eBook

Veiligheid in de organisatie



De meest gelezen blogs van dit moment!

Veiligheid in de organisatie

Beste lezer,

Ken je dat? Jij bent verantwoordelijk voor de veiligheid binnen jouw organisatie. Of het nu gaat om gebouwveiligheid, informatieveiligheid of veiligheid op de werkvloer….. als er iets te doen is op het gebied van veiligheid komen ze naar jou! Dit zou echter niet het geval moeten zijn want je bent gezamenlijk verantwoordelijk voor de veiligheid in jullie organisatie.

Loop jij ook tegen de volgende vraagstukken aan:

- Hoe overtuig je mensen die al jarenlang op een bepaalde manier werken?
- Hoe zorg je voor urgentiebesef bij zowel MT als medewerkers?
- Hoe vergroot je het veiligheidsbewustzijn in jouw organisatie?

In dit eBook lees je de 16 best gelezen blogs over veiligheid in de organisatie van dit moment.

Veel leesplezier!

Liz de Bie, congres-en opleidingsmanager veiligheid bij het Studiecentrum voor Bedrijf en Overheid

Inhoudsopgave:

Constructieve veiligheid AZ stadion. Goede raad is duur…….

We worden met regelmaat opgeschrikt door constructief falen bij een gebouw of een gebouwd complex. Gelukkig zijn er niet vaak slachtoffers te betreuren, maar dat is meer geluk dan wijsheid.

De instorting van de in aanbouw zijnde parkeergarage in Eindhoven heeft grote gevolgen gehad voor de toepassing van een bepaald vloertype, de breedplaatvloer die met zelf-verdichtend beton wordt gemaakt. De instorting vond plaats in mei 2017 en nu worden nog steeds reeds bestaande gebouwen gecontroleerd en versterkt als het volgens de daarna ontwikkelende reken-technische controles noodzakelijk blijkt te zijn.

Onlangs gebeurde het onverwachte in het AZ stadion in Alkmaar. Een gedeelte van het stadiondak stortte in bij een relatief hoge windbelasting. In eerste instantie worden door de media reacties gevraagd aan de betrokkenen en in hun commentaar hoor je direct een aantal zaken die tijdens de bouw niet volgens de normale procedures zijn verlopen. Veel betrokkenen spreken daar hun frustraties over uit. De betrokkenen verkleinen hun rol in de nieuwbouw en leggen snel de verantwoording bij 1 van de andere partijen. Opmerkingen die we aan kunnen halen: “De opdrachtgever wilde te goedkoop bouwen”. “De hoofdconstructeur had een beperkte opdracht”. “De detaillering was de taak van de staalbouwer”. “We moesten op het randje van de mogelijkheden ontwerpen”. “De hoofdconstructeur heeft aangegeven met welke belastingen we moesten rekenen”.

Deze opmerkingen geven direct al aan dat de verantwoordelijkheid voor de hoofddraagconstructie is verdeeld over meerdere partijen. Het is daarom heel complex om uit te zoeken wie de calamiteit heeft veroorzaakt. Nog belangrijker is de vraag hoe het voorkomen had kunnen worden.

Veel antwoorden zijn gegeven in het rapport van de raad voor de veiligheid, die het voorval heeft onderzocht. Vervolgens geeft het rapport van RHDHV, in opdracht van AZ, een gedetailleerde beschrijving van het bezwijkmechanisme. Een verkeerd gedetailleerde verbinding tussen de kolom en de dakliggers, dit is overigens de belangrijkste verbinding in het gehele complex, is verkeerd ontworpen met de verkeerde uitgangspunten van de windbelasting en is vervolgens met lichtere lassen uitgevoerd dan de berekening aangeven. Kortom op alle fronten tekortkomingen in het ontwerp en de uitvoering. De controle maatregelen tijdens de bouw hebben vervolgens ook gefaald.

Naast de conclusies van de onderzoekers zijn er nog meerdere opmerkingen te maken over de gang van zaken. De KNVB stelt veiligheidseisen aan stadions en organisaties van clubs die voetballen in de betaald voetbalcompetities: ze krijgen pas een licentie als de veiligheidsverklaring is ingevuld en ondertekend.

De KNVB vereist van de club en de gemeente dat het stadion waarin men speelt een periodieke veiligheidscontrole onder gaat. In dat geval gaat het onder andere over brandveiligheid, publieksveiligheid, veiligheid van vluchtwegen, constructieve veiligheid, controle van de medische hulpverlening (zoals EHBO-ruimten en de opstelplaats van de ambulance) en eisen ten aanzien van het ontruimingsplan en operationele oefeningen.

De eisen en normen (volgens bouwbesluit) ten aan zien van constructieve veiligheid die aan de veiligheidsverklaring ten grondslag liggen sluiten niet aan bij de praktijk. De gebruiksfunctie van een voetbalstadion wijkt af van andere bouwwerken die onder het Bouwbesluit vallen, zoals kantoren en ziekenhuizen. Omdat de voorschriften uit het Bouwbesluit zo breed zijn, is specifieke expertise vereist om te controleren of een stadion aan de gebruikseisen voldoet.

Het is goed om eens naar de aanpak in het Verenigd Koninkrijk te kijken.

In het Verenigd Koninkrijk is de '*Guide to Safety at Sports Grounds*' van toepassing (de *Green Guide*). Daarin staan wél specifieke regels voor voetbal- en andere sportstadions, onder meer over dakconstructies, tribunes en vluchtroutes.

In 2016 concludeerde het auditteam Voetbal en Veiligheid van het ministerie van Justitie en Veiligheid dat stadions soms gecontroleerd worden door mensen die onvoldoende verstand hebben van voetbalstadions. Het is helaas deze conclusie die bij uitstek van toepassing is op de gang van zaken in Nederland. In het bouwbesluit wordt niet aangegeven welke vakkennis de controleur constructieve veiligheid zou moeten hebben. Daarnaast wordt het vak construeren door opdrachtgevers en bouwmanagers niet op waarde beoordeeld, maar vaak als een bijzaak opgepakt. Waarschijnlijk met het idee dat constructies voldoende reserve capaciteit hebben. In de Engelse Green Guide is aangegeven dat de controle dient te worden uitgevoerd door een Chartered Engineer. In Nederland is er door de branche een constructeurs-register ingesteld, de in het register opgenomen Register Ontwerpers zijn in staat om een veiligheidscontrole op oordeelkundige wijze uit te voeren. In het geval Alkmaar zou zo'n controleur zeker de vinger op de zwakke plek hebben gelegd.

Het audit team Voetbal en Veiligheid zou regels moeten opstellen waarin wordt aangegeven welke normen en eisen aan de controle dienen te worden gesteld en welke vakkennis en opleiding de controleurs moeten bezitten die verantwoordelijk voor de controle moeten zijn.

De Nederlandse constructeurs zouden ook een voorbeeld kunnen nemen aan hun Engelse collega's, in het Verenigd Koninkrijk zijn speciale seminars voor Stadium Design, hier wordt veel aandacht besteed en discussie gevoerd over de constructieve veiligheid. Voor een gebouw met een publieksfunctie en de dynamische belastingen veroorzaakt door de mensenmassa is een regelmatige update van de state of the art geen overbodige luxe.

Geschreven door Jan van der Windt, Constructeur, Register Ontwerper

9 gouden tips bij gebouwontruiming

1. **Bij twijfel doen!**
   Als je twijfelt of er daadwerkelijk wat aan de hand is, ga dan toch de ontruiming starten en ga niet eerst onderzoeken of je vermoeden klopt. Als je te vroeg hebt gealarmeerd hebt dan is het een goede oefening en is iedereen veilig. En bedenk bij twijfel: Als je te laat alarmeert kunnen er slachtoffers vallen.

2. **Houd nooduitgangen en vluchtroutes vrij**
   Plaats geen stoelen, opgeslagen spullen, kerstbomen etc. in deze ruimtes. De architect heeft de ruimtes niet voor niks op deze manier ontworpen en heeft de ruimte er niet op berekend dat er extra spullen worden neergezet. Bij inspectie door de overheid kunnen geblokkeerde nooduitgangen ook bestuurlijke boetes opleveren!

3. **Doe de polonaise**
   Je ontruimt het gebouw het snelst als iedereen in polonaise naar buiten loopt omdat mensen achter elkaar aanlopen en met korte afstand van elkaar lopen. Daarnaast houd je overzicht doordat je weet wie er achter elkaar naar buiten loopt.

4. **Houd rekening met de zelfredzaamheid**
   De mate van zelfredzaamheid bij een ontruiming bestaat uit 3 factoren:
   - Menskenmerken: invalide mensen, reactievermogen, awareness van dreiging etc.
   - Gebouwkenmerken: complexe infrastructuur, hoogbouw etc.
   - Brandkenmerken: soort brand

5. **BHV'ers zijn ook 'gewoon' mensen**
   Zij kunnen **alleen** in veilig gebied werken want zij kunnen net als jij ook niet tegen rook en het gele hesje beschermd hen daar niet tegen. Train de BHV-organisatie regelmatig op lastige keuzes die zich voordoen in het proces van ontruiming. Vrijwillige deelname aan de BHV-organisatie is effectiever dan het verplichten van medewerkers om bedrijfshulpverlener te worden! Wees je bewust van het feit dat sommige mensen hier ook niet voor "ingericht" zijn.

6. **Houd het bedrijfsnoodplan to the point en overzichtelijk**
   Het Bedrijfsnoodplan is (onder meer) gebaseerd op de uitkomsten van de RI&E en gaat in op de risico's en genomen beheersmaatregelen. Het is goed als je beleid gemaakt hebt, maar je moet zorgen dat het daadwerkelijk gaat functioneren. Niemand gaat 150 bladzijden lezen dus je moet zorgen dat het meteen duidelijk is voor iedereen. Werk instructies uit in korte taakkaarten!

7. **Oefening baart kunst**
   Er zijn verschillende soorten oefeningen die je kunt uitvoeren. Je kunt alleen de BHV-organisatie trainen, 'droog' oefenen of oefenen met aanwezigen en eventuele hulporganisaties. Door te oefenen krijgen jij en jouw team niet alleen betere vaardigheden, maar krijg je ook beter zicht op de doorlooptijd. Staat iedereen nu wel binnen een kwartier buiten?

8. **Denk ook aan de taken na de ontruiming**
   Zorg voor nazorg van de medewerkers en BHV'ers nadat zich een incident heeft voorgedaan. Je weet niet wat iemand bijvoorbeeld eerder heeft meegemaakt (trauma).

9. **Tot slot: gebruik van social media**
   De huidige tijd veroorzaakt dat een deel van de aanwezigen het uitermate belangrijk vinden dat zij incidenten vastleggen op social media. De drang tot publiceren is soms krachtiger als het bewustzijn van gevaar! Geef als BHV'er strakke instructies en stuur mensen naar buiten!

Wie is er verantwoordelijk voor de veiligheid in jouw organisatie? IEDEREEN!

Ken je dat? Jij bent als QHSE/HSE/Safety manager verantwoordelijk voor de veiligheid binnen jouw organisatie. Is er iets te doen op het gebied van veiligheid? Ze komen naar jou! Dit zou echter niet het geval moeten zijn want je bent gezamenlijk verantwoordelijk voor de veiligheid in jullie organisatie. Loop jij ook tegen de volgende vraagstukken aan:

- Hoe overtuig je mensen die al jarenlang op een bepaalde manier werken?
- Hoe zorg je voor urgentiebesef bij zowel MT als medewerkers?
- Hoe vergroot je het veiligheidsbewustzijn in jouw organisatie?

Verbeter het veiligheidsbewustzijn

Ga de dialoog aan met jouw medewerkers zodat jullie elkaar beter begrijpen. Als jij beter begrijpt waar jouw medewerker tegenaan loopt, dan kun jij hem beter helpen om veilig te werken. Als de medewerker begrijpt wat de consequenties zijn van zijn/haar gedrag, dan zal hij/zij hier bewuster mee omgaan.

Vergroot kennis

Geef jouw medewerkers op creatieve wijze informatie over veilig werken en het gedrag dat daarbij hoort. Dit kun je bijvoorbeeld doen door informatie op het intranet of in de kantine te plaatsen. Daarnaast is het belangrijk om trainingen en workshops over veilig werken te faciliteren zodat medewerkers het gedrag van zichzelf en van elkaar gaan herkennen. Tenslotte is het belangrijk om de informatie te herhalen zodat mensen het daadwerkelijk gaan leren.

Van onbewust onbekwaam naar onbewust bekwaam

Medewerkers starten vaak met onbewust met onbekwaam veilig gedrag; zonder dat zij er erg in hebben, werken zij onveilig. Door het vergroten van de kennis en vaardigheden over veilig werken, gaan zij zich vanzelf bewust bekwamer gedragen. Met als uiteindelijke doel; onbewust bekwaam werken. Dit betekent dat jouw medewerkers door het herhalen van de kennis en vaardigheden onbewust veilig werken en anderen hiermee motiveren.

Veiligheidscultuur

Medewerkers werken vaak al jarenlang op een bepaalde manier. Dit doen zij vaak in team verband en vanuit de normen en waarden die het bedrijf uitdraagt. Dit uit zich bijvoorbeeld in processen, systemen en gedrag van MT en werknemers. Het is belangrijk dat je een veiligheidscultuur creëert waarbij het toegestaan is om fouten te maken en deze fouten ook gemeld worden (zonder dat een medewerker daarop wordt afgestraft).

Digitale veiligheid slimme consumentenapparaten niet op orde

Agentschap Telecom liet 22 veelgebruikte apparaten onderzoeken in de categorieën: routers, slim speelgoed, IP-camera's, slimme sloten, babyfoons en slimme thermostaten. Zeventien van de 22 apparaten scoorden matig tot zeer slecht op het gebied van basisveiligheid en privacyaspecten. In totaal vijf onderzochte apparaten zijn relatief veilig: bij de thermosstaat *Nest Learning V3* en de babyfoon *Alecto IVM-100* troffen de onderzoekers zelfs geen beveiligingsproblemen aan. Fabrikanten en leveranciers van onveilige apparaten zijn op de hoogte gesteld. Dit heeft in een aantal gevallen al geleid tot aanpassingen van de producten.

Frank van Summeren, adviseur veiligheid bij RONT Management Consultants

Consumenten beter beschermen tegen cyberaanvallen
Angeline van Dijk, directeur-hoofdinspecteur van Agentschap Telecom: "Het is zorgelijk dat de digitale veiligheid bij de meeste van de onderzochte slimme apparaten niet op orde is. Dit zijn producten die bij veel consumenten in huis staan. Wie vermoedt dat ze onveilig zijn kan dit aangeven bij Agentschap Telecom. Gelukkig laat het onderzoek ook zien dat goede beveiliging door fabrikanten wel mogelijk is. Als toezichthouder pleit ik voor aanvullende Europese regels om consumenten beter te beschermen tegen cyberaanvallen."

Producten moeten veilig en betrouwbaar zijn
Staatssecretaris Mona Keijzer (EZK): "Om ondernemers en consumenten optimaal van het *Internet of Things* te kunnen laten profiteren, is het essentieel dat deze producten veilig zijn en vertrouwd kunnen worden gebruikt. Ook dit onderzoek toont weer aan dat dit niet vanzelf gaat. Vooruitlopend op Europese en internationale regels, nemen we daarom nu al zelf maatregelen. Zo worden in opdracht van mijn ministerie metingen verricht naar onveilige en al gehackte IoT-apparaten in Nederland en start nog dit jaar een overheidscampagne om consumenten voor te lichten."

Apparaten maken gebruik van onveilige verbindingen en instellingen
Veel apparaten maken gebruik van slecht beveiligde verbindingen en standaardinstellingen die niet veilig zijn. Het uitvoeren van een update is vaak omslachtig. Hierdoor zijn persoonlijke gegevens of zelfs wachtwoorden te bekijken en kan de besturing worden overgenomen. Dat maakt apparaten kwetsbaar voor infecties en ongewenste toegang. De resultaten van het onderzoek benadrukken het belang van de maatregelen zoals gesteld in de *Roadmap Digitaal Veilige Hard- en Software* die staatssecretaris Keijzer vorig jaar heeft gepubliceerd. Deze maatregelen moeten leiden naar een aanzienlijke verbetering van de digitale veiligheid van slimme apparaten. Bijvoorbeeld door het streven naar het stellen van minimum veiligheidseisen via het Europese *Radio Equipment Directive.*

Gebruik IoT-apparatuur, maar doe het bewust

Gebruikers van IoT-apparatuur kunnen zelf veel doen om hun apparatuur minder kwetsbaar te maken voor ongewenste toegang en cyberaanvallen. In het rapport staat een aantal tips: voer regelmatig updates uit, kies een sterk wachtwoord, deel zo min mogelijk informatie met het apparaat en koppel het apparaat niet onnodig aan een netwerk. Veel apparaten hoeven voor gebruik niet online te zijn.

Veiligheid is mensenwerk

‘Het is gewoon niet sexy, praten over veilig werken. Veiligheid wordt voornamelijk beleefd als het opvolgen van regels en procedures en o wee als je deze niet volgt, dat zwaait er wat! Terwijl veiligheid begint en eindigt met de factor mens’, zegt Gert-Jan Kamps, Human Factors Engineer. ‘Mensen maken veiligheid, niet die dikke handboeken met regels en procedures die toch niemand leest.’

Gert-Jan Kamps is werkzaam bij Intergo en heeft onlangs een interview gegeven in OK Visie over dit onderwerp.

De OK is een werkomgeving waar potentiele gevaren op de loer liggen. Er wordt gewerkt in een complexe omgeving in vaak suboptimale omstandigheden. We werken met formaldehyde, anesthesiegassen en staan urenlang op onze benen. Dit soms midden in de nacht, in een dienst waarin we al uren bezig zijn geweest, en de vermoeidheid onverbiddelijk toeslaat. ‘En in deze omstandigheden is een ‘foutje’ snel gemaakt. Veelal onbedoeld en onbewust. Dan kunnen we wel met een beschuldigende vinger naar OK-medewerker gaan wijzen, maar dat verandert niets wezenlijk aan de situatie waarin deze persoon moet werken. Begin daarom met het veranderen van de omstandigheden waarin we onze mensen laten werken.”

Gert-Jan gaat verder: ‘De mens speelt een dominante rol bij kwaliteit en veiligheid. Ongeveer 80 procent van de incidenten op de werkvloer is gelieerd aan wat we veelal een menselijke fout noemen, daarom is specifieke kennis van hoe een mens functioneert essentieel. Overigens is de mens in net zo veel gevallen ook betrokken bij succes, maar daar hoor je niemand over. Deze specifieke kennis over menselijk succes en soms dus ook falen, is geborgd binnen het Human Factors vakgebied.

Human Factors
Human Factors staat in de volksmond beter bekend als ergonomie. De Nederlandse Vereniging voor Ergonomie hanteert de volgende definitie voor ergonomie: “Ergonomie streeft naar het zodanig ontwerpen van gebruiksvoorwerpen, technische systemen en taken dat de veiligheid, de gezondheid, het comfort en het doeltreffend functioneren van mensen wordt bevorderd.”

‘Onze dagelijkse werkomgeving heeft nogal wat invloed op onze werkprestaties. En mensen maken fouten, omdat ze moeten werken in een suboptimale omgeving. Dus die omgeving moet aangepast worden, zodat deze minder ‘fout-uitlokkend’ is. De mens moet werken met de imperfectie van het werksysteem, wat heel veel tijd en energie kost. In een ideale situatie moet de omgeving aansluiten bij een persoon in plaats van andersom. Neem het voorbeeld van een auto, vervolgt Gert-Jan. “`Ik kan in iedere willekeurige auto stappen en zo wegrijden. Het gaspedaal zit namelijk altijd rechts en het rempedaal in het midden. Waarom zou elk anesthesietoestel of OK dan anders bediend of ingericht moeten worden? Dat lokt alleen maar fouten uit, zeker als we steeds meer personeel gaan uitruilen in deze arbeidsmarkt.’

Waan van de dag & gewoontes

Om veilig te kunnen werken ligt een grote rol voor het management weggelegd. Mensen zijn complex, maar werken wel via voorspelbare wetmatigheden. Bij managers wil het weleens schorten aan inzicht in deze wetmatigheden. Er is al veel bekend over onder welke omstandigheden mensen het beste kunnen werken. Het is de taak van de manager om deze omstandigheden optimaal in te richten. Helaas wordt de manager zelf ook vaak opgeslokt door de waan van de dag en komt deze helemaal niet aan toe aan het analyseren van het proces dat hij aan het managen is. Ook als operatieassistent of anesthesiemedewerker word je vaak zo meegesleurd in de waan van de dag, dat er geen tijd is om stil te staan bij de mogelijke risico's die we lopen. Dit is een bekend fenomeen binnen de psychologie, op een gegeven moment zien we risico's niet meer en gaan we ze tolereren.

Maar het begint natuurlijk met de vraag wiens verantwoordelijk dit eigenlijk is. Te vaak wordt deze bij de persoon op de OK gelegd. Iedereen herkent wel die stressvolle momenten, situaties waarin je eigenlijk met te weinig personeel bent, voorbereidend werk wat niet goed is gedaan, je te weinig gegeten hebt en ook nog eens naar het toilet moet terwijl je aan tafel staat. Ja, dan kan het gebeuren dat er een keer een snauw uitgedeeld of verkeerde informatie gedeeld wordt. We spreken dan al snel van een 'cultuurprobleem'. 'Onterecht', vindt Gert-Jan. 'Cultuur is ontzettend belangrijk, maar wordt mijns inziens te snel gebruikt als een soort magische verklaring voor alles wat fout gaat. Tegelijkertijd wordt het ook gepresenteerd als Het Grote Antwoord wat alle problemen gaat oplossen. Alsof er een soort dark side binnen de organisatie is waarin mensen bewust een duistere organisatiecultuur aanhangen. Maar niemand gaat vol enthousiasme naar zijn werk om de boel eens even lekker te verkloten. Iedereen doet zijn stinkende best vol passie en overgave onder mentaal en fysiek zware omstandigheden, en dan gaan we naar deze mensen wijzen dat hun houding en gedrag fout is. We moeten dan juist die mentale en fysieke zware omstandigheden aanpakken.'

'Wat natuurlijk wel zo is', nuanceert Gert-Jan, 'is dat je bepaald gedrag mag verwachten op de werkvloer nadat de basis op orde is. Creëer de randvoorwaarden en faciliteer het gedrag, sleutel eerst aan de omgeving en daarna pas aan de factor mens.' Soms is die basis er wel, en toch handelen we er niet altijd naar. 'Dit ligt vaak aan de sociale norm die er op een afdeling heerst. Wanneer niemand op de afdeling een spatbril draagt tijdens een operatie, ben jij ook geneigd dit niet te doen. Je wilt immers niet opvallen of uit de boot vallen. Ook wordt er op een operatiekamer veel te weinig gezeten, terwijl je weet (en voelt) dat langdurig staan niet goed voor je is. Maar zitten wordt vaak geassocieerd met luiheid en zo willen we natuurlijk niet overkomen. Mensen zijn nu eenmaal kuddedieren en vertonen graag gewenst gedrag, óf gedrag waarvan ze denken dat het gewenst is.'

Daar komt het fenomeen van psychologische veiligheid bij kijken. Voel ik me veilig om iets te benoemen en wordt er ook naar gehandeld? Dus voel jij je op jouw afdeling veilig genoeg om een chirurg aan te spreken die zijn smoeltje nog draagt op de gang of durf je te vragen of hij of zij de rookafzuig wil gebruiken? 'Overigens kan hij of zij een hele goede reden hebben om de rookafzuig niet te gebruiken, bijvoorbeeld omdat het ding te veel lawaai maakt en het de chirurg uit de concentratie haalt. Het is dan beter om te werken aan geluidsreducerende maatregelen in plaats van een 'teamtraining' te doen. Onveilig gedrag heeft altijd een reden, een veilige organisatie onderzoekt deze en stuurt op deze oorzaken in plaats van instrueren dat mens zich anders moet gedragen.'

Personeelstekorten

Over de vraag hoe hij als human factors engineer tegen de huidige personeelstekorten aankijkt, moet Gert-Jan even nadenken. "Je kan grofweg aan 2 knoppen draaien, vraag en aanbod. Ik zou beginnen met kijken in hoeverre er nog winst te behalen valt aan de vraag kant, in het efficiënter inrichten van onze processen, waardoor de behoefte aan personeel af zou kunnen nemen. Deze stap wordt vaak overgeslagen, maar blijft de moeite waard om ernaar te kijken. Ik ben van mening dat er in tijden van krapte goed nagedacht moet worden over oplossingen. Zo zie je nu dat er op operatieafdelingen andere disciplines dan operatieassistenten worden ingezet om hun werkzaamheden over te nemen. Dit is natuurlijk verre van ideaal, maar op zich hoeft dat geen direct gevaar te vormen. Laat ik vooropstellen dat dit geen structurele oplossing voor het personeelstekort moet worden, maar in deze situatie, waarin er geen blik operatieassistenten opengetrokken kan worden, moet er creatief nagedacht worden.'

Gert-Jan vervolgt: 'Wanneer de juiste competenties aanwezig zijn en alle taken voor iedereen duidelijk en afgebakend zijn, zou dit mogelijk moeten zijn. Maar wat hierbij heel belangrijk is, is het nadenken over noodscenario's. En daarnaast moeten er duidelijke beslisregels komen. Wie doet wat in het geval van een complicatie of calamiteit? Zijn alle processen ook dan goed ingericht? Ook hierin is weer een duidelijke rol voor het management weggelegd. Zij moeten analyseren en onderbouwen wat wel en niet kan en in welke situatie, uiteraard met input van de werkvloer.'

PRI

Wanneer er gekozen wordt voor een degelijke oplossing, zou het beste zijn om eerst een prospectieve risico-inventarisatie te maken. Bij een PRI gaat het om de vraag; wat kan er misgaan? Je denkt dus vooraf na over de risico's met betrekking tot patiëntveiligheid. Dit in tegenstelling tot een VIM-melding, daarbij wordt geanalyseerd wat er mis is gegaan.
'Die PRI's zijn wel een soort moetje geworden hoor', lacht Gert-Jan. Veel instellingen doen het wel, maar dan verdwijnt het in een la en handelen er niet altijd naar.

Op het moment dat er bijvoorbeeld blijkt dat een medisch apparaat een potentieel risico met zich meebrengt, moet op zoek gegaan worden naar alternatieven of contact gezocht worden met de leverancier. Maar het traject wat daarvoor afgelegd moet worden, blijkt toch te veel tijd, en misschien ook wel moeite, te kosten. De urgentie zakt dan ook weg. Het is een tijdrovend en arbeidsintensief proces. De afdeling inkoop moet op zoek naar alternatieven, dit moet aanpast worden in het systeem, personeel moet ingewerkt worden et cetera. Het sleutelwoord hierbij is verbetertijd. Er moet verbetertijd ingepland worden om mensen aan nieuwe situaties te laten wennen en er mee te leren werken. En laat het aan tijd nu net vaak ontbreken op een OK, terwijl je op de lange termijn veel beter af bent'

Nog even terug naar die potentiele gevaren die er op een OK heersen. De fysieke gevaren kunnen we waarschijnlijk allemaal wel benoemen. Een slechte werkhouding, repetitieve bewegingen, langdurig staan, noem het maar op. Maar een ergonoom kijkt niet alleen naar de invloed van onze werkomgeving op ons fysieke welbevinden, maar ook naar mentale, psychische en cognitieve processen bij werkende mensen. En ook hierbij zit het gevaar in een klein hoekje.

'Op een OK werken veel verschillende disciplines samen in een kleine ruimte, met één gezamenlijk doel; de zorg voor de patiënt. Deze verschillende disciplines werken veelal in een wisselende samenstelling, vrijwel iedere dag sta je met andere collega's ingedeeld. Dit terwijl een teamgevoel enorm belangrijk is. Het weten wat je aan elkaar hebt en wat je van elkaar kunt verwachten. Ik realiseer me dat het plan-technisch niet altijd te realiseren is, maar vanuit ergonomisch oogpunt is het werken in dedicated en vaste teams een aanbeveling.

Vermoeidheid, ook zo'n ding. De diensttijdenregeling is een hot topic onder ok-personeel en terecht. Voldoende slaapuren na een dienst zijn gewoon een must. Meerdere studies hebben het effect van vermoeidheid op de kwaliteit van zorg onderzocht en een relatie laten zien tussen vermindering van performance en het maken van medische fouten. Hier moeten we uiteraard voor waken en ook hierin ligt een taak bij het management. De kennis over hoe dit aan te pakken is er al wel, maar onvoldoende ingebed in de bedrijfsvoering.

Brandweer waarschuwt over brandveiligheid bij hoogbouw

Onlangs verscheen in een interview met het AD dat de brandweer zich grote zorgen om de brandveiligheid van hoogbouw. Esther Lieben werd hierover geïnterviewd en zij is brandweercommandant en landelijk portefeuillehouder incidentbestrijding bij de brandweer. Zij geeft aan dat de brandweer zich zorgen maakt om de forse toename van hoogbouwprojecten, doordat de veiligheid te vaak 'onderaan' de prioriteitenlijst staat.

Hoogbouw
In de gehele Randstad worden op dit moment hoge torens gebouwd die de 100 meter ruimschoots overschrijden. Hoogwerkers komen tot 30 meter hoogte. Daarboven kan de brandweer de brand alleen van binnenuit bestrijden. Ze geeft in het AD aan dat als een toren helemaal in brand vliegt, zij niemand meer kunnen komen redden. Bewoners overleven een dergelijke brand alleen als er vooraf is nagedacht over vluchtroutes, brandwerend materiaal, scheidingswanden en interne blusinstallaties. Volgens Lieben moet zo'n 10% van de bouwkosten gereserveerd worden voor brandveilig bouwen. Daarnaast pleit ze voor het gebruik van betere bouwmaterialen.

Brandgevaarlijke panden
Een voorbeeld waar het volledig mis ging, was de brand in de Grenfell tower inLonden. Na de brand in de Grenfell tower was er grote ophef in binnen en buitenland over brandgevaarlijke gevelplaten. Deze platen zijn er veelal nog, maar de ophef is inmiddels weer weg. Onlangs presenteerde de gemeente Nijmegen de resultaten van een inventarisatie van panden met gevelbeplating waarvan de brandveiligheid mogelijk in het geding is. Dit blijken er maar liefst 62 te zijn.

Minister Ollongren gaf gemeenten vorig jaar nog de opdracht om een inventarisatie van mogelijke risicopanden in hun stad te maken. Naar verwachting wordt dit overzicht binnen enkele maanden gepresenteerd.

3 Tips om jouw gebouw te beveiligen tijdens vakanties

Miljoenen Nederlanders gaan ieder jaar op vakantie. Scholen sluiten, kantoorgebouwen gaan dicht en bedrijventerreinen liggen er verlaten bij. Juist in rustige vakantieperiodes is de beveiliging en veiligheid van jouw gebouw belangrijker dan ooit!

In meer dan 100 gemeenten stijgt het aantal inbraken in de zomermaanden. Inbrekers houden een gebouw vaak langere tijd in de gaten. Ze plaatsen bijvoorbeeld een steen op de parkeerplaats of leggen een takje voor de deur. Als dit er na een aantal dagen nog ligt, weten zij dat er niemand is langs geweest.

Beveiliging tijdens de zomervakantie
Met de volgende simpele tips zorg je ervoor dat de kans op inbraak afneemt;

1. Beveiliging

Zorg voor goede beveiliging van het pand. Dit kan in de vorm van een alarm, camerasystemen, het inschakelen van beveiligers of zorg dragen voor goed hang- en sluitwerk. Maak vooral zichtbaar welke vorm van beveiliging je gebruikt want dit schrikt inbrekers af. Je kunt dit bijvoorbeeld kenbaar maken met stickers op de deur.

2. Sluit ramen en deuren

Het lijkt zo voor de hand liggend om voor de zomerstop alle ramen en deuren van het kantoorpand te sluiten, maar het gebeurd maar al te vaak dat een collega van een andere verdieping verwacht dat jij de ramen op jouw kantoor dichtdoet, terwijl jij had verwacht dat jouw collega nog een laatste ronde door het pand zou maken om alles te sluiten. Maak hierover dus goede afspraken en zorg dat iemand altijd dubbelcheckt of alles goed afgesloten is.

3. Verzorgde indruk

Zoals je ervoor zorgt dat jouw huis bewoont lijkt als je op vakantie bent, moet ook jouw bedrijfspand een verzorgde indruk hebben. Houd het struikgewas rondom het gebouw kort en laag zodat het pand (en dus ook de inbreker) vanaf de openbare weg goed zichtbaar is.

Business continuity management; een hype, een mythe of een lifechanger?

Je kunt op dit moment niemand spreken binnen de veiligheidssector of er wordt gesproken over het weerbaar maken van je organisatie en het zorgdragen voor business continuity management. In deze blog beantwoorden wij de vraag of het een hype, een mythe of een lifechanger is voor een organisatie.

Wat is business continuity management?
Business continuity management is het proces dat potentiele gevaren en de gevolgen hiervan identificeert zodat de bedrijfsvoering in geval van een incident niet verstoort wordt. Er zijn tal van incidenten die de continuïteit van de bedrijfsvoering kunnen verstoren. Enkele voorbeelden; Staking van het personeel, Cyberaanval, Noodweer, Stroomuitval, Brand

Maar hoe zinvol is het om je voor te bereiden op iets wat waarschijnlijk nooit gebeurd?
Zonder een goede voorbereiding en respons kan een incident ervoor zorgen dat jouw organisatie niet verder kan functioneren en dat de continuïteit van de bedrijfsvoering in gevaar is. Business continuity is van belang voor diverse stakeholders;

- Supply chain: als leverancier moet je te allen tijde kunnen leveren omdat anders de andere organisaties in de keten ook in de problemen komen. Je wilt geen imagoschade bij jouw partners oplopen *('Met die leverancier werken we niet meer want hij komt zijn afspraken niet na')* en in contracten zijn vaak boeteclausules opgenomen dus je kunt ook nog financiële schade hebben.
- Verzekeraar: jouw verzekeraar wil graag weten hoe jij reageert als er een incident zich voordoet. Hier worden de premies op aangepast; ten gunste of niet ten gunste van jou.
- Werknemers: door de krapte op de arbeidsmarkt is het moeilijk om goed personeel te vinden en te behouden. Werknemers zijn veeleisender dan een aantal jaar geleden en willen zekerheid over hun loopbaan. Deze zekerheid kun jij hen bieden door business continuity management goed in te richten en risico's te minimaliseren.
- Overheid: risicovolle bedrijven zoals BRZO bedrijven wordt steeds striktere wetgeving opgelegd door de overheid. Om aan deze strenge wet- en regelgeving te voldoen is het belangrijk om te weten waar jouw risico's liggen en hoe je hierop kunt anticiperen.

Business continuity management: een lifechanger!
Risico's die de continuïteit van jouw organisatie bedreigen nemen exponentieel in omvang toe (denk aan lekken van informatie en cybercrime). Daarnaast hebben ook politieke besluitvorming, snel veranderende omstandigheden in de markt en klantgedrag hier invloed op. Het inrichten van business continuity management is een lifechanger want de continuïteit van jouw bedrijfsvoering is niet alleen voor jezelf belangrijk, maar vooral voor de andere stakeholders zoals werknemers, klanten, leveranciers en de overheid.

Zijn uw medewerkers het grootste gevaar voor digitale veiligheid?

Er zijn tussen oktober 2017 en juli 2018 ruim 429 veiligheidsincidenten bij gemeenten gemeld bij de Informatiebeveiligingsdienst (IBD), dat meldt het IBD in een rapport aan de VNG. De IBD is een gezamenlijk initiatief van alle Nederlandse Gemeenten en richt zich op ondersteuning op het gebied van informatiebeveiliging.

Onbewuste medewerkers
Uit het onderzoek blijkt dat 49% van de incidenten door onbewuste medewerkers zijn ontstaan. Medewerkers zijn zich onvoldoende bewust van de gevolgen van een kleine menselijke fout. Het rapport Dreigingsbeeld Informatiebeveiliging Nederlandse Gemeenten 2019/2020 biedt een handvat om de informatiebeveiliging verder te verbeteren en daarmee de digitale weerbaarheid van gemeenten te verhogen.

Prioriteiten om informatiebeveiliging te verbeteren
Om de belangrijkste risico's te beheersen is het noodzakelijk om een combinatie van technische en organisatorische maatregelen op te stellen. De prioriteiten volgens dit rapport zijn:

- Informatiebeveiliging op de politieke agenda: wanneer de top van de organisatie het belang van informatiebeveiliging uitstraalt, wordt het bewustzijn onder medewerkers vergroot en ontstaat er een cultuur met voldoende aandacht voor informatiebeveiliging.
- De basis op orde: om de digitale weerbaarheid van gemeenten te verhogen moeten processen op orde zijn en bij de juiste verantwoordelijke medewerker belegt zijn
- Versterk de menselijke schakel: door medewerkers de mogelijkheid te geven om veilig te werken en zich bewust te zijn van de risico's want bewuste medewerkers zijn de beste beveiligingsmaatregel
- Versterk de Chief Information Security Officer (CISO): door hem/haar strategisch en onafhankelijk te positioneren en de juiste middelen te geven zodat hij de organisatie optimaal kan inrichten en weerbaar kan maken
- Inzicht in technologieën: nieuwe technologische ontwikkelingen gaan super snel en zorgen voor nieuwe kwetsbaarheden en risico's dus het is belangrijk om de juiste medewerkers hiervoor verantwoordelijk te stellen zodat zij vroegtijdig kunnen inspelen op de kwetsbaarheden en risico's.

Hoe kunnen we voorkomen dat een politierapport over lekken gelekt wordt?

Begin januari stonden de kranten er vol mee; een vertrouwelijk rapport over een onderzoek naar het lekken door agenten is gelekt aan De Telegraaf.

Een derde van de zaken is daadwerkelijk gelekt
N.a.v. politiemol Mark M, die vijf jaar cel kreeg vanwege het lekken van vertrouwelijke informatie aan criminelen, is het onderzoek naar lekken bij de politie gestart. Er zijn 761 dossiers doorgenomen. Bij een steekproef van 20% van de dossiers bleek dat bij een derde van de zaken daadwerkelijk gelekt was.

Onoplettendheid van de agent grootste oorzaak
Uit het onderzoek blijkt dat in zeer beperkte gevallen een crimineel het initiatief heeft genomen om informatie van een agent te ontvangen. In de meeste gevallen ontstaat het lekken van vertrouwelijke politie-informatie vaak door onoplettendheid van een agent zelf.

Lekkende agenten halen bijvoorbeeld informatie uit systemen voor zichzelf of een familielid. Er wordt bijvoorbeeld gecheckt of het nieuwe vriendje van zijn/haar dochter geen boef is. Het typische profiel van de lekkende agent is volgens de Telegraaf een autochtone man, tussen de 20 en 30 jaar, die maximaal 10 jaar in dienst is. Onachtzaamheid, bezorgdheid en eigenrichting zijn de belangrijkste drijfveren om te lekken.

Hoe heeft het rapport nu kunnen lekken?
Na het ontdekken van het lek, heeft de politie besloten om de belangrijkste conclusies uit het rapport alsnog zelf te publiceren. Hoe het rapport heeft kunnen lekken wordt volgens de politie nog onderzocht.

Kijkend naar het onderzoek, blijkt dat bij 71 van de 161 onderzoeken niet duidelijk is wie lekte en wat de drijfveren van deze betrokken medewerker waren. Zouden we dus ooit te weten komen wie het rapport gelekt heeft en waarom deze persoon dit gedaan heeft…? De belangrijkste vraag is dan ook niet hoe het rapport heeft kunnen lekken, maar hoe dit in de toekomst voorkomen kan worden.

Informatiebeveiliging en IT beheer bij rijksoverheid nog steeds niet op orde: en nu?

De rekenkamer publiceerde afgelopen week een artikel dat de Rijksoverheid haar informatiebeveiliging nog steeds niet op orde heeft. Digitale verstoring is op dit moment een van de grootste bedreigingen voor onze nationale veiligheid. Bij 11 organisaties van de rijksoverheid signaleert de Algemene Rekenkamer grote problemen in de informatiebeveiliging. De organisaties hebben niet alle beveiligingsmaatregelen genomen die door en voor de rijksoverheid verplicht zijn gesteld.

Verouderde systemen
Uit het onderzoek blijkt dat circa 25% van de rijksuitgaven aan ICT betrekking hebben op vernieuwing. De overige 75% wordt besteed aan de instandhouding van de huidige ICT maar dit is buiten beeld. Hierdoor is het voor het parlement onduidelijk hoeveel systemen verouderd zijn en op termijn problemen kunnen opleveren in de dienstverlening aan bedrijven en burgers. Het is dus niet te controleren of de continuïteit van de dienstverlening is gewaarborgd. Binnen de belastingdienst worden verouderde ICT-systemen bijvoorbeeld wel vernieuwd, maar dit gaat niet snel genoeg.

Gebrek aan professionals
Het percentage studenten dat ICT studeert is vele malen lager dan de verwachte behoefte. Zij krijgen vaak aantrekkelijke aanbiedingen van Google, Facebook of startups of zij gaan zelf als ZZP-er aan de slag vanwege het grote aanbod aan opdrachten dat zij krijgen. Het tekort aan de juiste professionals is dus erg groot.

Geef je huidige personeel nieuwe kansen
Een grote kans ligt in het omscholen van huidig personeel met een business achtergrond naar IT gerelateerde thema's. Het intern invullen van ICT functies biedt organisaties namelijk een aantal kansen:

- Op een efficiënte manier capaciteit opbouwen omdat je gebruik maakt van jouw eigen mensen zodat je verouderde systemen kunt vernieuwen
- Je bent als organisatie minder afhankelijk van krapte op de arbeidsmarkt
- Huidige werknemers krijgen nieuwe kansen voor persoonlijke ontwikkeling, wat leidt tot een hogere werknemerstevredenheid.

Het om- en bijscholen van huidig personeel kan op een gemakkelijke manier met kortdurende opleidingen van professionals voor professionals.

Ontwrichting van de maatschappij ligt op de loer

De digitale dreiging voor de nationale veiligheid is permanent. Vrijwel alle vitale processen en systemen in Nederland zijn deels of volledig gedigitaliseerd waarbij er nauwelijks terugvalopties of analoge alternatieven zijn. Deze factoren gecombineerd met het achterblijven van de weerbaarheid, maken Nederland kwetsbaar voor digitale aanvallen.

De effecten van de forse investeringen van zowel overheid als bedrijfsleven, de nieuwe meldplicht cybersecurity en strengere wet- en regelgeving zullen de komende jaren zichtbaar moeten worden. Dit blijkt uit het Cybersecuritybeeld Nederland (CSBN) 2019 van de Nationaal Coördinator Terrorismebestrijding en Veiligheid (NCTV).

Landen vormen blijvende dreiging
De grootste digitale dreiging voor de nationale veiligheid gaat uit van landen zoals China, Iran en Rusland, in de vorm van spionage, verstoring en sabotage. Dat blijkt ook uit de afgelopen jaarverslagen van de diensten. Verreweg de grootste dreiging van economische spionage komt uit China. Voor Rusland is ons land een interessant doelwit van spionage vanwege onder andere MH17. Nederland is afhankelijk van een beperkt aantal aanbieders en landen, dit maakt ons kwetsbaar voor hun (veranderende) intenties. Zo wordt het overgrote deel van de hard- en software ontworpen dan wel geproduceerd in China en de Verenigde Staten. Ook kunnen andere landen bepaalde wetgeving hanteren die afwijken van onze privacy-eisen of leiden tot het verkrijgen van toegang tot data van Nederlandse gebruikers of bedrijven. Daarnaast blijft de dreiging van cybercriminaliteit onverminderd. Doordat aanvalsmiddelen laagdrempelig beschikbaar zijn en er weinig kennis nodig is om een cyberaanval uit te voeren, is de verwachting dat dit de komende jaren een probleem zal blijven.

Analoge alternatieven en terugvalopties ontbreken
De vrijwel volledige afhankelijkheid van digitalisering heeft digitale veiligheid essentieel gemaakt voor het functioneren van onze maatschappij en economie. Een incident in een netwerk kan leiden tot een keten van incidenten en uiteindelijk uitval van bijvoorbeeld gas, water of elektra. Door het bijna volledig verdwijnen van analoge alternatieven en de afwezigheid van terugvalopties is de afhankelijkheid zo groot geworden dat aantasting kan leiden tot maatschappij ontwrichtende schade. Dit hoeft niet altijd het gevolg te zijn van een cyberaanval, een simpele fout kan al forse gevolgen hebben.

Weerbaarheid nog altijd niet op orde
Weerbaarheid is het belangrijkste instrument om risico's te verminderen, aangezien het beïnvloeden van dreiging en afhankelijkheid te complex is. Organisaties worden nog steeds succesvol aangevallen met eenvoudige methoden. Incidenten hadden voorkomen kunnen worden en schade had beperkter kunnen zijn door het nemen van basismaatregelen. De komende jaren zal het een uitdaging blijven om de weerbaarheid dusdanig op peil te houden, dat we de toenemende afhankelijkheid en veranderende dreiging het hoofd kunnen bieden.

Nieuwe campagne roept mensen op zich beter te beschermen tegen internetcriminaliteit

Overheid en bedrijfsleven bundelen krachten: meer dan 20 partijen tekenen convenant ‘Preventie cybercriminaliteit’.

Internetcriminelen worden slimmer. Daardoor is het steeds lastiger te herkennen als zij een nepbericht gebruiken om persoonlijke gegevens van mensen te misbruiken of om geld afhandig te maken. Tijdens de Landelijke Veiligheidsdag in Almere trapte minister Grapperhaus (Justitie en Veiligheid) de publiekscampagne ‘Eerst checken, dan klikken’ af. De campagne roept mensen op zich beter te beschermen tegen phishing en andere vormen van internetcriminaliteit. Ook tekenden minister Grapperhaus, staatssecretaris Keijzer (EZK) en een groot aantal bedrijven en brancheorganisaties het convenant ‘Preventie cybercriminaliteit’. Zij trekken samen op in de strijd tegen internetcriminaliteit.

Alerter online
Uit politiecijfers blijkt dat traditionele criminaliteit zoals overvallen, woninginbraken en geweldsmisdrijven daalt. Dit geldt echter niet voor internetcriminaliteit. In 2017 was 1 op de 9 mensen slachtoffer, berekende het CBS. Het kabinet investeert daarom fors om internetcriminelen op te sporen. Dat is echter niet voldoende. Omdat internetcriminelen steeds handiger worden om toegang te krijgen tot computers, tablets en smartphones, is het belangrijk dat mensen zelf ook alerter online worden. De nieuwe campagne roept mensen daarom op eerst te checken of een link, bijlage of betaalverzoek in een e-mail, sms of appje te vertrouwen is en pas te klikken als ze daar zeker van zijn.

Taboe op slachtofferschap
“We moeten af van het taboe op slachtofferschap van phishing. Het kan iedereen gebeuren, het is niets om je voor te schamen. Iedereen heeft er last van, dus we moeten iets doen. Allemaal. Wees daarom voorzichtig wanneer u op een link, bijlage of betaalverzoek klikt. Voordat u het weet, geeft u internetcriminelen toegang tot uw digitale leven. Want de internetcriminelen worden steeds handiger in het namaken van mailtjes, sms’jes en appjes. Die alertheid moet een gewoonte worden, net zoals het op slot doen van de deur als je van huis gaat. Dus: eerst checken, dan klikken” Aldus minister Grapperhaus.

Convenant ‘Preventie cybercriminaliteit’
Naast de Rijksoverheid zetten ook gemeenten, brancheorganisaties en bedrijven zich in om mensen beter te wapenen tegen internetcriminaliteit. Meer dan twintig partijen ondertekenden op 25 mei het convenant ‘Preventie cybercriminaliteit’. Daarin spreken zij met elkaar af zich in te zetten om mensen te stimuleren preventieve maatregelen tegen internetcriminaliteit te nemen, zoals het gebruik van een virusscanner en verschillende sterke wachtwoorden, software-updates direct uitvoeren en het regelmatig maken van back-ups. Ook zetten banken en ICT-, internet- en telecombedrijven zich in om onder hun klanten het gebruik van hun huidige en nog te ontwikkelen beveiligingsmogelijkheden te bevorderen.

Over de campagne

Met de publiekscampagne tegen internetcriminaliteit wil het ministerie van Justitie en Veiligheid mensen helpen zich beter tegen internetcriminaliteit te beschermen. De campagne is vanaf maandag 27 mei te zien op tv, online en sociale media. Een groot aantal partners uit onder andere de banken-, ICT-, internet- en telecomsector ondersteunt de publiekscampagne. Zij roepen via hun eigen kanalen mensen op zich beter te wapenen tegen internetcriminelen en delen tips hoe zij dat kunnen doen. Op www.veiliginternetten.nl staat meer informatie over de campagne.

Aanpak foute en lakse ICT-bedrijven in strijd tegen online kinderporno

Internet moet worden opgeschoond van kinderporno. Minister Grapperhaus van Justitie en Veiligheid kondigt aan de Tweede Kamer een bestuursrechtelijke aanpak aan: foute en lakse internetbedrijven die na een melding beeldmateriaal van seksueel kindermisbruik niet snel van het openbare web verwijderen riskeren straks een boete of dwangsom, die fors kunnen oplopen.

Publieke-private samenwerking
Minister Grapperhaus is aan het begin van deze kabinetsperiode direct een publiek-private samenwerking gestart om kinderporno van internet af te krijgen. Er zijn al goede afspraken met ICT-bedrijven, koepelorganisaties, politie, Openbaar Ministerie, wetenschap, het Expertisebureau Online Kindermisbruik (EOKM) en de Nationaal Rapporteur Mensenhandel en Seksueel Geweld tegen Kinderen om de handen ineen te slaan voor het opschonen van internet van kinderporno. De brancheorganisaties van hostingbedrijven en organisaties in de digitale infrastructuur hebben eind 2018 afgesproken om bij een melding van kinderpornografisch materiaal door het EOKM deze binnen 24 uur te verwijderen van hun servers.

Wetsvoorstel
Eind 2019 zal minister Grapperhaus een wetsvoorstel in consultatie doen voor de zogenoemde bestuursrechtelijke aanpak van foute en lakse bedrijven. Het wetsvoorstel zal een toezichthouder aanwijzen, die bedrijven zal aanpakken die een melding over kinderporno niet snel genoeg of zelfs helemaal niet verwerken. In de praktijk betekent dit straks dat een bedrijf een melding kan krijgen van de toezichthouder dat er kinderporno op één van zijn eigen servers staat. Dan gaat de stopwatch aan. Lukt het een bedrijf niet om binnen een opgelegd kort tijdsbestek de kinderporno te verwijderen, dan wordt een dwangsom verbeurd verklaard: het bedrijf moet een geldsom betalen. Hoe kort dat tijdsbestek precies wordt, zal nog nader worden beslist. Daarnaast kan de toezichthouder nog een boete opleggen. Die boete is omzet-afhankelijk en zal bij herhaalde overtredingen oplopen.

Niet vrijblijvend
“Stapsgewijs verbannen we kinderporno van internet. De meeste ICT-bedrijven in Nederland verwijderen kinderporno snel en accuraat, en de rest moet dat ook gaan doen. Het verwijderen van kinderporno is niet iets vrijblijvends: bedrijven moeten dit zelf snel en goed kunnen, simpelweg als onderdeel van hun eigen bedrijfsvoering. Eigenlijk hebben bedrijven die kinderporno niet snel van eigen servers kunnen verwijderen geen bestaansrecht in Nederland” aldus Grapperhaus.

Monitor

Als onderdeel van de publiek-private samenwerking van minister Grapperhaus, heeft de politie een database met 1,4 miljoen hashcodes van kinderpornografisch beeldmateriaal beschikbaar gesteld. Hashcodes zijn unieke cijfercodes die een soort digitale vingerafdruk van een plaatje vormen. Het EOKM heeft hiermee een hashcheck-server gebouwd, waarmee bedrijven een check kunnen uitvoeren, zonder dat de bijbehorende illegale afbeeldingen en informatie zichtbaar worden. Dit systeem wordt op dit moment uitgetest door diverse grote hostingbedrijven. Daarnaast bouwt de TU Delft aan een monitor die inzicht gaat geven welk bedrijf waar en hoe lang kinderpornografisch beeldmateriaal na een melding nog online heeft staan.

Kabinet zet eerste stap in bescherming telecomnetwerken en 5G

Goed, snel en veilig internet is onmisbaar in de Nederlandse economie en voor het Nederlands bedrijfsleven. De sterke positie van Nederland als digitaal koploper binnen de Europese Unie wil het kabinet behouden. Tegelijkertijd blijkt uit recente jaarverslagen van de diensten en het Cybersecuritybeeld Nederland van de NCTV de dreiging van spionage en sabotage door landen permanent aanwezig is. Deze zorgen zijn ook meer specifiek de afgelopen tijd geuit over de uitrol van 5G. Vanwege deze dreiging heeft de Taskforce Economische Veiligheid onder leiding van de NCTV een advies uitgebracht over deze problematiek. Recent stuurden minister van Justitie en Veiligheid Ferd Grapperhaus en staatssecretaris van Economische Zaken en Klimaat Mona Keijzer de voorgenomen aanpak ten aanzien van de beveiligen van het huidige en toekomstige 5G netwerk naar de Tweede Kamer.

Weerbaarheid tegen dreiging verhogen
De huidige netwerken zijn aangemerkt als vitaal proces en de continuïteit en beschikbaarheid zijn van cruciaal belang voor ons bedrijfsleven en de maatschappij. Op basis van de risicoanalyse van de Taskforce worden de telecomaanbieders verplicht om aanvullende beveiligingsmaatregelen te nemen om de weerbaarheid tegen de dreiging vanuit landen te verhogen. Een van deze maatregelen is het stellen van extra hoge eisen aan leveranciers van diensten en producten in de kritieke onderdelen van het telecomnetwerk. Op deze manier wordt de kwetsbaarheid van misbruik verder verminderd. De noodzakelijke aanscherpingen van de netwerken zullen worden vastgesteld in een Algemene Maatregel van Bestuur die dit najaar wordt gepubliceerd.

Gezamenlijke Europese aanpak
Europese samenwerking in de beveiliging van het 5G netwerk en het nemen van maatregelen is noodzakelijk. Het kabinet steunt dan ook een gezamenlijke Europese aanpak. Hierbij kan gedacht worden aan internationale wetgeving, coalitievorming of internationale ontwikkeling van normen en standaarden.

Structurele aanpak nodig
De Taskforce heeft ook vastgesteld dat een structurele aanpak nodig is omdat er continu ontwikkelingen zijn in het dreigingsbeeld en technologische ontwikkelingen razendsnel gaan binnen de telecomsector. In samenwerking met de telecomaanbieders wordt een structureel proces ingericht waarbij zoveel mogelijk rekening gehouden wordt met bedrijfseconomische aspecten, voor zover de nationale veiligheid hierdoor niet in het geding komt.

Meten van besmette IoT-apparaten verhoogt digitale veiligheid

Het aantal met internet verbonden apparaten (Internet-of-Things) groeit razendsnel. Om ondernemers en consumenten optimaal hiervan te kunnen laten profiteren, is het essentieel dat deze producten veilig zijn en vertrouwd kunnen worden gebruikt. Daarom gaan er in Nederland metingen worden verricht naar besmette IoT-apparaten. Fabrikanten van deze slimme apparaten en consumenten worden actief geïnformeerd over hoe dit op te schonen.

Dat staat in de voortgangsbrief over de Roadmap Digitaal Veilige Hard- en Software die staatssecretaris Mona Keijzer (Economische Zaken en Klimaat) recent verstuurd heeft. In de vorig jaar gepubliceerde Roadmap staan maatregelen zoals toezicht en certificering om de markt te bewegen om het veiligheidsniveau van het IoT te verhogen. Nederland neemt nu al deze maatregelen vooruitlopend op structurele Europese en internationale regels.

Samenwerking tussen overheid, bedrijven en kennisinstellingen
Staatssecretaris Mona Keijzer (EZK): “Steeds meer apparaten, naar verwachting dertig miljard in 2020, zijn verbonden met het internet. Slimme thermostaten, koelkasten, speelgoed en tv’s: ze zijn aantrekkelijk voor consumenten en bieden ondernemers extra kansen op inkomsten. Daarmee veilig omgaan, gaat niet vanzelf. Doe je dat niet, dan ben je kwetsbaar of wordt je besmette apparaat ingezet om bij anderen aan gegevens of zelfs geld te komen. Daarom gaan kennisinstellingen, bedrijven en overheid samenwerken om dit te verbeteren.”

Besmette apparaten in kaart brengen en opschonen
De TU Delft gaat met financiële steun vanuit het ministerie van EZK tot en met 2021 metingen doen naar onveilige en al gehackte IoT-apparaten in Nederland. Dat doen zij door bijvoorbeeld netwerken van besmette apparaten in kaart te brengen, zogenoemde botnets. Het Digital Trust Center van het ministerie van EZK gaat vervolgens in gesprek met fabrikanten over maatregelen om besmette apparaten veilig te maken. Door besmettingsinformatie over apparaten te delen met de vereniging Abuse Information Exchange, een Nederlands samenwerkingsverband van internetaanbieders, kunnen zij hun klanten informeren hoe zij besmettingen kunnen opschonen.

Onderzoek EZK: bewustzijn aanwezig, nog weinig kennis over te nemen maatregelen
Het ministerie van Economische Zaken en Klimaat heeft door KANTAR onder meer dan 2.600 ondernemers en consumenten laten onderzoeken hoe zij omgaan met het Internet-of-Things. Eén op de vijf consumenten geeft aan (helemaal) niet te weten hoe apparaten die met het internet verbonden zijn, beveiligd moeten worden. Een ruime meerderheid van de consumenten zegt te weten hoe ze een computer of mobiele telefoon moeten beveiligen. Voor andere slimme apparaten zoals speelgoed, lampen of koelkasten is dit nog minder dan de helft. Software updates worden in grote mate uitgevoerd, regelmatig wachtwoorden wijzigen doet een minderheid. Ook ondernemers voeren in meerderheid actief en frequent software updates uit. Met uitzondering van de computer/mobiele telefoon wijzigen ook bedrijven in minder dan de helft van de gevallen frequent de wachtwoorden van andere slimme apparaten.

Publiekscampagne over digitale veiligheid
Het ministerie van Economische Zaken en Klimaat start mede op basis van de onderzoeksresultaten en de Roadmap Digitaal Veilige Hard- en Software eind dit jaar een overheidscampagne om consumenten en ondernemers te informeren hoe zij hun digitale veiligheid kunnen verbeteren.

Veiligheid in de organisatie

Meer weten? Bekijk ons opleidingsaanbod:

Safety manager
Om te zorgen dat ongevallen in jouw organisatie uitblijven, zijn maatregelen nodig. Daarvoor moet je dan wel eerst de risico's kennen en weten hoe je deze risico's kunt voorkomen of beperken. In deze opleiding leer je;

- Moeiteloos de verbanden tussen strategische veiligheidsprocessen te leggen
- Inzicht te krijgen in de organisatie en veiligheidscultuur
- Dit te operationaliseren door praktijkoefeningen

www.sbo.nl/safety

QHSE-manager
Jouw organisatie is gebaat bij een veilige en gezonde werkplek waarbij de kwaliteit van het geleverde product/dienst voorop staat en er tegelijkertijd rekening wordt gehouden met de belasting van het milieu. Tijdens deze opleiding leer je:

- Hoe je voldoet aan geldende wet- en regelgeving op het terrein van arbeidsomstandigheden, veiligheid, gezondheid en het milieu
- Op welke manier je de kwaliteit van producten en diensten bevordert
- Hoe je draagvlak creëert voor QHSE binnen jouw organisatie

www.sbo.nl/qhse

Adviseur kwaliteit en veiligheid in de zorg
Hoe informeer, adviseer en ondersteun je zorgverleners en het management om de kwaliteit binnen jouw organisatie continue te verbeteren? Tijdens deze opleiding leer je:

- Hoe je de veiligheidscultuur kunt vergroten binnen jouw organisatie
- Op welke manier je risico's in kaart brengt en dit vertaalt naar een plan van aanpak
- Hoe je streeft naar een continue verbetering en anderen hiertoe aanzet

www.sbo.nl/kwaliteitzorg

Security Manager
Met de dreigingen van tegenwoordig, zoals terrorisme en (cyber) criminaliteit, staat security management hoog op de prioriteitenlijst binnen veel organisaties. In deze opleiding leer je op praktische wijze;

- Hoe je de toegangsverlening en het toegangsbeheer organiseert in jouw organisatie
- Hoe je mogelijke dreigingen in kaart brengt
- Op welke manier je jouw organisatie beschermt tegen deze dreigingen

www.sbo.nl/securitymanager

Veiligheid in de organisatie

Veiligheid van gebouwen
Deze opleiding is voor iedereen die in control wilt zijn over asbest, brandveiligheid, legionella, constructierisico's en installatierisico's in jouw gebouw. Je hebt vaak te maken met allerlei adviseurs en onderaannemers en het is belangrijk dat je als opdrachtgever over een basis kennisniveau beschikt. In deze opleiding leer je op een praktische wijze;

- Hoe je de veiligheid van jouw gebouw in kaart brengt en risico's beheerst
- Aan welke veiligheidswetten, regels en voorschriften jouw gebouw moet voldoen
- Hoe je het bouwbesluit eenvoudig vertaalt naar jouw praktijk

www.sbo.nl/veiliggebouw

Beveiliging van gebouwen
Na het volgen van deze opleiding heb je kennis in huis om alle organisatorische, juridische en bouwkundige eisen te stellen en te beoordelen om gebouwen en terreinen zo kosteneffectief mogelijk te beveiligen. Je leert;

- Wanneer en onder welke voorwaarden je cameratoezicht mag toepassen
- Met welke juridische aspecten je rekening moet houden bij toegangsverlening en toegangsbeheer
- Veiligheidsgevoel onder medewerkers, klanten en bezoekers vergroten

www.sbo.nl/beveiliging

Brandveiligheid van gebouwen
Met de juiste maatregelen voldoe je aan de wet- en regelgeving, verklein je de kans op brandgevaarlijke situaties en voorkom aansprakelijkheidsclaims. In deze opleiding leer je;

- Aan welke wetten, regels en voorschriften jouw bouwwerk moet voldoen
- Hoe je de brandveiligheid van jouw gebouw waarborgt
- Hoe erop wordt toegezien dat bouwregelgeving wordt uitgevoerd en nageleefd

www.sbo.nl/brandveiligheid

Information Security Officer
Cybercriminaliteit dreigt de wereldmarkt in 2021 jaarlijks meer dan vijf biljoen euro te gaan kosten Voor zowel grote als kleine bedrijven is de kans dat bedrijfsgevoelige informatie lekt steeds groter. Bedreigingen zoals Phishing, hacken, DDos-aanvallen, datalekken, informatiediefstal en identiteitsfraude zijn aan de orde van de dag. Criminelen azen op informatie en medewerkers creëren -vaak onbewust- een onveilige situatie. In deze opleiding leer je de beschikbaarheid, integriteit en vertrouwelijkheid van informatie binnen jouw organisatie te behouden.
www.sbo.nl/informationsecurity