen, OT Cybersecurity Expert Stedin ligt een belangrijk deel van het antwoord niet bij de nieuwste technologie. De eerste prioriteit is fundamenteler: zorgen dat de basis aantoonbaar op orde is.

Cyber is een extra front geworden

Dat energie-infrastructuur een aantrekkelijk doelwit is voor statelijke en andere geavanceerde actoren, is niet nieuw. De aanvallen op de Oekraïense energievoorziening maakten dat ruim tien jaar geleden al duidelijk.

Wat wel verandert, is de kennis die aanvallers opbouwen over operationele technologie (OT): de systemen waarmee fysieke processen worden aangestuurd. Aanvallers zoeken volgens Boshuizen steeds gerichter naar manieren om OT-systemen en daarmee vitale infrastructuur te ontregelen.

Tegelijkertijd is cyber steeds sterker verweven met geopolitieke ontwikkelingen. Digitale aanvallen kunnen in het verlengde liggen van fysieke conflicten en spanningen tussen landen. Cyber is daarmee een extra front geworden.

Voor bestuurders maakt dat cybersecurity veel meer dan een IT-vraagstuk. Wanneer digitale aanvallen fysieke processen kunnen raken, gaat het direct over bedrijfscontinuïteit, operationeel risico en de maatschappelijke verantwoordelijkheid van de organisatie.

Ieder incident is een stresstest voor de eigen organisatie

Een incident in Polen of Engeland is niet alleen relevant voor de organisatie die wordt getroffen. Het biedt de hele sector informatie over de eigen weerbaarheid.

Daarom worden dergelijke incidenten op internationaal, nationaal en lokaal niveau geanalyseerd. Volgens Boshuizen staan daarbij twee vragen centraal: hoe gingen de aanvallers te werk en zou die aanpak ook bij onze infrastructuur kunnen werken?

Nieuwe inzichten kunnen vervolgens aanleiding zijn om bestaande beveiligingsmaatregelen opnieuw te beoordelen of aanvullende maatregelen te nemen. Cyberweerbaarheid is daarmee geen project

dat op enig moment ‘af’ is. Dreigingen veranderen, infrastructuur verandert en dus moet ook de verdediging continu worden getoetst en aangepast.

Voor het bestuur is daarbij vooral van belang om verder te kijken dan de vraag of maatregelen aanwezig zijn. Hoe weet de organisatie dat die maatregelen in de praktijk ook daadwerkelijk werken?

De grootste valkuil: de basis overslaan

AI, statelijke hackers en geavanceerde aanvalstechnieken krijgen veel aandacht. Begrijpelijk, maar volgens Boshuizen kan dat ook afleiden van een minder spannend onderwerp: de basishygiëne.

Bij cyberincidenten blijken fundamentele beveiligingsmaatregelen nog regelmatig onvoldoende op orde. Denk aan patchmanagement, netwerksegmentatie, toegangsbeheer en monitoring.

Juist voor OT-omgevingen is die basis cruciaal. Systemen hebben vaak een lange levensduur en beschikbaarheid van fysieke processen staat voorop. Dat vraagt niet alleen om een duidelijke scheiding tussen IT en OT, maar bijvoorbeeld ook om goede segmentatie binnen de OT-omgeving zelf.

De vraag aan securityverantwoordelijken zou daarom niet alleen moeten zijn: *hebben we dit geregeld?*

De betere vraag is: kunnen we aantonen dat het werkt?

Kijk verder dan het certificaat van een leverancier

Diezelfde kritische blik is nodig voor de keten.

Energiebedrijven zijn afhankelijk van een groot ecosysteem van leveranciers, technologiepartners en dienstverleners. Daarmee wordt de cyberweerbaarheid van de eigen organisatie mede bepaald door partijen buiten de eigen muren.

Een ISO-certificering van een leverancier biedt daarbij niet automatisch voldoende zekerheid. Volgens Boshuizen moeten organisaties ook daadwerkelijk toetsen of belangrijke leveranciers en ketenpartners voldoen aan het beveiligingsniveau dat voor kritieke processen nodig is.

Daarmee verschuift het gesprek op bestuursniveau van compliance naar daadwerkelijke weerbaarheid. Niet alleen vragen of aan een norm wordt voldaan, maar inzicht krijgen in de risico's die een leverancier introduceert en hoe die worden beheerst.

Vijf vragen voor de bestuurstafel

Nieuwe incidenten in de energiesector zouden daarom niet alleen aanleiding moeten zijn voor een technische analyse door securityteams. Ze kunnen ook worden gebruikt als moment voor bestuurlijke reflectie.

Iedere bestuurder zou volgens Godfried in ieder geval antwoord moeten kunnen krijgen op vijf vragen:

1. **Is onze basishygiëne aantoonbaar op orde?**
   Denk aan patching, netwerksegmentatie – ook binnen OT – toegangsbeheer en monitoring.
2. **Weten we welke systemen werkelijk kritiek zijn?**
   En belangrijker: zijn die systemen aantoonbaar voldoende afgeschermd?
3. **Wanneer is onze weerbaarheid voor het laatst onafhankelijk getoetst?**
   Niet alleen intern controleren, maar ook kritisch laten beoordelen of maatregelen daadwerkelijk functioneren.
4. **Weten we wat we doen als het toch misgaat?**
   Een incidentresponsplan op papier is niet genoeg. Het moet ook daadwerkelijk zijn geoefend.
5. **Hoe weerbaar is onze keten?**
   Leveranciers en partners kunnen onderdeel zijn van het aanvalsoppervlak. Hun beveiligingsniveau moet daarom niet alleen worden uitgevraagd, maar waar nodig ook worden getoetst.

Niet vragen óf het geregeld is, maar of het werkt

Over het gemelde incident in Engeland is nog te weinig bekend om conclusies te trekken over de oorzaak of aanvalsmethode. Maar dat maakt het incident voor bestuurders niet minder relevant.

De belangrijkste vraag is namelijk niet:

Kan precies deze aanval onze organisatie ook overkomen?

Maar:

Wat gebeurt er als morgen iemand onze kritieke processen probeert te verstoren – en hoe zeker weten we dat onze maatregelen dan standhouden?

Cyberweerbaarheid ontstaat niet door na ieder nieuw incident nóg een beveiligingsoplossing toe te voegen. Het vraagt erom te leren van incidenten in de sector, de eigen aannames voortdurend te toetsen en ervoor te zorgen dat fundamentele maatregelen aantoonbaar werken.

Voor bestuurders ligt daar misschien wel de belangrijkste les. Neem geen genoegen met de mededeling dat cybersecurity ‘geregeld’ is.

Vraag om bewijs dat de organisatie weerbaar is wanneer het er daadwerkelijk op aankomt.