Situation awareness en menselijke fouten

Security is en blijft mensenwerk. Organisaties spenderen jaarlijks miljoenen euro's aan camera's, X-ray apparatuur en bewegingsdetectiesystemen. Toch hebben ze nog altijd mensen nodig om informatie uit al die systemen te interpreteren en een inschatting te maken van het dreigingsniveau. Maar wat bedoelen we precies als we het hebben over 'mensenwerk', en hoe zorg je ervoor dat securityprofessionals hun werkzaamheden optimaal uitvoeren en zo min mogelijk fouten maken? Paul Hulshof *

Tachtig tot negentig procent van de security-incidenten is toe te schrijven aan menselijke fouten, zo blijkt uit een recent artikel van *Melcher Zeilstra* (2011). Dat komt meestal niet doordat securityprofessionals te weinig kennis en inzicht hebben in potentiële dreigingen – integendeel, ze zijn meestal voldoende veiligheidsbewust. Het probleem ontstaat doordat ze niet altijd alert reageren op de momenten die er echt toe doen.

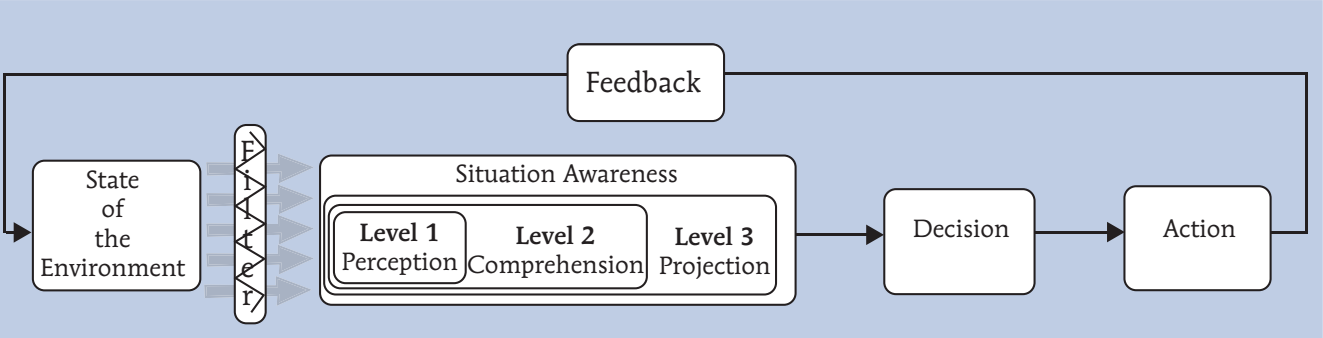
Creëren van alertheid

Een analyse van de *situation awareness* maakt duidelijk hoe mensen keuzes maken bij het uitvoeren van complexe taken. Daaruit blijkt dat de mate van alertheid afhangt van verschillende factoren. Onderzoeker Endsley onderzocht hoe gevechtspiloten in complexe omstandigheden informatie verwerken, beslissingen nemen en tot actie overgaan en ontwikkelde een theoretisch model dat in drie stappen verloopt. Ook securityprofessionals doorlopen dagelijks dit proces.

De eerste fase (*perception*) is die van het waarnemen. Securitypersoneel op bijvoorbeeld een luchthaven is opgeleid en getraind om met hun zintuigen en met behulp van apparatuur de omgeving te scannen op mogelijke security-risico's. De kwaliteit van de waarneming hangt onder meer af van de ervaring en competenties van de desbetreffende persoon. Een goede waarnemer heeft alleen aandacht voor prikkels die van belang zijn voor zijn taak en schenkt geen aandacht aan prikkels die er niet toe doen. Van securityprofessionals verwachten we als het ware een automatische filter, die voorkomt dat zij tijdens hun werk worden overladen met prikkels die de uitvoering van werkzaamheden kunnen verstoren: aandacht voor het weer, de kleur van de muren of een aantrekkelijke voorbijgangster.

In de tweede fase (*comprehension*) wordt een waargenomen prikkel beoordeeld. De waarnemingen worden gecombineerd met eerdere ervaringen en kennis. Een securityprofessional ziet bijvoorbeeld een groepje mannen staan bij de ingang van het gebouw en herkent één van hen als notoire insluiper. Hij koppelt de kennis uit het verleden aan de waarneming van het moment.

De derde fase (*projection*) draait om vooruit denken en het beoordelen hoe concreet een dreiging is. De security- »



Het proces van situation awareness.

professional maakt in deze fase een inschatting van de ernst van de situatie, de kans dat er ook daadwerkelijk iets gaat gebeuren en de verschillende manieren waarop hij kan acteren. Uiteindelijk leidt dit tot een besluit om op een bepaalde manier op te treden. Of juist niet.

Kortom, de mate van alertheid van securityprofessionals wordt niet alleen bepaald door het aantal uren nachtrust, de kennis of de ervaring die iemand heeft. Het is een ingewikkeld proces dat bestaat uit waarneming, beoordeling en projectie. In dit proces kunnen verschillende fouten sluipen. Maar wat voor soort fouten zijn dat? Ook daarvoor is een model gemaakt.

Niet elke menselijke fout is hetzelfde

Knowledge based

Menselijke fouten kunnen grofweg ingedeeld worden in drie verschillende groepen. Ten eerste zijn er de zogenaamde *knowledge based mistakes*. Daarvan spreken we als iemand in een bepaalde situatie niet de juiste kennis en ervaring heeft om een goede inschatting te maken. Dit soort fouten komen veel voor onder beginnende securityprofessionals. Medewerkers met veel ervaring maken deze fouten nauwelijks, omdat zij veel handelingen en denkprocessen vrijwel geheel op de automatische piloot uitvoeren. Je kunt zeggen dat ze hun 'werkgeheugen' nauwelijks hoeven te gebruiken en daardoor veel aandacht overhouden voor wat er op het moment zelf gebeurt. Ervaren politiemensen kunnen zich tijdens hun optreden in een uitgaansgebied gemakkelijker afsluiten van opmerkingen van omstanders, waardoor hun aandacht gericht blijft op een groep verdachten. De minder ervaren agent heeft de neiging omgevingsprikkels te verwerken, waardoor hij eerder verrast wordt door plotselinge agressie van een verdachte.

Rule based

Stel, we gaan alle securityprofessionals nog meer trainen en opleiden op de werkvloer zodat ze ervaring opdoen. Zijn we er dan? Nee, want niet alleen onervaren mensen maken fouten. Ook securityprofessionals met meer ervaring kunnen de fout ingaan. Dan is sprake van een *rule based mistake*. Iemand neemt een beslissing gebaseerd op de verkeerde informatie of op eerdere ervaringen, terwijl het betreffende geval afwijkt van de situatie uit het verleden (of uit de opleiding). Zo is luchthavenpersoneel gewend om tassen van verdachte personen te openen voor controle, bijvoorbeeld omdat ze hopen dat de verdachte daardoor gedrag vertoont wat aanleiding is voor aanvullend onderzoek. Maar een tas openmaken is niet in álle gevallen de beste methode: het zou ook kunnen leiden tot het activeren van een bom.

Skill based

Stel dat een securityprofessional zijn opleiding netjes heeft gevolgd en afgerond, stage heeft gelopen op de werkvloer en weet dat het opentrekken van een tas een veiligheidsrisico met zich meebrengt. Gaat dan alles altijd goed? Nee, want mensen zijn geen voorgeprogrammeerde robots en worden beïnvloed door menselijke driften, behoeften en emoties waardoor tóch fouten kunnen ontstaan. Dit soort fouten noemen we de *skill based slips or lapses*. Dat zijn fouten die gemaakt worden tijdens de routinematige uitvoering van werkzaamheden, waarbij sprake is van een vergissing of geheugenfout. Een beveiliger is de avond voor zijn werkzaamheden naar een feest geweest, staat later op dan gepland, wijkt af van zijn dagelijkse routine en vergeet een belangrijk alarmsysteem in te schakelen. Geen enkele persoon zal te allen tijde foutloos werk uitvoeren.

Kortom, als gevolg van verschillende soorten menselijke fouten kunnen securityprofessionals in een specifieke situatie onvoldoende alert reageren. Grote vraag is natuurlijk hoe je dit soort fouten kunt beperken. Daarvoor is inzicht nodig in de achterliggende oorzaken.

Investeren in motivatie en werksfeer zou meer kunnen opleveren dan nóg een technische innovatie

Een voorbeeld uit de praktijk: Amsterdam Airport Schiphol

Op Schiphol worden allerlei maatregelen getroffen die de alertheid van het personeel verder moet vergroten. Personeel volgt jaarlijks en op verschillende momenten trainingen en er worden dagelijks testen uitgevoerd om te controleren of securitypersoneel alert is op potentiële dreigingen. Daarnaast wordt geprobeerd om het personeel zo veel mogelijk afwisselende werkzaamheden te laten verrichten. Het ene moment kijken medewerkers naar camerabeelden en het andere moment surveilleren zij in de terminal en praten zij met reizigers. Binnen het management is men overtuigd van het feit dat het op een goede manier inrichten van een werkomgeving doorslaggevend is voor de motivatie en kwaliteit van werkzaamheden. Hoe professioneler de omgeving eruit ziet, hoe professioneler de medewerkers zich gedragen. Dat betekent een mooi, schoon en professioneel uitziende werkplek. Ook wordt kritisch gekeken of de pauzeplekken van personeel dichtbij cateringlocaties liggen om te voorkomen dat de helft van de pauzetijd verloren gaat aan het wandelen van de werkplek naar een plek om te eten en drinken. Het is van belang een werkcultuur te creëren waarbinnen medewerkers zonder enige barrière bij hun leidinggevenden kunnen aangeven wanneer zij niet goed in hun vel zitten.

Niet alleen individuen

Veel mensen veronderstellen dat menselijke fouten alleen worden gemaakt door incapabel personeel: mensen die door onkunde, vergeetachtigheid, onoplettendheid, slechte motivatie, nalatigheid of onvoorzichtigheid fouten maken. In de wetenschap over menselijke fouten heet dit '*the just world hypothesis*', het idee dat slechte mensen hun werk op een slechte manier uitvoeren en dat daar weinig aan te veranderen is.

Deze theorie geeft een te simpel beeld van de werkelijkheid. Iedereen – zelfs de best gemotiveerde, opgeleide en capabele medewerker - kan fouten maken. Menselijke fouten ontstaan namelijk nooit zomaar: ze zijn vaak het gevolg van de interactie tussen de mens en de (werk)omgeving. Om het aantal menselijke fouten in security te beperken moet de nadruk niet alleen liggen op het ontwikkelen van kwaliteiten van *individuen* door opleiding, training en versterken van competenties.

Menselijke fouten kunnen ook worden beperkt door kritisch te kijken naar de situationele en organisatorische factoren, zoals de drukte en hectiek op een bepaalde plek, de fysieke en mentale belasting van het werk, toezicht op de kwaliteit van de werkzaamheden, de beloning en bestraffing van goed respectievelijk slecht presterend personeel, de manier waarop roosters worden ingedeeld, de waardering voor het werk, enzovoort.

Een werkgever op een vliegveld maakt het zichzelf en zijn personeel een stuk makkelijker menselijke fouten te voorkomen door de passagiersstromen op drukke momenten te verdelen over tien securityfilters in plaats van over vijf. De werkdruk per beveiliger neemt af en daardoor verbetert de kwaliteit van het werk direct.

Dat heeft niets te maken met de opleiding of training van elke afzonderlijke beveiliger, maar met de externe factor werkdruk. Dit geldt ook voor alle andere voornoemde factoren. Je kunt securityprofessionals laten bloeien in de juiste omgeving, maar diezelfde mensen kunnen onder slechte omstandigheden allemaal veranderen in incapabele werknemers.

Zorg voor een menselijke omgeving

Als ik zeg dat security mensenwerk is, dan bedoel ik dat securityprofessionals minder fouten maken in een werkomgeving waar nadrukkelijk rekening wordt gehouden met menselijke behoeften, neigingen en wensen. Hoewel er binnen de security-industrie een sterke nadruk ligt op technologische innovaties, blijven securityprofessionals de essentiële schakel in het veiligheidsbeleid. Daarom zou iedere security manager bij het opstellen van het beleid nadrukkelijk rekening moeten houden met de menselijke kant van security. Investeren in motivatie, waardering en werksfeer zou wel eens meer kunnen opleveren dan nóg een technische innovatie. «

* *Paul Hulshof is senior adviseur op het gebied van criminaliteit en veiligheid bij onderzoeks- en adviesbureau DSP-groep.*

Met dank aan Raymond Pronk, operationeel Manager Airport Security Safety & Support op Rotterdam/The Hague Airport en David van der Meer, Aviation Security Manager op Amsterdam Airport Schiphol.

Meer lezen?

- Hulshof, P. (2012), Awareness van security personeel - Hoe creëer je awareness en hoe houd je het vast in complexe situaties?, Amsterdam: DSP-groep BV
- Zeilstra, M. (2011), De mens als asset in een systeem - Beschouwing op de bijdrage van de mens aan de veiligheid van een systeem, Utrecht: Intergo BV
- Steden, R. van (2007), Privatizing policing: describing and explaining the growth of private security, Den Haag: Boom Juridische Uitgevers.
- Orshesky, C.M. (2003), Beyond technology – the human factor in business systems, in: journal of business strategy, vol 24 no. 4 pp. 43-47
- Parsons, K. McCormac, A. , Butavicius, M. en Ferguson, L. (2010), Human Factors and Information Security: Individual, Culture and Security Environment, Edinburgh: Defence Science and Technology Organisation
- Wilson, M. en Hash, J. (2003), Building an Information Technology Security Awareness and Training Program, Gaithersburg: National Institute of Standards and Technology
- Kraemer, S. en Carayon, P. (2006), Human errors and violations in computer and information security: the viewpoint of network administrators and security specialists, in: Journal of computer science and security, volume 38, issue 2, March 2007, pp.143-154
- Harris, D.H. (2002), How to really improve airport security, in: Ergonomics and design, winter 2002, pp. 17-22
- Talbot, J. & Jakeman, M., (2008). Security Risk Management Body of Knowledge. Risk Management Institution af Australasia Limited, Carlton South.
- Rasmussen, J. (1982), Human error – a taxonomy for describing human malfunction in industrial installations, in: journal of occupational accidents no. 4, pp.311-333.
- Endsley, M.R. en Garland, D.J. (2000), Situation awareness analysis and measurment, New York: Lawrence Erlbaum Associates
- Busse, D.K., Johnson, C.W. (1998), Using a Cognitive Theoretical Framework to Support Accident Analysis, Glasgow: University of Glasgow, dept. of computing science
- Warm, J.S., Parasuraman, R. en Mathhews, G. (2008), Vigilance requires hard mental work and is stressful, in: Human factors, the journal of the human factors and ergonomics society, june 2008, pp. 433-441
- Reason, J. (2000), human errors – models and management, Manchester: University of Manchester