Vereniging Preventie
&
Bedrijfshulpverlening Nederland

VPBN

INFORMATIEBULLETIN NUMMER 37 maart 2018

Vereniging Preventie & Bedrijfshulpverlening Nederland
Apeldoornsestraat 36 | 8266 AM Kampen | 038-3312377| info@vpbn.nl | www.vpbn.nl

Voor u ligt het zeven-en-dertigste informatiebulletin van de vereniging. Wanneer u als lid bijzondere gebeurtenissen, jubilea of ander nieuws heeft te melden, laat u het ons weten? Wij zullen er graag aandacht aan besteden.

Redactioneel

Jan Luijten

Colofon:

maart 2018
jaargang 10,
nummer 1

Redactie
Jan Luijten
Jo Thewissen
Annie van 't Zand

Redactieadres
VPBN
Apeldoornsestr. 36 |
8266 AM Kampen
info@vpbn.nl

Wat we van Prebes kunnen leren….

Dit keer is het redactioneel ontstaan als gevolg van een bijeenkomst van Prebes België. Prebes vertelde daar over de visie die zij hebben op de taak die de preventiemedewerker/ preventieadviseur zou kunnen hebben bij het doen van onderzoek naar de basis van veel ongevallen. Door dat onderzoek worden de mogelijke valkuilen op een rij gezet waardoor wellicht ook mogelijke oplossingen kunnen worden gevonden. De huidige praktijk leidt er volgens Prebes toe dat de resultaten van de huidige wijze van ongevallenonderzoek zelden leidt tot het vinden van basisoorzaken, waar het allemaal mee begint. Vaak worden enkel rechtstreekse of directe oorzaken geïdentificeerd omdat deze het meest zichtbaar zijn en daardoor het gemakkelijkst te benoemen. Helaas is er daarnaast meestal onvoldoende tijd voor en diepgang bij het zoeken naar de echte oorzaken.

Prebes stelt, dat wanneer er onvoldoende diepgang is bij onderzoeken van ongewenste gebeurtenissen in de organisatie, men bang is dat men de geloofwaardigheid van de functie van preventiemedewerker/preventieadviseur daardoor zelf ondermijnt Op deze wijze lopen we de kans om als preventiemedewerker/preventieadviseur buiten de boot te vallen tijdens de ontwikkeling van managementsystemen, én dat andere functies binnen de organisatie deze taken zullen oppakken. De functie van de preventiemedewerker/preventieadviseur is inmiddels wel wettelijk vastgelegd maar het risico blijft bestaan dat de functie inhoudelijk weinig (blijft) betekenen.

Als we praten over ongevallenonderzoek, wat bedoelen we dan? Bedoelen daarmee alle ongewenste gebeurtenissen in het bedrijf en niet enkel onderzoek van ongevallen met letsel? Bedoelen we ook onderzoek van ongevallen met materiële schade, milieuschade, bijna- ongevallen, onveilige situaties, productiestilstanden, afwijkende producten, onnodige energieverspilling ect. Er zijn genoeg onderzoeksystemen, modellen, en diagrammen voorhanden om na te gaan welke basisoorzaken tot het ongeval hebben geleid, en hoe we dan kunnen komen tot passende preventiemaatregelen ter voorkoming van gelijksoortige ongevallen.

Het advies is om te blijven graven naar de dieper liggende oorzaken en er voor te waken nooit het woord 'fout' in de mond te nemen en niet de wijsvinger te gebruiken. Het gaat er immers om de oorzaak van het gedrag van werknemers onder de loep te nemen en een eenzijdige visie te voorkomen.

Een onderzoek DOE JE NOOIT ALLEEN, zorg voor openheid, cultuurwijzigingen, overleg met alle betrokkenen, ook als ze in een andere groep werken aan dezelfde taak. Ga niet alleen achter je laptop zitten, maar werk met standaarden en voorschriften als je het onderzoek uitvoert en leg de gegevens na gezamenlijk overleg vast. Neem gelijkwaardige situaties mee in het onderzoek en durf ook verder te kijken naar bedrijven in dezelfde sector. Kies daarbij voor een begrijpelijk en werkbaar systeem en leidt indien nodig collega`s hiervoor op. Zorg altijd voor een laagdrempelige methode van onderzoek en voor goede communicatie, transparantie en openheid.

Op deze wijze leer je van ongewenste gebeurtenissen, werk je continue aan verbeteren, zorg je voor een lerende organisatie en kun je een link leggen naar de aanwezige beheersystemen. Hierdoor maak je de functie preventiemedewerker/preventieadviseur belangrijk en kun je anderen ervan overtuigen dat deze functie veel toevoegt aan een goede en veilige organisatie.

Jubileum van de redactie en het informatiebulletin

Jo Thewissen

Het was maart 2008 dat het praktijkblad voor BHV met de naam "Attent" werd uitgegeven onder gezamenlijke verantwoordelijkheid van de verenigingen NVB Centraal en Zuid Oost Nederland. De redactie werd gevormd door 2 leden van Centraal en 2 leden van Zuid Oost Nederland. Met ingang van september 2008 werd het blad een uitgave van Kerckebosch onder verantwoording van dezelfde redactie. Echter, door het uitblijven van meer abonnees waren de kosten te hoog en was het niet langer verantwoord om door te gaan. Eind 2008 verscheen dan ook de laatste uitgave van Attent.

Vrijwel gelijktijdig werd besloten om een eigen nieuwsbrief te gaan uitgeven voor de leden van Centraal en Zuid Oost Nederland onder verantwoordelijkheid van het bestaande redactieteam. Dit redactieteam nam de draad weer op en in april 2009 verscheen het 1e informatiebulletin**.** In principe is 2018 een jubileumjaar (10 jaar) voor het huidige redactieteam dat nog steeds bestaat uit de leden, Jan Luijten, Jo

Thewissen en Annie van 't Zand-Boerman. Dit is inmiddels de 37e nieuwsbrief die het licht ziet.

Waarom dit overzicht zult u denken, welnu in de 1e uitgave van april 2009 stond op de 1e pagina de volgende oproep:

Voor u ligt het 1e informatiebulletin van de vereniging.
Wanneer u als lid bijzondere gebeurtenissen, jubilea
of ander nieuws heeft te melden, laat u het ons weten".

Die oproep is elke uitgave herhaald ook nu weer, voor de 37e keer. Tot nu toe is hierop helaas niet gereageerd. Waardoor komt dit toch, is het koudwatervrees of hebben wij zo weinig tijd beschikbaar dat dit niet van de grond komt? Ongevallen, oefeningen, uitbreidingen, opleidingen enz. zijn voorbeelden van gebeurtenissen die in vrijwel elk bedrijf voorkomen en waar vast iets over valt te melden.

De kracht van onze vereniging is dat we via netwerken o.a. kennis opdoen van andermans ervaringen. Ook de nieuwsbrief biedt de mogelijkheid om anderen kennis te laten nemen van relevante zaken of gebeurtenissen bij jouw bedrijf. Hierdoor kan tevens een klankbord ontstaan waardoor er ook weer informatie terugvloeit. Het is te begrijpen dat we het steeds drukker hebben maar investeren in de uitwisseling van ervaringen levert ook een bijdrage aan de kwaliteitsverbetering van BHV, preventie en veiligheid.

Actuele gebeurtenissen uit de praktijk zijn altijd boeiend en leerzaam. Neem daarom contact op met het redactie team en "Kom op met je kopij". Een krant kan ook niet bestaan als er geen actuele zaken meer zijn te melden. Tot slot zij over dit onderwerp nog vermeld dat het redactieteam wel wat nieuw bloed kan gebruiken dus als je zin hebt om het team te versterken laat het ons weten. Je bent van harte welkom.

Stekelig

Onlangs nog een publicatie gelezen op "beveiligings-nieuws.nl" die bij mij enig ongeloof deed groeien. Volgens informatie uit brandweerkringen wordt het met ingang van 25 mei dit jaar verboden om het huisnummer te vermelden bij een incidentmelding vanwege privacy. Eén en ander is een rechtstreeks gevolg van de ingang van de nieuwe Europese Algemene verordening gegevensbescherming (AVG).

Toen ik het hoorde dacht ik dit is nepnieuws, dit kan niet waar zijn. Maar gezien de bron van dit nieuws neem ik aan dat het bericht klopt. Stel je voor je hebt dringend hulp nodig b.v. in verband met brand of hartproblemen. Moet de brandweer dan maar de straat afrijden totdat er rook zichtbaar is? En hoe moet dat dan met de ambulance? En hoe komen de burgerhulpverleners die een AED ter plaatse van een reanimatie moeten brengen en zij die werden opgeroepen om te reanimeren dan terecht bij de persoon met een hartstilstand? Om als voorbeeld maar de Laan van Meerdervoort in Den Haag te nemen met zo'n 1400 huisnummers.

Ik kan me niet voorstellen dat dit praktijk wordt, sterker nog dit mag geen praktijk worden want het gaat mensenlevens kosten. Over privacy is de afgelopen jaren al zo vaak gesproken dat we nu te ver zijn doorgeschoten. Het belang van de burger staat niet meer op de eerste plaats. We verzanden in theoretische beschouwingen waarbij de praktijk soms helemaal uit het oog wordt verloren. Bij een calamiteit telt elke seconde en dient elke melding zo concreet en duidelijk mogelijk te zijn. In Limburg is kort geleden nog een brandweerauto in eerste instantie naar een verkeerd adres gegaan omdat er verwarring was over de straatnaam.

Men maakt zich druk over de privacy maar die loopt al veel langer gevaar bijvoorbeeld omdat persoonsgegevens digitaal over het internet gaan. Hoe vaak moeten we niet vaststellen dat er weer bestanden zijn gekraakt bij bedrijven of overheidsinstanties. Zelfs verzoeken om steun of sponsoring van hulporganisaties komen via de brievenbus binnen en bevatten voor het gemak al voor-ingevulde acceptgiro kaarten met banknummer en adres. Hoezo privacy, en dan wordt nu onder de privacy-vlag een snelle hulpverlening belemmerd?

Hiermee zijn we niet meer het braafste jongetje maar het domste jongetje van de klas. I'm first is tegenwoordig een vaak gehoorde uitdrukking die wat mij betreft ook van toepassing is op de hulpverlening. Dus terugdraaien die uitschieter en "Hulpverlening First".

Zo zit ‘t met zorgplicht van opdrachtgevers

Zorgplicht, een begrip dat in de juridische wereld van veilig en gezond werken veelvuldig langs komt. Een werkgever heeft zorgplicht voor zijn werknemers. Maar hoe zit het met de zorgplicht van een opdrachtgever?

Op verzoek van de Tweede Kamer heeft minister Koolmees (SZW) de Kamer schriftelijk uitgelegd wat het begrip ‘zorgplicht van de opdrachtgever’ inhoudt. Koolmees licht de concrete betekenis toe van het begrip in de praktijk. Wat houdt de wettelijke zorgplicht van een opdrachtgever in?

Uit artikel 7:658 van het Burgerlijk Wetboek vloeit voort dat de opdrachtgever dezelfde zorgplicht heeft jegens zijn opdrachtnemer als de werkgever zou hebben ten opzichte van zijn werknemer. Die zorgplicht houdt in dat hij verplicht is de lokalen, werktuigen en gereedschappen waarmee hij de arbeid doet verrichten, zo in te richten en te onderhouden als redelijkerwijs nodig is om te voorkomen dat de opdrachtnemer schade lijdt. Ook voor het verrichten van de arbeid is de opdrachtgever verplicht zulke maatregelen te treffen en aanwijzingen te geven als redelijkerwijs nodig is om te voorkomen dat de opdrachtnemer schade lijdt. Dit vergt een actieve, alerte opstelling van de opdrachtgever, aldus Koolmees.

Bij een schending van de zorgplicht komt de wet de opdrachtnemer tegemoet door een verlichting van de bewijslast. De opdrachtnemer zal aannemelijk moeten maken dat de schade is opgelopen tijdens de uitvoering van zijn werkzaamheden. Het is vervolgens aan de opdrachtgever om aan te tonen dat hij aan zijn zorgplicht heeft voldaan. Slaagt hij hierin niet, dan is hij aansprakelijk voor de schade die de opdrachtnemer lijdt. De opdrachtgever kan ter dekking van zijn aansprakelijkheidsrisico een verzekering afsluiten bij een particuliere verzekeraar. Hij is daartoe niet verplicht. Als hij een dergelijke verzekering afsluit is dat geen collectieve verzekering voor opdrachtnemers, maar een verzekering die de opdrachtgever compenseert.

Bij een conflict beslist uiteindelijk de rechter over de omvang en de hoogte van de schadevordering van de opdrachtnemer jegens de opdrachtgever. Koolmees stelt niet te beschikken over informatie die inzicht biedt in de concrete betekenis van de zorgplicht in de praktijk. Wanneer een opdrachtnemer schade lijdt, bijvoorbeeld door een ongeval tijdens een skivakantie of een griep, kan hij de opdrachtgever daarvoor niet aansprakelijk stellen. Dit is in de verhouding van werkgever/werknemer niet anders. Het verschil is dat de opdrachtnemer in die situatie niet verplicht is verzekerd voor ziekte en arbeidsongeschiktheid en de werknemer wel, aldus de minister.

Bron: rijksoverheid.nl http://arbo-online.nl/zo-zit-t-met-zorgplicht-van-opdrachtgevers/

3M introduceert toolbox tegen gehoorbeschadiging

We hebben allemaal een emotionele band met wat we horen en houden van de geluiden die ons gelukkig maken. Tegelijkertijd is gehoorschade beroepsziekte nummer één. Het is belangrijk om hier dus wat meer aandacht aan te geven.

Overal is geluid: Elektrisch gereedschap. Grasmaaiers. Sirenes. Rock concerten. Onze oren zijn krachtige antennes die geluiden uit onze omgeving opvangen en vertalen naar verschillende klanken. Een eenmalige blootstelling aan een intensief impulsgeluid of langdurige blootstelling aan geluid boven 85 decibel (dB), kan het gehoor beschadigen. Dit betekent dat zelfs bovengenoemde alledaagse geluiden bij kunnen dragen aan gehoorverlies. En zodra het gehoor beschadigd is, klinkt het mogelijk nooit meer hetzelfde.

Gevolgen van blootstelling aan schadelijk geluid lopen uiteen van een constante piep, brom of ruis in het oor (Tinnitus) tot doofheid. Gehoorverlies kan leiden tot vermoeidheid, stress, depressie en onttrekking van sociale situaties. Daarmee maakt lawaai meer kapot dan je lief is. Dit maakt het des te belangrijker om het gehoor te beschermen tegen lawaai.

Sinds 2016 is schadelijk lawaai officieel erkend als een onomkeerbaar gevaar voor de gezondheid in de nieuwe PBM-verordening. Daarmee komt gehoorbescherming in dezelfde hoge risicocategorie (categorie 3) als ademhalingsbescherming en valbescherming. Werkt u in luide omgevingen maar bent u niet of onvoldoende beschermd? Even achter de oren krabben. Leer meer over blootstelling aan lawaai en hoe je jezelf hiertegen beschermt.

Download de toolbox op de website van 3M.

Data zijn het nieuwe goud

Als bedrijf kun je data het best beschermen met de CIA-methode, want data zijn het nieuwe goud. Dat beseffen organisaties maar al te goed. Daarom willen ze deze data goed beveiligen. Desondanks is de databeveiliging vaak ondermaats. Hoe kun je jouw data wel goed veiligstellen?

Cybercriminaliteit kost de Nederlandse economie jaarlijks 10 miljard euro. Een succesvolle aanval die je bedrijfsprocessen stillegt, vormt vaak grote financiële schade. Zo kon Q-park in mei dagenlang geen geld innen van parkeerders vanwege het WannaCry-virus. En de Petya-ransomware die vlak daarna rondreisde legde de containerterminal van Maersk in Rotterdam lam, met een directe schade van 170 tot 255 miljoen euro.

Het voorbeeld van Maersk betrof alleen directe schade, omdat het werk stil kwam te liggen. Voor andere organisaties zijn de gevolgen groter. Dat is het geval als het cyberincident de reputatie van de organisatie schaadt en (potentiële) klanten zich afvragen hoe veilig hun gegevens bij deze organisatie zijn. In sommige gevallen is dat catastrofaal. Zoals het inmiddels failliete DigiNotar ondervond toen dit beveiligingsbedrijf werd gehackt. Het bedrijf verzorgde certificaten waarmee de veiligheid van onder meer overheidswebsites werd gegarandeerd. Door het lek bleken malafide websites onterecht als ‘betrouwbaar’ bestempeld.

Ook het stilhouden van een hack kan je veel problemen opleveren. Zo werd taxibedrijf Uber in oktober 2016 gehackt. In totaal maakten de hackers 57 miljoen klant- en chauffeurgegevens buit. In plaats van het lek te melden aan de autoriteiten, betaalde Uber de hackers 85.000 euro om de diefstal stil te houden en de data te vernietigen. Daardoor wisten mensen niet dat hun gegevens gevaar liepen. Afgelopen maand is dit lek alsnog uitgekomen en zijn gebruikers en privacywaakhonden vooral boos dat dit voorval onder het tapijt is geveegd.

Om persoonsgegevens in de toekomst beter te beschermen, wordt de Algemene verordening gegevensbescherming (AVG) op 25 mei 2018 van kracht. Vanaf dan mag de Autoriteit Persoonsgegevens boetes uitdelen als bijvoorbeeld blijkt dat de cybersecurity in jouw organisatie tekort is geschoten en/of je verzaakt een hack binnen 72 uur te melden. Boetes voor het niet naleven van de wet kunnen oplopen tot wel 20 miljoen euro of 4 procent van de jaarlijkse wereldwijde omzet.

Kortom, redenen genoeg om je databeveiliging serieus te nemen. Helaas doen organisaties dit nog te beperkt en ongestructureerd. Bepaald robuust zijn de opgeworpen beveiligingswallen niet, zo blijkt uit onderzoek van accountants- en adviesorganisatie Grant Thornton onder 2.900 topmanagers in 36 landen.

Bijna twee derde (65 procent) van de organisaties tast volledig in het duister over hoeveel data er zijn en hoeveel schade er is als deze data worden gestolen, niet meer beschikbaar zijn of de integriteit ervan ter discussie wordt gesteld. Als ze al niet

over deze basiskennis beschikken, hoe kunnen ze er dan zeker van zijn dat ze hun data goed beheren en beschermen?

Een ander opvallend resultaat uit het onderzoek is dat meer dan driekwart van de organisaties (78 procent) beveiligingsmaatregelen neemt zonder speciale aandacht te schenken aan de voor hun bedrijfsvoering meest kritieke of waardevolle data. In het ergste geval betekent dit dat ze dure firewalls inzetten om data met weinig waarde te beschermen, terwijl de voor de bedrijfsvoering essentiële data kwetsbaar zijn. Hoe graag je ook alle data wilt beschermen. Het is niet mogelijk. Naast dat het te kostbaar is, is het vaak technisch niet haalbaar. Richt je daarom op de kritieke data. Data die je organisatie lamleggen als ze gestolen worden, je er geen toegang toe hebt of niet meer betrouwbaar zijn. Oftewel, bescherm je 'kroonjuwelen'.

Wat de kroonjuwelen in jouw organisatie zijn, hangt af van je sector, risicoprofiel en bedrijfsdoelstellingen. Het is niet altijd even makkelijk de kroonjuwelen op te sporen tussen alle spreadsheets, gearchiveerde e-mails en talrijke andere databestanden die in jouw organisatie rondzwerven. Er zijn tools die kunnen helpen bij databeheer, maar er is altijd een menselijk oordeel nodig. Vraag leidinggevenden en andere medewerkers actief na te denken over de verschillende soorten data die zij beheren en deze te classificeren. Grant Thornton doet dit aan de hand van de zogenoemde CIA-methode:

- *Confidentiality*: hoe belangrijk is het dat data vertrouwelijk blijven? Klantdata, patenten en R&D-data zijn bijvoorbeeld alleen bestemd voor ingewijden. Zeer belangrijk, dus.
- *Integrity*: hoe belangrijk is de data-integriteit? Denk aan vrachtgegevens. Manipulatie van deze data kan ertoe leiden dat goederen niet of verkeerd worden afgeleverd. Dat wil je koste wat kost voorkomen.
- *Availability*: hoe belangrijk is het dat data beschikbaar zijn? Data die onmisbaar zijn voor het primaire proces moeten idealiter altijd beschikbaar zijn, en worden beschermd tegen ransomware en andere cyberaanvallen.

Als de data geclassificeerd zijn kun je de risico's afwegen en kwantificeren, zodat je kunt inschatten hoeveel je moet en wilt investeren in beveiligingsmaatregelen. Uiteraard is dit niet van vandaag op morgen geregeld. Grip krijgen op data is tijdrovend. Vier adviezen om datarisico's effectiever te beheersen:

Databeveiliging moet onderdeel worden van de dagelijkse bedrijfsvoering en -cultuur wil het zijn vruchten afwerpen. Dat begint met databeveiliging als een organisatiebreed onderwerp te beschouwen, met het topmanagement als eindverantwoordelijke.

Welke data vallen onder de kroonjuwelen? Stel multidisciplinaire teams samen die de kroonjuwelen van jouw organisatie identificeren en classificeren aan de hand van bovengenoemde CIA-methode. Stel op management en operationeel niveau data-

eigenaren aan. Per project kan de data-eigenaar helpen de data te classificeren en nagaan aan welke privacy-verplichtingen moet worden voldaan.

Creëer meer bewustwording onder al je medewerkers. Zorg dat ze de risico's begrijpen door ze te vertalen naar de dagelijkse praktijk. Train ze om de waarde van data te herkennen en om privacy- en cyberrisico's op te kunnen sporen. En test of de training heeft geholpen.

Er komen voortdurend nieuwe data bij en ook cybercriminelen zitten niet stil. Voer jaarlijks een beveiligingsonderzoek uit zodat je weet of jouw (technische) beveiligingsmaatregelen (nog) de risico's afdekken. En evalueer en test periodiek ook de effectiviteit van de genomen organisatorische maatregelen en stel deze waar nodig bij. *Meer weten? Download de gratis whitepaper 'Wat is de waarde van uw data?' van Grant Thornton.*

CHECKLIST BETERE BRANDVEILIGHEID BIJ SENIOREN

Senioren willen steeds langer zelfstandig blijven wonen. Ook het beleid van de overheid is erop gericht om pas bij verregaande hulpbehoevendheid te zorgen voor intramurale huisvesting. Dit zorgt voor brandveiligheidsrisico's in steeds meer woongebouwen. Reden voor het Aedes-Actiz Kenniscentrum Wonen-Zorg om samen met Aedes, ActiZ en Brandweer Nederland een 'Checklist zelfstandig wonen & brandveiligheid' op te stellen. Een hulpmiddel voor gebouwbeheerders om huurwoningen te inspecteren, in het bijzonder voor seniorencomplexen.

Woningcorporaties willen senioren op een veilige manier langer thuis laten wonen. Het is dan wel belangrijk dat alle wettelijk vereiste brandveiligheidsvoorzieningen op orde zijn. Dit is niet altijd voldoende bij de meer kwetsbare personen. Er zit een zwart gat tussen de Nederlandse brandveiligheidsregelgeving en de praktijk van branden in seniorencomplexen. De regelgeving gaat bij wonen namelijk uit van zelfredzame personen. De veronderstelde mate van zelfredzaamheid is geen vast gegeven bij diverse kwetsbare groepen, zoals senioren. Dat risico wordt nog versterkt als er sprake is van een clustering van kwetsbare personen, denk aan seniorencomplexen.
Risico's én oplossingen in beeld

De 'Checklist zelfstandig wonen & brandveiligheid' helpt de gebouwbeheerder om de veiligheidsrisico's vast te stellen van een gebouw en de bewoners. Als maatregelen wenselijk zijn, draagt de checklist oplossingen aan. Die zijn divers van aard. De woningcorporatie zal samen met de betrokkenen, zoals bewoners (of hun vertegenwoordigers), zorgverleners, gemeente en veiligheidsregio aan de slag gaan om de geconstateerde risico's te reduceren.

De checklist geeft antwoord op twee vragen:
- Hoe herken ik situaties waar de brandveiligheid in het geding is en wat zijn de kritische brandveiligheidspunten?
- Wat zijn de oplossingsrichtingen per geconstateerde risicosituatie?

NTA 8220 ‘Methode voor het beoordelen van elektrisch materieel op brandrisico’ gepubliceerd

De installatiebranche, verzekeraars en inspecteurs hebben gezamenlijk een nieuwe beoordelingsmethodiek opgesteld voor brandrisico’s bij elektra. De manier waarop inspecteurs de risico's nu nog beoordelen, is niet helemaal sluitend en biedt ruimte voor onduidelijkheid. De nieuwe methodiek maakt daar een eind aan.

Brand is een groot gevaar voor mens, dier en milieu en kan leiden tot grote economische schade. Een brand met een elektrische oorzaak beperkt zich niet alleen tot een elektrische installatie, een elektrisch apparaat of elektrische uitrusting van een machine. Verspreiding van brand is daarom een belangrijk aandachtspunt in NTA 8220. Naast het beoordelen van het elektrisch materieel op brandrisico, moet ook worden beoordeeld of in de nabijheid van het elektrisch materieel brandbaar materiaal aanwezig is. Als verzekeraars kunnen verwijzen naar NTA 8220, is voor alle betrokkenen duidelijk dat en hoe het inspectiebedrijf de brandrisico’s van de installatie beoordeelt.

De beoordelingsmethode in NTA 8220 bestaat uit visuele waarnemingen, metingen en beproevingen. De visuele controle omvat al het elektrisch materieel dat deel uitmaakt van een installatie, en elektrisch materieel dat in gebruik is op het moment van de controle. Tijdens de controle moet rekening worden gehouden met brandbare materialen in de directe omgeving van het elektrisch materieel. Er wordt hierbij van uitgegaan dat het elektrisch materieel is geïnstalleerd volgens de van toepassing zijnde norm(en) en wordt gebruikt volgens de voorschriften van de fabrikant.

De NTA 8220 is geen wettelijke verplichting, maar kan geëist worden door verzekeraars aan hun klanten met een brandverzekering. Waar vroeger een vraag was naar bijvoorbeeld een NEN 3140 inspectie vanuit de brandverzekering kan dit hierdoor gaan verschuiven naar een NTA 8220 inspectie of wellicht beide inspecties (waarbij de NTA 8220 een aanvulling is op de NEN 3140).

NTA 8220 is een samenwerking van UNETO-VNI, I-keur (inspectiebranche) en het Verbond van Verzekeraars. De controlemethodiek is onder het beheer van het Nederlands Normalisatie Netwerk (NEN) vastgelegd in een Nederlands Technische afspraak (NTA).

Er is ook een nieuwe training NTA 8220 in één dag, tijdens deze training leert u wanneer en waarvoor u de NTA 8220-methode kunt gebruiken, en wat de verschillen zijn met andere type inspecties. Bovendien leert u hoe u de NTA 8220 daadwerkelijk toepast.

Die veiligheidshelm past ons allemaal

Een goede bescherming van het hoofd tijdens het werk is geen luxe. Een veiligheidshelm beschermt tegen verwondingen door stoten of vallende voorwerpen.

Waar moet u op letten bij de keuze van een goede veiligheidshelm? Welke punten moet u regelmatig checken? Op welke werklocaties bent u verplicht om een veiligheidshelm te dragen? Welke normen gelden er voor helmen? Dit en meer leest u hier.

Waar is het dragen van een veiligheidshelm verplicht?

- Daar waar de kans bestaat getroffen te worden door wegvliegende of vallende voorwerpen. Zoals in de bouw, in productiebedrijven en op werkplekken waar hijskranen aan het werk zijn.
- Daar waar een verhoogde kans bestaat op stoten of bekneld raken van het hoofd. Bijvoorbeeld in de buurt van machines.
- Daar waar dit door middel van een bord staat aangegeven. Een werklocatie met helmplicht is te herkennen aan een rond blauw bord met een witte afbeelding van een helm.

Een veiligheidshelm moet bescherming bieden tegen de risico's van het werk en de werkplek. Die risico's en de locatie bepalen wat een geschikte helm is. Daarom zijn er veel verschillende helmen voor verschillende toepassingen. Enkele voorbeelden van helmen voor specifieke situaties:

- standaard bouwhelm: beschermt tegen dagelijkse risico's als stoten of (kleine) vallende voorwerpen
- helm met korte klep: voor mensen die tijdens het werk veel naar boven kijken
- interventiehelm of motorhelm: voor mensen die werkzaam zijn bij ongevallen, zoals brandweer en medische hulpdiensten
- brandweerhelm: beschermt tegen penetratie, vlammen, elektriciteit en hittestraling

De keuze voor een veiligheidshelm moet terug te vinden te zijn in de risico-inventarisatie en -evaluatie (RI&E) en het plan van aanpak voor de uitvoering. Een goede veiligheidshelm is geschikt voor de werkplek, past perfect op het hoofd van de drager en zit daardoor comfortabel. Een helm die onder alle omstandigheden goed zit, draagt veel bij aan een veilige werksituatie.

Een veiligheidshelm is met recht een hoofdzaak bij veilig en gezond werken. Maar hoe lang blijft zo'n helm eigenlijk goed? Oftewel: wat is de levensduur van een veiligheidshelm?

De gebruiksduur van een veiligheidshelm is afhankelijk van twee zaken: het materiaal van de helm en de omstandigheden waaronder die wordt gebruikt. De invloed van externe factoren op het materiaal speelt daarbij een belangrijke rol. Denk aan UV-straling, temperatuur en aantasting door chemicaliën.

Veiligheidshelmen kunnen zijn vervaardigd uit thermoplastische kunststoffen zoals polyethyleen, polyamide en polycarbonaat. Ook kunnen ze zijn gemaakt van thermoharders of duroplasten zoals textielfenol, glasvezelpolyester en gelaagd materiaal.

Bij thermoplastische kunststoffen bepaalt onder meer een weekmaker in het materiaal de taaiheid en daarmee de sterkte van het materiaal. Door warmte en UV-licht, bijvoorbeeld zonlicht, 'verdampt' de weekmaker als het ware langzaam uit het materiaal. Dit maakt de helm op den duur bros. *Bron: Arbo online*

Gevaarlijke bijlagen in Office 365 onderscheppen

Als meest gebruikte zakelijke e-mail omgeving hebben hackers bijzondere aandacht voor Office 365. Microsoft biedt met Exchange Online Protection en Advanced Threat Protection een goede eerste verdediging, daarmee is uw email echter nog niet optimaal beveiligd.

In dit onderzoek van Mimecast werden meer dan 36 miljoen ontvangen e-mails onderzocht bij meer dan 40.000 Office 365 gebruikers. Uit dit uitgebreide onderzoek bleek dat mails toch nog verdachte bijlagen werden afgeleverd, met onder meer gevaarlijke malware.
Download nu dit rapport om te ontdekken:

- Welke typen gevaren werden aangetroffen en hoe vaak
- Welke maatregelen u kunt nemen om uw organisatie daartegen te beschermen

Herziene norm voor sprinklerinstallaties gepubliceerd

NEN heeft in samenwerking met het deskundigenpanel VBB-systemen van het Centrum voor Criminaliteitspreventie en Veiligheid (CCV) de Nederlandse aanvulling op de Europese (in het Nederlands vertaalde) norm voor ontwerp, installatie en onderhoud van automatische sprinklerinstallaties (NEN-EN 12845:2015) herzien en gepubliceerd.

NEN 1073:2018 vormt het eerste ‘tastbare’ resultaat van het convenant, dat op 31 maart 2016 door beide partijen is gesloten teneinde de wildgroei in normen en regels voor vastopgestelde brandbeheersings- en brandblussystemen (VBB-systemen) terug te dringen.

In deze nieuwe versie is een groot aantal besluiten en interpretaties van het deskundigenpanel VBB-systemen van het CCV opgenomen. Verder zijn NTA 8073-1 ‘Bepaling van middellijnen van armpijpen bij grote doorstroomhoeveelheden’ en NTA 8073-2 ‘Eisen voor toepassing van thermoplastische spanplafonds in gesprinklerde gebouwen’ van 2011 opgenomen. Tenslotte is NEN 1073 aangepast naar aanleiding van de publicatie in 2015 van de eerste revisie van NEN-EN 12845.

Voor meer informatie over deze norm of over het normalisatieproces: Marc Mergeay, Consultant Bouw & Installaties, telefoon 015 2 690 367 of e-mail bi@nen.nl.

Kiwa: “Veiligheid in gebouwen gaat beter, maar we zijn er nog niet”

We zijn er nog lang niet, maar het gaat steeds beter met de brandveiligheid in gebouwen in Nederland. Binnenkort zijn er certificeringsregelingen voor vrijwel alle onderdelen van actieve brandveiligheidsinstallaties. Er is zelfs een objectief en onafhankelijk certificeringsschema voor de noodverlichting en de vluchtweg-aanduiding. De integrale brandveiligheid van gebouwen – ook gloednieuwe – kan volgens Kiwa nog lang niet altijd daadwerkelijk worden gecertificeerd. Dit overigens met uitzondering van de wettelijk verplicht te certificeren onderdelen van actieve

brandveiligheidsinstallaties. Dat is de praktijkervaring van certificatie-instelling Kiwa Fire Safety & Security (FS&S). Maar het bewustzijn op dit gebied bij gebouweigenaren en eindgebruikers van grote organisaties groeit. De aandacht voor de passieve brandveiligheid, zoals brandscheiding en brandwering, kan beter. Het certificeren van noodverlichting en vluchtwegsignaleringssystemen gebeurt op basis van certificatieschema K21019.

Het schema kent drie toepassingsgebieden:
- Levering van de dienst onderhoud en nazorg zonder controle op detailontwerp.
- Levering van installatie en renovatie, waar detailontwerp een onderdeel van is.
- Levering van de dienst projectie, waar basisontwerp en detailontwerp een onderdeel van zijn.

Hier is een schakeldraad (zwart) gebruikt in plaats van een fasedraad (bruin). Het betreft een vluchtrouteaanduiding. Dit certificatieschema heeft eisen opgenomen op basis van een aantal normen die verderop in dit artikel aan bod komen.
De normen beschrijven de volgende doelstellingen van deze systemen:
NEN 1838: *Verlichtingstoepassingen – Noodverlichting. Deze Europese norm specificeert de eisen voor vluchtwegverlichting en stand-by-verlichting in ruimten of plaatsen waar dergelijke systemen zijn vereist. De norm is vooral van toepassing op plaatsen waar veel mensen toegang hebben;*

NEN 6088: *Brandveiligheid van gebouwen – Vluchtwegsignalering – Kenmerken en bepalingsmethoden. Ook deze Europese norm specificeert de eisen voor vluchtwegverlichting en stand-by-verlichting in ruimten of plaatsen waar dergelijke systemen zijn vereist, eveneens op plaatsen waar veel mensen toegang hebben;*

EN 50172: *Vluchtwegverlichting. Deze Europese norm specificeert de levering van verlichting van vluchtwegen en de vluchtwegsignalering in het geval van uitval van de primaire energiebron, en specificeert de minimale levering van noodverlichting op basis van de grootte, het type en het gebruik van de locatie. Deze norm heeft betrekking op de levering van elektrische vluchtwegverlichting op alle werkplekken en in gebouwen die open zijn voor het publiek.*

Op basis van deze normen mogen de volgende doelstellingen verwacht worden van deze systemen: Voldoende licht in noodsituaties, waarbij men uitgaat van de situatie dat de verlichting in het gebouw uitvalt ten gevolge van een stroomstoring, waarbij gebruikers van het gebouw in staat worden gesteld om met de beperkte noodverlichting het pand veilig te verlaten. Voldoende zichtbare vluchtwegsignalering, die in geval van een calamiteit de gebruikers van een gebouw in staat stelt het pand veilig te verlaten. Het doel in relatie tot de brandveiligheid is niet duidelijk, gezien vanuit deze normen. Deze omissie is ook terug te vinden in het Bouwbesluit.

Het calamiteitenscenario bij de eerdergenoemde normen gaat vooral over het uitvallen van de primaire energievoorziening, waardoor de verlichting uitvalt en de

noodverlichting en de vluchtwegsignalering gebruikers van het gebouw veilig naar buiten kunnen begeleiden. De eisen in deze normen voldoen prima aan dit calamiteitenscenario. Maar bij de huidige calamiteitenscenario's voor brand, waarbij veel sneller rook ontstaat door de toepassing van kunststoffen in vergelijking met dertig jaar geleden, zal een ruimte binnen 60 seconden gevuld zijn met rook. In dat geval zal de vluchtwegsignalering niet aan de verwachtingen kunnen voldoen. Daarnaast hangen de bordjes meestal op een verkeerde plaats. Over het algemeen worden ze vlak onder het plafond en boven een deur geplaatst. Maar warme rook stijgt op, waardoor de bordjes in de rooklaag komen te hangen. Het licht van de bordjes wordt door de rook weerkaatst, zoals ook gebeurt bij autolampen bij het rijden door mist. Hierdoor zijn de bordjes niet meer zichtbaar.

Alternatieve oplossingen zijn aanduidingen op knie- of vloerhoogte, zoveel mogelijk onder de rook. Ook dynamische vluchtrouteaanduidingen, zoals de lopende lampjes in een vliegtuigvloer, zijn mogelijke alternatieven voor de groene transparanten bovendeuren. Meest verbazingwekkend is het scenario 'rook door brand in ruimten zonder daglicht', waarbij van noodverlichting en vluchtwegsignalering volgens de huidige normen en wetgeving slechts een beperkte bijdrage ten aanzien van de vluchtveiligheid verwacht mogen worden.

Het ontwerp van dit soort systemen moet uitgevoerd worden door deskundigen. Hier zijn opleidingen en examens voor. Verkeerde installatiekabel gebruikt. De fase wordt als aarde gebruikt en de schakeldraad als fase. Verder aluminiumfolie om de twee aarders aan elkaar te verbinden.

In hoofdlijnen moet het ontwerp noodverlichting zorgen voor licht(punten) verdeeld over ruimten en vluchtwegen, waardoor er ook bij een calamiteit voldoende zichtbaar licht aanwezig is ter oriëntatie op de (nood)uitgang, waarbij extra aandacht gevraagd wordt voor verhogingen en verlagingen in de vluchtroute(s). De hoofdlijn van het ontwerp vluchtwegindicatie is dat de groene transparanten vanuit elke positie in een ruimte zichtbaar zijn, zodat de gebruiker zijn vluchtweg kan bepalen. Hierbij moet de vluchtwegindicatie onderscheid maken tussen een uitgang en een nooduitgang. Dit onderscheid zal de gemiddelde gebruiker echter niet kennen en de bedoeling hiervan dus ook niet begrijpen.

Verkeerde verwijzing door het pictogram.

De praktijk is dat systemen aangelegd en onderhouden worden zonder certificaat, en dus niet aantoonbaar voldoen aan de normen. Van de gebruiker en de eigenaar van het gebouw wordt door de wetgever verwacht dat zij systemen hebben die adequaat werken en adequaat worden onderhouden. Tijdens controles worden voldoende omissies vastgesteld, die de noodzaak van goed aangelegde en onderhouden systemen onderschrijven. Met het hebben van goede systemen wordt de wettelijk gevraagde zorgplicht vervuld. De systemen zijn in te delen in decentrale en centrale systemen.

Decentrale systemen hebben de noodstroomvoeding voor de noodverlichting in het armatuur zelf zitten, vaak in combinatie met de vluchtwegsignalering. Deze armaturen moeten wel op de primaire energievoorziening aangesloten worden. Gelukkig zijn door de toepassing van LED in de armaturen, de batterijen kleiner geworden.

De kabelgoot te kort en aardedraad

Het onderhoud wordt vooral door REOB-bedrijven gedaan. REOB-gecertificeerde bedrijven doen ook het onderhoud van de draagbare blusmiddelen, die apart gecertificeerd worden. De betreffende bedrijven zien dit als belangrijke aanvulling op hun bestaande dienstenpakket. Via een specifieke training 'Onderhoud decentraal' is deze kennis goed overdraagbaar aan REOB-monteurs. De levering en het ontwerp zitten bij elektrotechnisch opgeleide personen van REOB-bedrijven en beveiligingsbedrijven. Er is bij deze toepassing aandacht voor de standaard NEN 1010/NEN 3140-issues.

Bij centrale systemen zijn de noodvoedingen centraal op één plek in het gebouw aanwezig en lopen er kabels van de noodvoeding naar de armaturen. De kabels zijn in het hele gebouw aanwezig. Als de bewakingseenheid in deze centrale noodvoeding vaststelt dat de primaire energie wegvalt, zal deze de noodverlichting inschakelen. De grotere gecertificeerde beveiligingsbedrijven (REOB en brandmeldinstallaties) zien dit als een aanvulling op hun bestaande dienstenpakket, vaak in combinatie met brandmeldinstallaties. Elektrotechnische installatiebedrijven schuiven aan als verlengstuk van deze bedrijven. Bijzondere technische aandachtspunten zijn: de berekening van de kabeldiameter, de capaciteit van de accu, de bepaling van de toestand van de accucapaciteit en een juiste aansluiting volgens NEN 1010.

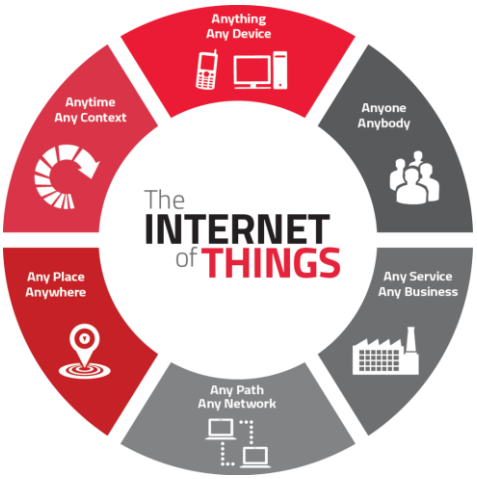
Op dit moment werkt Kiwa aan de invulling van een aantal onderwerpen binnen dit certificatieschema, zoals: Voldoende licht in noodsituaties gerelateerd aan diverse noodsituaties en het gebruik van de ruimte. Het geven van een zichtbare vluchtrichting op basis van het gebouwontwerp, rekening houdend met: 1) brandcompartimenten en brandscheidingen (rookscheidingen) en 2) gelijktijdigheidsfactoren van mensen. *Bron en tekst Peter Voshol , manager business development bij Kiwa*

IoT-toepassingen bedreiging voor veiligheid en privacy

Nieuwe technologieën, zoals het Internet of Things (IoT), zijn een belangrijke drijfveer voor innovatie en economische groei. Maar de technologische en economische kansen gaan hand in hand met digitale dreigingen voor economische groei, veiligheid en vrijheid. Hiervoor waarschuwd de Cyber Security Raad (CSR).

De Raad is vooral bezorgd over de beheersbaarheid van het IoT als het om cybersecurity en privacy gaat en heeft hierover het advies 'Naar een veilig verbonden digitale samenleving; Advies inzake de cybersecurity van het Internet of Things (IoT)' opgesteld. Vanmiddag overhandigde de CSR het advies persoonlijk aan de minister van Justitie en Veiligheid prof. mr. F.B.J. (Ferdinand) Grapperhaus en de Staatssecretaris van Economische Zaken en Klimaat mr. drs. M.C.G. (Mona) Keijzer. Daarnaast wordt het advies schriftelijk aangeboden aan de staatssecretaris van

Binnenlandse Zaken en Koninkrijksrelaties drs. R.W. (Raymond) Knops alsook ondersteuning van het advies aan de voorzitter VNO-NCW, drs. J. (Hans) de Boer.



Het advies bevat zes strategische oplossingsrichtingen om de uitdagingen die het IoT met zich meebrengt het hoofd te bieden: certificering, keurmerken, toegangseisen, transparantie, bewustwording, productaanspra-kelijkheid, intermediaire verantwoordelijkheden en versterking handhaving.Aanleiding voor dit CSR-advies is het besef dat als er geen maatregelen worden genomen het IoT ingrijpende gevolgen kan hebben in de fysieke en digitale wereld en daarmee voor de digitale toppositie van Nederland. Het is van belang dat de veiligheids- en privacyrisico's worden aangepakt om schade zoveel mogelijk te beperken en voorkomen. Om te kunnen profiteren van de kansen die het IoT biedt, moet er tevens op een veilige manier ruimte worden geboden voor nieuwe ontwikkelingen en innovatie. Daarvoor is gerichte actie nodig van onder andere de ministeries van Economische Zaken en Klimaat, Binnenlandse Zaken en Koninkrijksrelaties en Justitie en Veiligheid.

Zo adviseert de CSR onder andere een 'labelling-systeem' in het kader van bewustwording. Stickers op de verpakkingen van IoT-producten moeten consumenten informeren over onder andere het level van beveiliging van het betreffende apparaat en of het apparaat van het internet kan worden afgeschakeld met behoud van de 'reguliere' functionaliteit. Ook een voorlichtingscampagne en een eenvoudige handleiding over het nieuwe 'labelling-systeem' maken onderdeel uit van het CSR-advies.

Het IoT is per definitie een grensoverschrijdend vraagstuk dat in EU-verband moet worden opgepakt. De Europese Unie is een belangrijke speler op het gebied van standaardisatie, wet- en regelgeving en Digital Single Market. In EU-verband kunnen veiligheidseisen makkelijker worden afgedwongen. De raad onderschrijft het belang van het voorstel van de Europese Commissie om te komen tot de oprichting van een Europees kader voor cyberbeveiligingscertificering voor ICT-producten en –diensten.

Opleiding brengt BHV naar strategisch niveau

Elke grotere organisatie heeft wel bedrijfshulpverlening (BHV). Maar hoe manage je dat? Dat leren deelnemers aan de Post-HBO opleiding BHV-Management van SOBA Security Academy. Er gaat onder andere aandacht uit naar het leren spreken van de 'taal' van het hoger management. Dat laatste is niet onbelangrijk.

Vaak wordt BHV gezien als iets wat nu eenmaal moet, totdat het een keer goed fout gaat natuurlijk. Als er doden en gewonden vallen, zal het topmanagement dit moeten verantwoorden. Daarom is het volgens SOBA van groot belang dat BHV bij de bedrijfstop op de agenda komt te staan. Dat gaat echter niet vanzelf. Daarom wordt met name hoofden BHV nu de mogelijkheid geboden om te leren hoe je het belangrijke onderwerp op strategisch en beleidsmatig niveau kunt brengen. De

eerste lichting cursisten heeft recent het diploma gehaald en de nieuwe cursus gaat 4 april van start.

De opleiding omvat acht dagen of zestien avonden en gaat in op tal van inhoudelijke en beleidsmatige onderwerpen. Centraal staat het transformeren van BHV naar een strategische discipline binnen de organisatie. Daarbij komen onder andere de verschillen tussen strategisch, tactisch en operationeel handelen aan de orde.

En dat alles in de 'taal' van het management. Met de modules Veiligheidscultuur, Crisismanagement en Continuïteitsmanagement wordt een goede basis verschaft voor het optimaliseren van de BHV-organisatie. Verder komen onder andere de nieuwe NEN 8112, het bedrijfsnoodplan, wet- en regelgeving, de rol van verzekeraars en financiën aan de orde. Meer informatie is te vinden op de website.

'Security awareness kan altijd nog een stapje beter'

Binnen overheidsorganisaties is een bewuste omgang met de persoonsgegevens van burgers een vanzelfsprekendheid. "Richtlijnen vanuit de Baseline Informatiebeveiliging Nederlandse Gemeenten (BIG) en de Algemene Verordening Gegevensbescherming (AVG) leggen daar nog eens extra de nadruk op", stelt Kaj Siekman, Chief Information Security Officer bij de gemeente Utrecht. Hoe zet deze gemeente met circa 4000 medewerkers 'security awareness' over informatieveiligheid op de agenda?

Security awareness gaat over het 'beveiligingsbewustzijn' onder medewerkers. "Privacy en security zijn belangrijke onderwerpen op de werkvloer", zo stelt Siekman aan het begin van het gesprek in het gloednieuwe stadskantoor van de gemeente Utrecht. Dat blijkt volgens de CISO onder andere uit de vragen die er zowel vanuit de organisatie als van de raad komen over de beveiliging van persoonsgegevens, bijvoorbeeld bij het inrichten van processen en applicaties volgens de nieuwe privacywetgeving. De vraag is dan al snel: wanneer is de inrichting goed genoeg? Joost Heijn, Projectleider U-Flex IPM bij de gemeente Utrecht: "Het zijn professionals die zeer bewust omgaan met privacy en security."

"Maar uiteraard vinden wij dat het altijd nog een stapje beter kan", vervolgt Hans van Impelen, bij de gemeente Utrecht functionaris voor de gegevensbescherming (FG). "De AVG vereist dat je passende technische en organisatorische maatregelen neemt om je informatiehuishouding te beveiligen. Het continu en blijvend investeren in beveiligingsbewustzijn is zo'n maatregel. De Autoriteit Persoonsgegevens kan het een organisatie bij een datalek extra zwaar aanrekenen als er niet of onvoldoende is geïnvesteerd in security awareness. Dat weegt dan mee in de strafmaat."

"De AVG legt organisaties zware verplichtingen op. Wij zijn dan ook al vroegtijdig aan de slag gegaan met de voorbereidingen op de Europese privacyverordening", aldus

Siekman. Zo heeft de gemeente inmiddels de dataverzamelingen in kaart gebracht en vastgesteld met welk doel die data zijn verzameld. In de ‘Utrechtse privacyverordening’ is daarnaast bepaald dat ieder organisatieonderdeel binnen de gemeente een aanspreekpunt moet hebben voor privacy- en informatiebeveiliging. “Deze ‘decentrale security-officers’ (DISO’s) moeten ervoor zorgen dat de onderwerpen security en privacy binnen de gehele organisatie landen.”

“Iedereen moet weten wat gevoelige persoonsgegevens zijn en hoe je daarmee omgaat”, legt Heijn uit. “Hoe ga je bijvoorbeeld om met ip-adressen? Want dat zijn ook persoonsgegevens. En hoe breng je informatie veilig over van a naar b? Als de security awareness daarover toeneemt, groeit ook de vraag naar tooling voor een veilige bestandsoverdracht.” Om gevoelige data veilig te delen met externe partners nam de gemeente Utrecht ruim twee jaar geleden mSafe van Motiv in gebruik. “Dit is een goed en laagdrempelig alternatief voor bijvoorbeeld WeTransfer”, aldus Heijn. Inmiddels wordt mSafe binnen de gemeente Utrecht breder ingezet dan alleen voor de communicatie met externen.

Heijn is bij de gemeente Utrecht belast met het verder vormgeven van het security-awarenessprogramma ‘Bewust Informatie Gebruiken’ (BIG) dat zo’n drie jaar geleden in gang is gezet. Het programma bestaat onder andere uit meerdere activiteiten en een website met tips en trucks over een veilige omgang met persoonsgegevens, en een nieuwsbrief die ingaat op actuele onderwerpen. De projectleider gelooft daarbij in ludieke acties om aandacht te krijgen voor de onderwerpen privacy en security. “Denk aan het serveren van ‘preivacysoep’ of een ‘BIG Mac’ tijdens de lunch om met een woordgrap aandacht voor het onderwerp te vragen, of het ontwikkelen van een escaperoom op basis van informatie in een werkpleksetting. Uiteraard in combinatie met een inhoudelijke presentatie in de kantine over het onderwerp.”

“In de zomer hebben we aandacht besteed aan security op vakantie”, vervolgt Heijn. “Wat zijn de risico’s als je op de camping gebruikmaakt van het gratis wifi? Als je daar de aandacht voor krijgt, dan is de vertaalslag naar de werkvloer weer eenvoudiger. Zeker als je de gegevens van burgers verwerkt, moet je daar integer mee omgaan en dus stilstaan bij informatieveiligheid.” “Om de aandacht vast te houden, moet je vooral variatie aanbrengen in het programma”, vult Van Impelen aan. “Zo hebben we onlangs een mystery guest uitgenodigd om te kijken of die met medewerkers mee naar binnen kon lopen. Die persoon zat uiteindelijk met een cocktail aan onze bar. Dan gaan er wel ogen open. ‘Vreemden kunnen dus ook bij mijn spullen.’”

“Voor het programma Bewust Informatie Gebruiken hebben we als logo een biggetje dat we in alle uitingen laten terugkomen. Het mooie is dat de medewerkers dit biggetje ook zijn gaan associëren met de onderwerpen privacy en security. Dat zegt wel iets over het effect van het programma.”

“We nemen ook regelmatig interviews af waarin we vragen stellen als ‘doe je je scherm op slot?’ en ‘gebruik je een pincode op je telefoon?’”, vervolgt Siekman. “Aan de hand van de antwoorden kun je ook vaststellen of je vooruitgang boekt. Ook zien we dat steeds meer partijen binnen de organisatie met privacy en security aan de

slag gaan en ook cursussen volgen op het gebied van privacy en informatiebeveiliging."

"Het is wel belangrijk dat je aandacht blijft besteden aan privacy en security", benadrukt Heijn. "Dat moet ook wel, want medewerkers komen en gaan. Het bevorderen van het beveiligingsbewustzijn is geen eenmalige actie, maar een voortdurende herhaling van allerlei acties. We kijken nu naar de mogelijkheid om de onderwerpen privacy en informatiebeveiliging deel te laten uitmaken van de introductiedag die nieuwe medewerkers doorlopen. Je laat niet alleen iets van de stad zien, maar geeft ook mee dat goede informatiebeveiliging de standaard is." Siekman: "Een volgende stap is dat elke medewerker een cursus op het gebied van informatiebeveiliging volgt. Voor iedereen moet duidelijk zijn: als we iets doen, dan doen we het veilig." *Bron : Gemeente.nu*

Veilige vluchtwegen en trends in brandpreventie

De brand in de Grenfell Tower in Londen leidde internationaal tot zeer verontruste discussies over de brandveiligheid van hoge woontorens. Het diepgaande onderzoek naar de oorzaken van de brand in de 24 verdiepingen tellende toren in West-Londen is nog niet afgerond. Aan speculaties is ondertussen geen gebrek. Zo zijn er vermoedens dat het vuur in de toren zich snel en makkelijk verspreidde door brandbaar materiaal aan de buitenkant van het gebouw. Duidelijk is dat een deel van de bewoners op de fatale dag – 14 juni 2017 – niet tijdig en veilig kon vluchten.

De brand in een studentenflat in Diemen, waar in de zomer van 2017 een 27-jarige student om het leven kwam, heeft de discussie over veilige vluchtwegen in hoogbouw verder aangewakkerd. De brand ontstond in de vroege ochtend van 19 juli op de begane grond van het zestien verdiepingen hoge gebouw. De student werd na het blussen gevonden in het trappenhuis op de twaalfde verdieping. Zijn vriendin overleefde het incident: ze werd ernstig gewond aangetroffen op de tiende verdieping van het trappenhuis.

"Veilig vluchten bij brand is in Nederland tot nu toe niet een groot issue voor de gemiddelde gebouwgebruiker of -bezoeker. Dit omdat het relatief veilig is in Nederland en we ons vaak moeilijk iets kunnen voorstellen bij brand", zegt Willem van Oppen, adviseur Conformiteitschema's bij het Centrum voor Criminaliteitspreventie en Veiligheid (CCV). "Bovendien is de veiligheidscultuur in Nederland passief, terwijl fire safety in Angelsaksische landen meer onderdeel van het DNA van burgers en bedrijven lijkt te zijn." Voor het thema veilige vluchtwegen komt langzamerhand wel steeds meer belangstelling, zegt Lieuwe de Witte, onderzoeker en adviseur brandpreventie bij de Brandweeracademie van het Instituut Fysieke Veiligheid (IFV). "Dat komt vooral doordat het verschil tussen theorie en praktijk steeds pregnanter wordt. Bij een toenemend aantal gebouwtypen, zoals complexen waar senioren of andere verminderd zelfredzame mensen wonen, sluiten het ontwerp van het gebouw en de inrichting van de vluchtwegen niet aan bij de manier waarop de vluchtroutes worden gebruikt – áls die al worden gebruikt. Neem het vluchten via het trappenhuis. Voor hulpbehoevende ouderen is vluchten via de trap niet logisch of mogelijk. Terwijl het standaard uitgangspunt is dat de lift bij brand niet mag worden gebruikt."

Het IFV (Instituut Fysieke Veiligheid) vraagt inmiddels aandacht voor deze kwestie. “We gaan niet zeggen dat bewoners de lift moeten gaan gebruiken bij brand, maar we moeten de mogelijkheden wel onderzoeken. Zeker omdat we zien dat er steeds meer gebouwen komen voor specifieke doelgroepen zoals zelfstandig wonende ouderen. Daar kunnen verminderd zelfredzamen bij een noodsituatie dus niet direct een beroep doen op hulp van buren om te vluchten.”

Het belang en de urgentie van het thema veilig vluchten zijn steeds duidelijker nu er een toenemend bewustzijn is van de risico’s van rook en rookverspreiding. “In zekere zin is rook en rookverspreiding vele malen gevaarlijker dan brand”, zegt De Witte. “Rook verspreidt zich veel sneller en onvoorspelbaarder dan brand, waardoor mensen onverwacht in een gevaarlijke situatie terecht kunnen komen. Dat is een risico voor degenen die moeten vluchten. Daarbij kunnen de gevaarlijke elementen in rook (bijvoorbeeld brandgassen) ook nog eens de brandbestrijding moeilijker maken. ”

Er is nieuwe regelgeving in de maak, die ertoe moet leiden dat de rookwerendheid van brandscheidingen verbetert. De Witte nuanceert het effect daarvan. “De regels gaan alleen voor nieuwbouw gelden en het is niet duidelijk of de vereiste maatregelen echt toereikend zijn. Het kan bijvoorbeeld belangrijker zijn dat een brandscheiding tijdens de vluchtfase rook- en luchtdicht is dan dat die warmte lang tegenhoudt.”

De Witte waarschuwt dat wet- en regelgeving sowieso niet zaligmakend is voor de veiligheid van vluchtwegen tijdens brand. “Ontwerpers, bouwers en adviseurs zijn sterk gericht op de bouwregelgeving. Maar die regels zijn niet afgestemd op specifieke gebruikers. Nieuwe regels zullen dit probleem niet oplossen. De samenhang tussen gebouw, mens en brand ontbreekt nogal eens bij het op orde brengen van vluchtwegen. En dat vraagt veranderingen op allerlei vlakken, niet alleen in de wet- en regelgeving. Het gaat erom dat we goed kijken naar het doel – in dit geval: veilige vluchtwegen – en de keuzes maken voor maatregelen die passen bij het gebouw en de gebruikers ervan. Dat vereist een cultuuromslag bij alle partijen die betrokken zijn bij brandpreventie. Zo kunnen woningcorporaties en gebouwaanbieders kijken of een gebouw wel geschikt is om er een bepaalde doelgroep, zoals zorgbehoevenden, te huisvesten.” “Alles staat of valt met het bewustzijn bij bewoners en gebouwgebruikers van de noodzaak om brandveiligheid in de gaten te houden”, vult Van Oppen aan. De “rode veiligheid” kan daarbij in samenhang worden gezien met “blauwe veiligheid”. Zo besteedt het Politiekeurmerk Veilig Wonen aandacht aan woningbrand en ontvluchting.

Het oefenen van ontruimingen noemt Van Oppen een absolute noodzaak. “Oefenen is niet alleen belangrijk in gebouwen met gebruiksfuncties – zoals kantoren, fabrieken, conferentieoorden en winkelcentra – waar een BHV-organisatie is opgeleid om ontvluchtingen te assisteren. Het geldt ook voor woningen. Ik begrijp best dat ontruiming van een pand in sommige gevallen bezwaarlijk is. Bijvoorbeeld in een gevangenis, een volle IKEA of een ziekenhuis met bedgebonden patiënten. Maar de ervaring leert dat alleen in de praktijk duidelijk wordt of mensen tijdig en gezond een gebouw uit kunnen komen. Dat valt niet op papier te bewijzen. Alleen door te oefenen kun je leren of je ontruimings- of calamiteitenplan klopt, en of je iets

moet aanpassen om het in de praktijk doeltreffend te laten functioneren." De Witte herkent dat fenomeen – en signaleert de opmars van innovatieve oplossingen. "Een van de dingen die we keer op keer terugzien in brandonderzoek is dat mensen niet bekend zijn met de vluchtroutes. De gewone routes die mensen in de dagelijkse praktijk gebruiken zijn namelijk niet altijd ook de vluchtroutes. Dan is het niet logisch om die bij brand opeens wél te gebruiken. Door gebruiks- en vluchtroutes op elkaar af te stemmen kan al een hoop verbeteren. Maar er vinden ook interessante experimenten plaats met dynamische vluchtroutes en gepersonaliseerde vluchtroutebegeleiding."

De Witte benadrukt het belang van een omslag in denken, waardoor vluchtwegen meer op maat worden ontworpen, voorzieningen worden afgestemd op specifieke doelgroepen en meer doelgericht (op basis van risico's) wordt gewerkt aan de brandveiligheid van gebouwen. "Er zijn allerlei (nieuwe) maatregelen, zoals het luchtdicht maken van brandscheidingen, het toepassen van automatische blusinstallaties, zoals sprinklers-, watermist- en mobiele watermistinstallaties, en het ontwikkelen van brandveilig meubilair. Maar bij veilige vluchtwegen gaat het niet altijd zozeer om nieuwe innovatieve technieken als om de samenhang tussen verschillende maatregelen die worden toegepast."

Het analysemodel voor vluchtveiligheid dat IFV in 2010 publiceerde is wat dit betreft actueler dan ooit, zegt De Witte. "Het hart van het model is dat je inzichtelijk maakt wat de kenmerken zijn van een gebouw, brand en gebruikers (mensen) in een specifieke situatie. Hoewel het model een analyse oplevert – en dus geen ontwerprichtlijnen geeft – raakt de gedachtegang erachter steeds meer ingeburgerd in de praktijk. De uitgangspunten sluiten logisch aan op een doelgerichte benadering van brandveiligheid en kunnen worden vertaald naar branchespecifieke handreikingen." Het Aedes-Actiz Kenniscentrum Wonen-Zorg publiceerde recent de 'Checklist zelfstandig wonen & brandveiligheid', een hulpmiddel voor gebouwbeheerders om huurwoningen en seniorencomplexen te inspecteren. De checklist, die is ontwikkeld door Aedes, ActiZ en Brandweer Nederland, reikt ook oplossingen aan. Daarbij onderscheidt de publicatie maatregelen gericht op de bewoner, het gebouw en voorlichting.

Gezien de digitalisering van onze samenleving is het geen wonder dat in de wereld van brandveiligheid ook steeds meer digitale oplossingen worden gezocht. Van Oppen: "Met het gebruik van apps is het misschien mogelijk om mensen veiligheidsbewuster te maken. Ook de mogelijkheden voor e-learning zijn veelbelovend. Deze worden nu al ingezet om bijvoorbeeld winkelpersoneel te trainen op winkeldiefstal, overval en agressieve klanten, maar zouden ook goed kunnen worden gebruikt voor brandpreventie." De brandweerregio Zaanstreek Waterland ontwikkelde als onderdeel van het project Brandveilig Leven al een app over het veilig ontvluchten uit een woonhuis.

Ook het IFV ziet dat er steeds meer apps en tools worden ontwikkeld, zowel vanuit de brandweer als vanuit belangenorganisaties in bijvoorbeeld de zorg. "Deze helpen partijen om inzicht te krijgen in brandveiligheid. Het lastige is dat de adviezen uit apps zich niet altijd goed verhouden tot wet- en regelgeving. De praktijk beseft niet altijd dat het voldoen aan wettelijke vereisten niet automatisch betekent dat een pand ook veilig is." *Bron: brandveilig.com*