Security in de energiesector

De eigen medewerker als zwakste schakel

DOOR KEES KAPPETIJN EN IMKE HERMANS

Bedrijven hebben grote belangen die constant en structureel bewaakt moeten worden. Het veiligstellen van deze belangen vraagt doorgaans aanzienlijke bedragen en organisatorische inspanningen. Bouwkundige en elektronische beveiliging zoals toegangsbeveiliging, cameracontrole en legitimatie met automatische terreindetectie. En organisatorische beveiliging zoals inlogprocedures, gedragscodes en firewalls voor ICT. Alles om binnen te houden wat binnen hoort. De zwakste schakel in de beveiligingsketen? Dat zijn de eigen medewerkers, vaak onwetend, meestal onbedoeld. De oplossing? Maak medewerkers bewust van deze zwakheid en de hele beveiligingsketen wordt sterker. Veel sterker.

Van iedereen die werkt voor een bedrijf of overheidsinstelling wordt een beveiligingsbewuste houding verwacht, maar van medewerkers in de energiesector wordt een extra inspanning gevraagd. De energiesector (elektriciteit, aardgas en olie) maakt onderdeel uit van de vitale infrastructuur, samen met de drinkwatersector, de telecommunicatie en de ICT-sector. De overheid verlangt in die sectoren extra alertheid van medewerkers bij de beveiliging van gebouwen en installaties (fysieke beveiliging) en processen (informatiebeveiliging). Uitval van vitale voorzieningen heeft immers snel brede impact op de samenleving en kan daarmee in relatief korte tijd tot maatschappelijke onrust of ontwrichting leiden. Welk bedrijf kan vier uur zonder stroom of (drink)water zonder daar de negatieve effecten van te merken? Criminelen en terroristen kunnen hier hun voordeel mee doen. In 2013 zijn 151 van de 256 geregistreerde cyberincidenten op de kritische infrastructuur in Amerika toegeschreven aan de energiesector. Alerte medewerkers zijn dus van belang, hiermee staat security awareness voor de opkomende Energy Valley in Noord-Nederland bovenaan de agenda.

USB-STICK

De focus op 'de alerte en veiligheidsbewuste medewerkers' in de energiesector is geen nieuw gegeven. De overheid ontwikkelt al jaren programma's, samen met de branche, voor bedrijven die onderdeel uitmaken van de vitale infrastructuur. Programma's die gericht zijn op het verhogen van de security awareness. Helaas blijken organisaties vaak nog niet alert genoeg. Voorbeelden laten zien dat de energiesector wereldwijd, maar ook in Nederland vaak slachtoffer is van grootschalige inbreuken en hackacties. GazProm raakt na een hack in 1998 (met hulp van binnenuit…) de controle over haar processen 24 uur kwijt, het Department of Energy in Amerika scoort bijna honderd procent op tachtig penetratietesten bij energiebedrijven in 2004. Nog in 2013 halen twee Amerikaanse energiebedrijven kwaadaardige software binnen via een USB-stick van medewerkers. USB-sticks die door een IT-medewerker (!) regelmatig werd gebruikt voor configuratie-updates. En in Nederland, waar een regionaal energiebedrijf alle systeemapparatuur in een (niet-afgesloten) ruimte heeft staan die ook toegang geeft tot de bezemkast voor schoonmakers. Denk aan de golf van (D)Dos-aanvallen in 2013 die vooral de sectoren financiën en overheid raakten, en voor het ministerie van Veiligheid & Justitie aanleiding waren om ook de bedrijven uit de vitale sector op strategisch niveau aan te laten sluiten voor kennisdeling.

CYBER-RISICO'S

Criminelen proberen door middel van cyberaanvallen bedrijfssystemen te benaderen, om waardevolle informatie te verkrijgen of om systemen te saboteren. Eigen gewin of andermans chaos. Door dergelijke aanvallen kan bijvoorbeeld de leveringszekerheid van elektriciteit in gevaar komen. Doorgaans onderschatten medewerkers de risico's die ze kunnen veroorzaken via ICT, door USB-uitwisseling

Foto: Danny Cornelissen

of 'gewoon' internetgebruik, zoals de gevaren van phishing. Phishing is een veelgebruikte methode door hackers en kan het beste worden omschreven als het verleiden van werknemers tot het openbaar maken van gevoelige informatie door middel van nep-e-mails en gefingeerde websites. Geen enkele medewerker wil door onoplettendheid of een lek in zijn beveiligingssoftware onbewust een virus binnenhalen dat vervolgens het complete bedrijfsnetwerk platlegt en discontinuïteit van een of meerdere bedrijfsprocessen veroorzaakt. Security awareness op cyber-risico's verdient dus extra aandacht.

EEN SLUITENDE BEVEILIGINGSKETEN

De beveiligingsketen is krachtig in al z'n eenvoud, mits consequent gevolgd: een veilig proces in een veilig gebouw met veilige installaties, verpakt in veilige organisatorische processen. Met mensen die hun werk doen met inachtname van deze veiligheden. Dat mensen de vereiste veiligheden niet altijd honoreren, is geen kwaadwil. Ze zijn eenvoudigweg niet (goed genoeg) bewust gemaakt van de dreigingen, de impact op de bedrijfsvoering en de schade die het bedrijf en haar klanten kunnen lopen door onveilig handelen. Financiële en materiële schade, aansprakelijkheid, imagoschade, impact op de bedrijfscontinuïteit? Dit bewustzijn is nu juist zo belangrijk. Beveiligingsbewuste medewerkers kunnen beveiligingsincidenten voorkomen die het bedrijf veel schade kan besparen. Technische, bouwkundige en organisatorische beveiligingsmaatregelen worden in samenhang gekozen zodat ze elkaar versterken. Deze maatregelen op zich zijn niet voldoende (hoe kostbaar ze vaak ook zijn), ze verliezen hun waarde als medewerkers er niet juist mee omgaan. Medewerkers vormen dus uiteindelijk de belangrijkste schakel om de beveiligingsketen krachtig te maken en te houden.

SCHADEDREIGING

Op het gebied van beveiliging lag de focus vroeger primair op fysieke afscherming van terreinen en gebouwen. Maar 'binnen' en 'buiten' het bedrijf zijn inmiddels relatieve en gedateerde begrippen geworden. Toegangscontrolesystemen met pasjes en bijbehorende autorisaties zijn ontoereikend als medewerkers onderling pasjes aan elkaar uitlenen en zo onbevoegden toegang verschaffen. De inbraakwerende functie van deuren en poorten komt te vervallen als deze niet deugdelijk worden afgesloten. Echter, niet alleen fysieke beveiliging kent beperkingen als medewerkers er niet op de juiste wijze mee omgaan. Dit geldt ook voor informatiebeveiliging. Toegang tot een bedrijf kun je vanuit een ver en exotisch land regelen. Smartphones, tablets en andere digitale informatiedragers kunnen open platforms zijn met vaak vertrouwelijke informatie die via open verbindingen eenvoudig beschikbaar worden gemaakt. Het gevaar hierbij is dat medewerkers sneller onzorgvuldig met deze vertrouwelijke informatie omgaan. Bij verlies van het apparaat kan vertrouwelijke informatie eenvoudig in handen komen van kwaadwillenden, met schadedreiging tot gevolg.

BEDRIJFSGEVOELIGE INFORMATIE

Dat het van groot belang is dat medewerkers zorgvuldig met vertrouwelijke bedrijfsinformatie omgaan, blijkt uit een reeks pijnlijke incidenten uit het verleden. Zoals eerder aangehaald: de IT-medewerker die niet secuur met z'n USB-stick omgaat. Maar ook de officier van justitie die een pc vol met vertrouwelijke informatie op straat bij het grof vuil zet, medewerkers van defensie die USB-sticks met daarop staatsgeheimen verliezen, een rechter die zijn aktetas met daarin twee strafdossier in de trein laat liggen of laptops met daarop bedrijfsgevoelige informatie die uit leaseauto's worden gestolen. Het zijn allemaal bekende voorbeelden van situaties waarin bedrijfsgevoelige informatie bewust of onbewust op straat is komen te liggen. In al deze voorbeelden blijken mensen de zwakste schakel.

> Zorg dat security awareness op de agenda komt te staan in de dagelijkse werk- en verantwoordingsprocessen

VAN ONBEWUST NAAR BEWUST

De belangrijkste manier om de beveiligingsketen sluitend te krijgen, en de zwakste schakel te versterken, is om medewerkers beveiligingsbewust te maken. Dit wordt ook wel security awareness genoemd. Security awareness is de mate waarin medewerkers het belang van de beveiliging voor de organisatie begrijpen en accepteren en hier vervolgens ook naar handelen. Enerzijds gaat het om het begrijpen van de fysieke beveiliging en anderzijds de beveiliging van informaties (assets) van een organisatie. Als medewerkers het doel en het nut van beveiligingsmaatregelen begrijpen, zullen ze meer geneigd zijn zich aan die maatregelen te houden. Medewerkers dienen zich ervan bewust te zijn dat een organisatie in de huidige maatschappij eenvoudig grote negatieve effecten ervaart als vertrouwelijke documenten op straat komen te liggen. Klanten kunnen voelen dat, als er niet zorgvuldig met klantinformatie wordt omgegaan, dit ook wel zo zal zijn met de administratie en overige processen van de organisatie. Burgers vragen zich bezorgd af: 'Hoe eenvoudig kan de levering van stroom worden onderbroken?' Of: 'Wordt mijn drinkwater wel zorgvuldig en veilig gemaakt?'. Die zorgen zijn des te groter als blijkt dat criminelen of terroristen eenvoudig toegang tot bedrijven hebben gehad met het oogmerk belangrijke processen bewust te verstoren. Het zijn gebeurtenissen die grote maatschappelijke onrust kunnen veroorzaken en die bedrijven serieus in de problemen kunnen brengen door omzetverlies of juridische gevolgen. Beveiligingsbewuste medewerkers kunnen dus direct of indirect verstoringen van bedrijfsprocessen helpen voorkomen. Een diepgeworteld awareness bij medewerkers is dus

Vijf stappen naar security awareness

Het kweken van beveiligingsbewustzijn is een continu proces. Vaak is pas na enige tijd resultaat zichtbaar. Menselijk gedrag verander je niet zomaar, zeker niet als je al jaren gewend bent om op een bepaalde manier te werken. Ontwikkel daarom een bewustwordingstraject voor de langere termijn op basis van een stappenplan.

Stap 1: Bepaal om te beginnen de risico's en dreigingen. Wat kan ons overkomen? Vertaal die risico's vervolgens naar de impact die ze hebben op de bedrijfsvoering. Leg vervolgens in richtlijnen en procedures vast wat van de medewerkers wordt verwacht ten aanzien van veilig werken. Ga met de meest risicovolle groep medewerkers om de tafel zitten en bekijk wat hun rol is en waarom zij in het bijzonder kwetsbaar zijn voor beveiligingsincidenten. Vaak zijn het medewerkers die met kritische bedrijfsprocessen te maken hebben, zoals operators.

Stap 2: Creëer bewustzijn. Een programma op maat is belangrijk, bepaal ook welke minimale basiskennis alle medewerkers dienen te hebben. Stel basisbeveiligingsregels op en zorg dat deze bekend worden bij alle medewerkers. Train medewerkers jaarlijks in beveiligingsbewustzijn. Dat kan via presentaties of een interactief rollenspel. Zorg er als management ook voor dat het thema regelmatig op tafel komt tijdens werkoverleg. De Nationaal Coördinator Terrorismebestrijding en Veiligheid (NCTV) heeft materiaal ontwikkeld om bedrijven en overheidsdiensten te ondersteunen bij hun bewustwordingscampagnes. Zoals 'Zeker van je Zaak' en 'Alert online'. Dit zijn prima algemene hulpmiddelen, maar een bewustwordingscampagne heeft meer effect als die is toegesneden op de organisatie. Laat de eerder aangewezen ambassadeurs meedenken over de inhoud van het programma, zodat het programma steeds blijft aansluiten bij het niveau en de belevingswereld van medewerkers. 'Het gaat over ons!'

Stap 3: Meten is weten. Bouw controle- en ijkmomenten in. Om de effectiviteit van een awarenessprogramma te meten, kan bijvoorbeeld gebruik worden gemaakt van een mystery guest. Die kan periodiek testen in hoeverre medewerkers bedrijfsgevoelige informatie loslaten. Verder kunnen leidinggevenden onverwacht controleren op naleving van de beveiligingsvoorschriften, zoals de 'clean desk policy' en de afdeling ICT kan zogenaamde phishingmails naar medewerkers sturen om na te gaan hoeveel medewerkers op de verdachte link klikken. Op deze manieren kan proefondervindelijk worden vastgesteld of het beveiligingsbewustzijn bij de medewerkers begint te aarden en in hoeverre nog bijsturing nodig is.

Stap 4: Formuleer en implementeer sanctiebeleid: bepaal wat normaal gedrag is dat van iedereen verwacht wordt, en formuleer beloningsbeleid voor bijzondere positieve uitschieters en straffen voor negatieve uitschieters. Wees in de omgang met beide uitschieters niet terughoudend, beloon ruim wat zich positief onderscheidt, en bestraf fair wat bij herhaling fout gaat. Stuur op meer beloningen dan straffen...

Stap 5: Maak beveiligingsbewustzijn onderdeel van de reguliere bedrijfsvoering. Betrek het thema in beoordelingsgesprekken en zorg dat medewerkers elkaar aanspreken op het niet naleven van voorschriften. Met behulp van ludieke acties kan een aanspreekcultuur worden gecreëerd en kan positief beveiligingsgedrag worden beloond. Zo kan bijvoorbeeld een afdelingstop-3 worden gemaakt van medewerkers die hun werkplek het best opruimen. In een bedrijf met een goede beveiligingscultuur is het belangrijk dat collega's elkaar scherp houden. Als een medewerker zijn computer niet heeft vergrendeld bij het verlaten van zijn werkplek, stuur dan uit zijn naam een bericht naar zijn leidinggevende. Signaleer je dat een collega zijn zakelijke telefoon onbeheerd op het bureau heeft laten liggen? Neem deze dan mee en laat de betreffende medewerker de telefoon bij jou ophalen. Scherpe lessen, maar ze geven medewerkers wel inzicht in hun gedrag.

belangrijk voor elk bedrijf. Zie het kader voor de vijf stappen naar awareness.

BEVEILIGING IS IETS VAN ONS ALLEMAAL

Niet alleen van medewerkers wordt een alerte houding verwacht, gestart moet worden bij het management dat hier een voorbeeldfunctie in heeft. Beveiliging is van ons allemaal. Een voorwaarde voor het succesvol verhogen van de security awareness bij medewerkers is dat het thema een plek krijgt in het hart van het bedrijf: het besturingsmodel. Zorg dat security awareness op de agenda komt te staan in de dagelijkse werk- en verantwoordingsprocessen. Het management moet zich ervan bewust zijn dat zij hier een belangrijke voorbeeldfunctie heeft. Het naleven van beveiligingsmaatregelen moet een vanzelfsprekend onderdeel worden van het dagelijks werk. Leidinggevenden spelen hierin een belangrijke, sturende rol. Herinner medewerkers er bijvoorbeeld regelmatig aan hoe belangrijk het voor een bedrijf is dat bedrijfsinformatie geheim moet blijven. Het lekken van bedrijfsgevoelige informatie richting de buitenwereld kan grote gevolgen hebben voor een bedrijf. Medewerkers dienen zich hier bewust van te zijn. Zorg er dus voor dat de zwakste schakel de sterkste wordt.

KappetijnBriks is een jonge adviesorganisatie, opgericht door ervaren adviseurs, die zich richt op de beleidsvelden brandweerzorg, risico- en crisisbeheersing en externe veiligheid. Adviseurs van KappetijnBriks ondersteunen bedrijven en overheden in het veiligheidsveld bij het nemen van beslissingen over de inrichting van een veilige leefomgeving, de organisatie van veilig werken en beheersing van risico's en bedrijfscontinuïteit. Veiligheidsregio's en BRZO-bedrijven worden ondersteund bij de inrichting en voorbereiding van hun hulpdiensten en operationele bestrijdingsorganisaties. Omdat voorbereiden loont. www.kappetijnbriks.nl ■