Beveiligingsbewustzijn in de nutssector

Verschijningsdatum: 1 augustus 2014

Geschreven door:
Imke Hermans, junior veiligheidsadviseur bij KSS

Opleiding:
2013: OCR / Rampenbestrijding & Crisisbeheersing, Brandweer Zuid Limburg
2010-2011: Master Forensica, Criminologie en Rechtspleging, Universiteit Maastricht
2006-2010: Integrale Veiligheid, Avans Hogeschool 's-Hertogenbosch

Werkervaring:
Jan 2013 – mrt 2014: Medewerker security & crisisbeheersing bij Waterleiding Maatschappij Limburg
Apr 2014: Adviseur Kappetijn Safety Specialists, betrokken bij de volgende projecten:

- Waterleiding Maatschappij Limburg: beleidsadviseur security awareness, cybersecurity & crisisbeheersing
- Gezamenlijke Brandweer: ontwikkelaar & organisator crisisopleiding level 3 Bedrijfsdeskundige
- Veiligheidsregio Noord-Holland Noord: opstellen rampenbestrijdingsplan Onderzoekslocatie Petten
- Veiligheidsregio Limburg-Noord: uitvoeren organisatieanalyse

Samenvatting

Binnen de nutssector wordt steeds meer aandacht gevraagd voor beveiligingsbewustzijn: de mate waarin medewerkers het belang van beveiliging voor de organisatie begrijpen en hier ook naar handelen. Beveiligingsbewustzijn als 'grondhouding' is belangrijk op alle niveaus binnen een organisatie. Oplettende medewerkers die de beveiligingsmaatregen in acht nemen, kunnen verstoring van bedrijfsprocessen door incidenten voorkomen. Zo kan de organisatie kosten besparen, imagoschade vermijden, aansprakelijkheden voorkomen en de continuiteit van de dienstverlening waarborgen.

Beveiligingsbewustzijn ontstaat niet van de ene op de andere dag. Basisprincipes kun je vastleggen in een reglement, ernaar leven en handelen is een attitude die moet groeien. Een bewustwordingsprogramma op maat kan helpen dat doel te bereiken. Beveiligingsbewustzijn gaat de hele organisatie aan. Leidinggevenden hebben een voorbeeldfunctie, van hen wordt verwacht dat zij hun medewerkers stimuleren om hun bijdrage te leveren aan een goed beveiligde werkomgeving.

Beveiliging is iets van ons allemaal
"Beveiligingsbewustzijn in de nutssector"

Van iedereen die werkt voor een bedrijf of overheidsinstelling wordt een beveiligingsbewuste houding verwacht, maar van medewerkers van nutsbedrijven wordt een extra inspanning gevraagd. De nutssector (energie, gas, drinkwater) maakt deel uit van de vitale infrastructuur, net als bijvoorbeeld gezondheidszorg (ziekenhuizen), de ICT-sector en zeehavens. De overheid verlangt in die sectoren extra alertheid van medewerkers bij de beveiliging van gebouwen, installaties en processen, omdat uitval van vitale voorzieningen kan leiden tot maatschappelijke onrust of ontwrichting. Maar wat is beveiligingsbewustzijn? En hoe maak je medewerkers beveiligingsbewust? Dit artikel beantwoordt deze vragen en geeft een aantal praktische tips.

Wat is beveiligingsbewustzijn?

Beveiligingsbewustzijn is de mate waarin medewerkers het belang van beveiliging voor de organisatie begrijpen en hier ook naar handelen. Als medewerkers het doel en het nut van beveiligingsmaatregelen begrijpen, zullen ze meer geneigd zijn zich aan die maatregelen te houden. Beveiligingsbewuste medewerkers kunnen direct of indirect verstoringen van bedrijfsprocessen voorkomen. Dat is in het belang van de bedrijfscontinuïteit. Een goede beveiligingscultuur kan organisaties geld besparen, helpt imagoschade voorkomen, verhoogt de

leveringsbetrouwbaarheid en draagt bij aan de klantvriendelijkheid en serviceverlening. Een diepgeworteld beveiligingsbewustzijn bij de medewerkers is dus belangrijk voor elke organisatie.

Beveiligingsbewustzijn lijkt vanzelfsprekend, maar het is opvallend dat we in onze thuissituatie beter op beveiliging letten dan op het werk. Thuis vinden we het bijvoorbeeld logisch om ramen en deuren te voorzien van goed hang- en sluitwerk, trouwboekjes, paspoorten en belangrijke sleutels in een kluiskastje te bewaren en pincodes en wachtwoorden gescheiden te bewaren van banknummers en inlognamen. In de werkomgeving lijken we over het algemeen echter minder alert te zijn op beveiligingsrisico's. Zakelijke communicatiemiddelen laten we vaak onbeveiligd en onbeheerd achter, met vertrouwelijke documenten wordt niet altijd zorgvuldig omgegaan en contracten versturen we steeds vaker als PDF via de mail. En de bedrijfspoort laat men voor het gemak open, want het is zo'n gedoe om deze steeds te openen en te sluiten voor in- en uitgaand verkeer. Dan is er het thuiswerken, dat steeds populairder wordt bij zowel het bedrijfsleven als de overheid. Heel fijn dat die mogelijkheid er is, maar dan moeten we er wel voor waken dat we bedrijfsgevoelige informatie die we mee naar huis nemen onderweg niet verliezen en dat vertrouwelijke documenten nooit onbeheerd op de keukentafel blijven liggen.

Waarom is het belangrijk dat medewerkers beveiligingsbewust zijn?

Qua beveiliging lag de focus vroeger vooral op fysieke afscherming van terreinen en gebouwen. Maar die geweldige stalen hekconstructie heeft weinig nut als medewerkers dit hek niet goed afsluiten. En toegangscontrolesystemen met pasjes voor geautoriseerde personen werken niet als medewerkers onderling pasjes aan elkaar uitlenen en zo onbevoegden toegang verschaffen. Maar niet alleen fysieke beveiliging kent beperkingen als medewerkers er niet juist mee omgaan. Dat geldt ook voor bijvoorbeeld informatiebeveiliging. Mooi spul, die smartphones, tablets en digitale informatiedragers. Ze maken het gemakkelijk om onderweg in de trein even snel de mail in te zien of een document te lezen. Maar bij verlies van het apparaat kan gevoelige informatie gemakkelijk in handen komen van anderen met snode bedoelingen.

Medewerkers dienen zich ervan bewust te zijn dat een organisatie in de huidige maatschappij imagoschade, financiële schade en zelfs continuïteitsschade kan oplopen, als vertrouwelijke documenten op straat komen te liggen. Klanten kunnen voelen dat, als 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: 'Wordt mijn drinkwater wel zorgvuldig en veilig gemaakt?' Of: 'Hoe eenvoudig kan de levering van stroom worden onderbroken?' Die zorgen zijn des te groter als blijkt dat criminelen of terroristen eenvoudig toegang tot de organisatie 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. Een stevig beveiligingsbewustzijn bij alle medewerkers kan deze situaties helpen voorkomen.

Wat kunnen we uit het voorgaande concluderen? Technische en bouwkundige beveiligingsmaatregelen zijn nodig en belangrijk, maar de medewerker is de belangrijkste schakel om de keten sluitend te maken. Technische, bouwkundige en organisatorische maatregelen dienen in samenhang te worden gekozen en moeten elkaar versterken.

Hoe maak je medewerkers beveiligingsbewust?

Beveiligingsbewustzijn kan alleen groeien als het thema regelmatig bij de medewerkers onder de aandacht wordt gebracht. Wijs daarom iemand aan binnen de organisatie die dit traject coördineert. Bijvoorbeeld de security manager of de facility manager. Als er geen verantwoordelijke is met de opdracht om het proces te sturen en te coördineren, bestaat het risico dat het bewustzijnstraject verslapt. De aangewezen coördinator en de leidinggevenden moeten medewerkers op een stimulerende manier meenemen in het bewustwordings-traject. Een valkuil is dat activiteiten worden bedacht die niet aansluiten bij de belevingswereld van de medewerkers. Dat is funest, omdat medewerkers dan minder zullen open staan voor gedragsverandering. Een goede methode is om binnen de organisatie 'ambassadeurs' te zoeken, mensen met uitstraling die andere medewerkers kunnen enthousiasmeren. Zo kan het bewustzijnsprogramma met meer effect worden uitgedragen in de organisatie.

Beveiligingsbewustzijn dient ook een plek te krijgen in het stuurmodel van de organisatie. Verwachtingen jegens de medewerkers moeten worden vastgelegd en een vanzelfsprekend onderdeel zijn van het dagelijks

werk. Leidinggevenden spelen hierin een belangrijke sturende rol. Zorg er dus voor dat beveiligingsbewustzijn op de agenda van het management komt te staan. En maak het management duidelijk dat zij in het bewustwordingstraject een voorbeeldfunctie heeft!

Voor security managers of facility managers is het belangrijk dat zij medewerkers kunnen meenemen in 'hun wereld'. Managers moeten medewerkers op een herkenbare manier het waarom achter de beveiligingsmaatregelen tonen. Ook moeten zij de medewerkers duidelijk maken dat zij een onmisbare rol spelen in de beveiliging van hun organisatie. Zo wordt het draagvlak onder de medewerker vergroot, ze zijn belangrijk! Tussen beveiligingsbewust denken en er ook daadwerkelijk naar handelen zit nog wel een verschil. Hoe kunnen we denken omzetten in daden? De beste manier om medewerkers aan te zetten tot veilig handelen is om ze zoveel mogelijk ter plekke op het gewenste gedrag te wijzen en ze direct de (mogelijke) gevolgen van hun handelen te laten inzien.

Nadat medewerkers begrip hebben gekregen voor nut en noodzaak van beveiligingsmaatregelen, komt vaak de volgende vraag: 'Ja maar, hier gebeurt toch nooit iets?' Mensen beseffen vaak niet dat hun vitale organisatie kwetsbaar is voor criminelen of terroristen. Een oplettende houding van medewerkers kan criminaliteit voorkomen. Als medewerkers vreemden in een kantoorlocatie of op een buitenterrein durven aanspreken, kan bijvoorbeeld ongewenste insluiping worden voorkomen. Een promotiefilm van ProRail van enkele jaren geleden laat zien dat een oplettende medewerker van de Spaanse spoorwegen een aanslag heeft kunnen voorkomen doordat hij bij zijn leidinggevende aan de bel trok toen hij een verdachte tas tussen het spoor zag liggen. In de tas bleken explosieven te zitten.

Het is goed om medewerkers inzicht te geven in de incidenten die eerder in de organisatie hebben plaatsgevonden. Dan komen zij wellicht tot de conclusie dat er toch meer beveiligingsincidenten gebeuren dan ze dachten. Ook moet het belang van het melden van incidenten en verdachte situaties worden benadrukt en moet er een goede meldingsprocedure zijn, die bij iedereen bekend is. Als een organisatie inzicht heeft in voorgekomen incidenten en bijna-incidenten, kan actie worden ondernomen om herhaling te voorkomen. Laat medewerkers ook zien wat de organisatie met meldingen doet.

Een risico dat ook niet onderschat moet worden is het fenomeen 'social engineering'. Een social engineer is iemand met vaak een nette en gezaghebbende uitstraling, die probeert bedrijfsgevoelige informatie bij medewerkers te ontfutselen of spullen te ontvreemden. Deze sluwe vos speelt dan in op de goedheid van medewerkers. Het is altijd fijn als je iemand de weg kunt wijzen of als je iets interessants over je organisatie kunt vertellen. Een social engineer kan ook telefonisch of per mail proberen bedrijfsgevoelige informatie te verkrijgen. Maak dus bindende afspraken over welke informatie telefonisch en per mail wel of niet wordt gedeeld. Spreek ook af hoe je een beller kunt verifiëren.

Tot slot is er een nieuwe trend op het gebied van beveiligingsbewustzijn: cyber security awareness, aandacht voor de risico's en gevaren van de digitale snelweg. Sinds vorig jaar besteedt de overheid actief aandacht aan cyber security. Veel mensen onderschatten de risico's die ze lopen bij internetgebruik, zoals de gevaren van phishing. Niemand wil door onoplettendheid of een lek in zijn beveiligingssoftware onbewust een virus binnenhalen dat vervolgens het complete bedrijfsnetwerk platlegt. Ook internetbeveiliging vraagt dus aandacht om de beveiligingscultuur van een organisatie compleet te maken.

Tips voor een bewustwordingsprogramma

Het kweken van beveiligingsbewustzijn is een continu proces. Vaak is pas na enige tijd resultaat zichtbaar. Dit is logisch, 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 en stel een stappenplan op voor de uitvoering.

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, maar bepaal ook welke minimale basiskennis alle medewerkers dienen te hebben. Stel basisbeveiligingsregels op en zorg dat deze bekend worden bij alle medewerkers. Verder is het belangrijk dat medewerkers jaarlijks worden getraind 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 hulpmiddelen, maar een bewustwordingscampagne heeft meer effect als die qua inhoud en presentatie 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 het 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: 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. Dat zal werken. 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. Laat hem wel eerst even zoeken, die telefoon kan toch niet zomaar weg zijn? Het zijn harde lessen, maar ze geven medewerkers wel inzicht in hun gedrag.

Slot

Een hoger beveiligingsbewustzijn kweken in een organisatie is geen eenmalige actie, maar vraagt een continu inspanning. Van alle medewerkers in alle lagen van de organisatie, directie en management voorop. Het is belangrijk om de vinger aan de pols te houden en te meten wat het effect is van acties die beveiligingsbewustzijn moeten stimuleren. Is er weerstand tegen beveiligingsmaatregelen? Bekijk dan of ze net even anders ingericht kunnen worden. Vaak heerst bij medewerkers het gevoel dat beveiligingsmaatregelen lastig zijn en extra werk opleveren. Minder overlast vergroot het draagvlak. Na verloop van tijd zal het traject zijn vruchten afwerpen en kan de conclusie worden getrokken dat met een relatief kleine investering een beter beveiligingsbewustzijn kan worden gecreëerd.