Whitepaper
Incidenten: voorkomen en begrijpen

SECURITAS

Incidenten: voorkomen en begrijpen

Incidenten voorkomen, beheersen, registreren en bespreken met de juiste personen op het juiste niveau; goed omgaan met incidenten is in elke branche, in elke organisatie een belangrijk onderdeel van het integraal veiligheidsbeleid. Maar hoe pak je dat nu aan?

Eén op de drie veiligheidsmanagers heeft de beveiliging niet op orde, in grotere bedrijven is dat zelfs een op de twee, zo blijkt uit de nationale veiligheidsbarometer van Securitas begin dit jaar. De gegevens komen uit onderzoek van Multiscope onder 374 beslissers op het gebied van veiligheid in middelgrote en grote bedrijven.

'Bijna een vijfde van de managers heeft bovendien geen idee waar de veiligheidsrisico's zitten. Terwijl dat toch het eerste is wat je moet weten voordat je aan je beveiliging kunt gaan werken', zegt Stijn Merkelbach, business developer bij Securitas.

Risico's inventariseren
Inzetten op het voorkomen en goed omgaan met incidenten begint bij een goede risicoinventarisatie. Merkelbach: 'Daarbij is het belangrijk zowel naar safety als naar security te kijken.'

Safetymanagement bestaat uit het omgaan met bijvoorbeeld brand, technisch, organisatorisch of menselijk falen en natuur- en omgevingsdreigingen. Securitymanagement gaat over het omgaan met moedwillig menselijk handelen, het voorkomen en het beheersen van acties van mensen die kwade bedoelingen hebben.

Gevaren inschatten is maatwerk
De gevaren goed inschatten blijkt in elke branche, op elke locatie en in elke onderneming maatwerk. Zo gelden in de chemische industrie van oudsher strenge veiligheidsvoorschriften. De gevolgen van een (schijnbaar klein) incident kunnen in deze branche immens zijn. Denk bijvoorbeeld aan de brand

De gevaren goed inschatten blijkt in elke branche, op elke locatie en in elke onderneming maatwerk.

bij Chemie-Pack in 2011 waar vermoedelijk het gebruik van een gasbrander twee bedrijven volledig in de as legde.

Net als in andere branches raken ook in de chemische industrie security en safety elkaar meer en meer. De industrie is kwetsbaar voor nieuwe dreigingen zoals terrorisme en cybercrime, stelt de Vereniging van de Nederlandse Chemische Industrie (VNCI). Zo is het in theorie mogelijk salessystemen binnen te dringen. Nog ernstiger is het als buitenstaanders controle weten te krijgen over besturingssoftware.

Denken vanuit core business

Volgens Merkelbach is het bij het inventariseren van risico's belangrijk te kijken naar de kritische processen in een organisatie en daarbij niets over het hoofd te zien. 'Het is belangrijk te denken vanuit de core business van een onderneming: beveiligen wat écht belangrijk is voor een organisatie.' Toch is het volgens hem een van de grootste uitdagingen nuchter te blijven bij het inschatten van gevaren.

'Je moet je steeds afvragen of een risico reëel is, er wordt veel overdreven. Het is de kunst niet te veel te gaan doemdenken. Neem bijvoorbeeld het inschatten van het risico op het toevoegen van chemicaliën aan een glas water. Tenzij je een gast als president Obama op visite krijgt, is die kans wel heel erg klein.'

Aan de andere kant is het belangrijk te beseffen dat incidenten een onverwacht verloop kunnen hebben', zegt Merkelbach. 'Zo kan na maanden onderzoek blijken dat het niet een buitenstaander, maar de manager is die steelt uit het bedrijfsmagazijn.'

Proactief veiligheidsbeleid

De put wordt vaak gedempt als het kalf verdronken is. Regelgeving omtrent veiligheid en toezicht op de naleving ervan, komt dikwijls reactief tot stand. Een incident dient dan als wake-up call. De ramp bij Chemie-Pack in Moerdijk is daarvan een treffend voorbeeld, maar ook de cafébrand in Volendam in 2000.

Om incidenten te voorkomen, te beheersen en te begrijpen, is het volgens Merkelbach belangrijk om integraal veiligheids- en beveiligingsbeleid te maken waarin wordt ingezet op preventie. 'Vooruit kijken in plaats van te reageren op incidenten.'

'Stel dat dataverkeer deel uitmaakt van je core business, dan is het verstandig om afspraken met meerdere providers te maken. Een grote storing bij een provider als Vodafone of KPN hoeft dan niet onmiddellijk een groot incident te worden', zegt Merkelbach.

"Vooruit kijken in plaats van te reageren op incidenten."

'Een ander voorbeeld van vooruitdenken is het nemen van preventieve maatregelen in het geval van een griepgolf. Preventief te werk gaan, is er in dit geval bijvoorbeeld voor zorgen dat medewerkers in staat zijn elkaars taken over te nemen en dat er desinfecterende middelen op de werkplek voorhanden zijn.'

Merkelbach: 'Proactief veiligheids- en beveiligingsbeleid is er in tegenstelling tot reactief beleid op gericht het aantal onveilige handelingen en onveilige situaties structureel omlaag te krijgen. Een instelling of bedrijf wacht niet tot een ongeval plaatsvindt (reactief), maar gaat actief aan het werk om incidenten te voorkomen (proactief).'

Incidenten: registreer ze
Goed reageren op incidenten is minstens zo belangrijk als het voorkomen ervan. Incidentenregistratie geeft goed inzicht in wat er daadwerkelijk gebeurt en kan herhaling voorkomen. Ook kunnen op basis van incidentenregistratie tactische maatregelen worden genomen.

Incidentenregistratie wordt in veel branches steeds belangrijker. Het beveiligingsbeleid van scholen bijvoorbeeld steunt steeds vaker op incidentenregistratie waarbij alle medewerkers worden verplicht om afwijkende zaken te rapporteren.

Ook in de rijksmusea is incidentenregistratie verplicht. Alle musea moeten incidenten met de rijkscollectie aan de Erfgoedinspectie melden. Zo kunnen eventuele interventies op tijd worden ingezet en wordt voorkomen dat bedrijfsrisico's en structurele tekortkomingen buiten beeld blijven.

Melden alleen is niet voldoende
Minstens zo belangrijk als het registreren van incidenten vindt Merkelbach het bespreken van incidenten. 'Alleen het melden of het rapporteren van het incident is niet voldoende. Bespreek incidenten op het juiste niveau van de organisatie zodat er ook daadwerkelijk van wordt geleerd en er wat mee wordt gedaan.'

Een goed voorbeeld is een case bij een bedrijf waar een aantal IT-infrastructuurlocaties aan elkaar zijn gekoppeld. Als één locatie uitvalt of als er sabotage plaatsvindt, dan betekent dat vrijwel zeker het faillissement van het bedrijf door de volledige uitval van systemen.
Merkelbach: 'Een van de locaties bleek zo slecht beveiligd, dat de boel gesaboteerd zou kunnen worden zonder dat iemand dat zou merken. Deze informatie werd echter alleen in een operationeel rapport gemeld bij een lokale manager. Onverstandig, want als de manager de risico's niet serieus neemt dan kan dat grote gevolgen hebben. Ook worden er wellicht eerder maatregelen genomen als de directie gelijk op de hoogte wordt gesteld.'

'Beleid wordt vaak pas aangepast op het moment dat een incident bekend is bij de directie of het hoger management', zegt Merkelbach. 'Anderzijds is het – om herhaling te voorkomen – net zo belangrijk dat incidenten worden besproken op de plek waar ze plaatsvinden. Bijvoorbeeld op de werkvloer.'

Incidenten voorkomen en beheersen

- Vergroot inzicht in uw organisatie
- Denk vanuit de core business van uw bedrijf
- Stel risicobronnen vast
- Registreer incidenten
- Bespreek incidenten op het juiste niveau binnen de organisatie

Tips om de veiligheid te vergroten

- **Stel controle in op afgesproken maatregelen / procedures**
  Nodig bijvoorbeeld een collega-bedrijf uit of neem een externe veiligheidspartner in de arm voor een objectief beeld van de veiligheid in uw organisatie.

- **Creëer een veiligheidscultuur onder al het personeel**
  Iedereen dient zich te houden aan de veiligheidsregels. Maak van uw medewerkers ambassadeurs voor veiligheid door het creëren van een veiligheidscultuur.

- **Benoem per kwartaal een of meer veiligheidsthema's**
  Besteed op een leuke manier aandacht aan veiligheid door elke maand één of meer thema's centraal te stellen. Schrijf bijvoorbeeld een extra artikel over het onderwerp in de nieuwsbrief, maak een prijsvraag en laat medewerkers actief meedenken over wat beter kan.

- **Maak werknemers bewust van onveilig gedrag en beloon veilig gedrag**
  Een goed voorbeeld is de clean desk-policy waarbij medewerkers een groene smiley krijgen als ze hun werkplek netjes achterlaten, een rode als dit niet het geval is.

- **Blijf investeren in veiligheidsinstructies. Zorg dat deze up to date zijn**
  Werknemers, bezoekers en leveranciers; iedereen dient de geldende veiligheidsprocedures te kennen. Alleen het afgeven van een blaadje met de geldende regels blijkt vaak onvoldoende. Toon instructievideo's en laat een test maken. Vijftien minuten investeren kan jarenlang leed besparen.