den. Of zij de bedoelde beveiligingsexperts zijn laat zich nu nog raden. Bij de nadere invulling van dit begrip lijkt een belangrijke rol voor de VBN weggelegd.

PREVENTIE EN REPRESSIE

Gaat het bij beveiliging en bewaking na een incident meestal om de repressieve aandachtspunten, bij een langer voortdurende dreiging lijkt het logisch dat de overheid meer aandacht zal schenken aan de preventieve kanten van beveiligingszorg.

De kans bestaat dat geen enkele instantie in staat is om gedurende zeer lange tijd een hoog bewakingsniveau te garanderen, noch qua capaciteit noch qua kosten hiervan. Meer aandacht voor preventie lijkt dan een betaalbare en minstens even veilige oplossing.

De brief van de minister aan de Tweede Kamer geeft hier echter geen uitsluitsel over.

Verder wordt in de evaluatie nog stilgestaan bij de wens van de CBB om vaste locaties te gebruiken voor grootschalige evenementen zodat er niet voor ieder evenement een nieuw beveiligingsdraaiboek hoeft te worden gemaakt, denkt men na over een basisbeveiligingsniveau voor departementsgebouwen en gebouwen van internationale organisaties en last but not least wordt nog een voornemen geïntroduceerd om veiligheidsverkenningen uit te voeren op beveiligde objecten. Met name over dit laatste, ongetwijfeld zeer gevoelig liggende onderwerp, zal heel goed gecommuniceerd moeten worden met de diverse belangendragers.

Met de komst van het Stelsel Bewaken en Beveiliging in 2004 is al een grote en noodzakelijke verbeterslag gemaakt met de professionalisering van de beveiliging van ernstig bedreigde personen, objecten en diensten. Met de laatste evaluatie is het Stelsel over de kinderziekten heen gegroeid en is hard op weg naar een volwassen instrument. Nu is de tijd gekomen om over de schutting van het publieke domein te kijken en de samenwerking met de private partijen te zoeken.

De kans bestaat dat geen enkele instantie in staat is om gedurende zeer lange tijd een hoog bewakingsniveau te garanderen, noch qua capaciteit noch qua kosten hiervan.

Feelings are facts

Ronald Eygendaal

Dit artikel gaat over de bewustwording van u als security manager en de uitstraling van de security manager op de werkomgeving. Vergeet niet dat u als security manager door anderen binnen het bedrijf als lastig en vervelend wordt ervaren. U bent het immers die lastige, vervelende en niet-werkbare regeltjes bedenkt en oplegt, althans dat vinden anderen van u. Daarnaast heeft u als security manager een voorbeeldfunctie binnen het bedrijf. Veel Security managers zijn zich vaak van bovenstaande 'feelings' niet bewust waardoor de boodschap die zij verkondigen niet goed overkomt. Voorkomen moet worden dat 'feelings are facts' scenario's ontstaan, dit versterkt immers het niet goed overkomen van de boodschap.

MAIL, WORD EN EXCEL

Ook bij u op kantoor hebben veel mensen de beschikking over een PC op hun werkplek.

Deze PC's zijn ingericht met de software die de mensen nodig hebben bij hun werk. Hierbij moet worden gedacht aan softwarepakketten zoals Windows, Microsoft Office, Microsoft Outlook vaak aangevuld met basale security software zoals antivirus software, een firewall en spyware killers. Het actueel houden van de software op uw PC gebeurt in de regel volledig automatisch.

Als security manager heeft u, net als anderen binnen uw organisatie, ook een PC op uw bureau staan. Wees u er van bewust dat, mits u geen maatregelen neemt, het voor een systeembeheerder vrij eenvoudig is om de informatie op uw PC te bekijken en uw e-mail te onderscheppen. Daar waar u gebruik maakt van Microsoft Office onderdelen zoals MS Word documenten of Excel sheets loopt u een extra risico. Hierover later meer.

Wees er van bewust dat, mits u geen maatregelen neemt, het voor een systeem-beheerder vrij eenvoudig is om de informatie op uw PC te bekijken en uw e-mail te onderscheppen.

Gelukkig hebben Microsoft Office en Microsoft Outlook talloze beveiligingsopties welke voor u als security manager aan moeten staan. Zo is het mogelijk om met behulp van Outlook e-mails te coderen en digitaal te ondertekenen. Waardoor 'meelezen' en manipulatie onmogelijk wordt. Hiervoor moet Outlook worden voorzien van een zogenaamd X509 beveiligingscertificaat. Wanneer dit gebeurd is, krijgt u een tweetal extra knoppen in Outlook. Een knop voor de handtekening en een knop voor het coderen van berichten. Als u gecodeerde berichten via internet wilt verzenden, moet u eerst een certificaat met de geadresseerde uitwisselen.

U verzendt een digitaal ondertekend bericht naar diegene waarmee u gecodeerde berichten wilt uitwisselen. De geadresseerde voegt uw e-mailnaam aan zijn of haar contactpersonen toe en voegt daarmee ook uw certificaat toe. Vervolgens kunt u gecodeerde berichten uitwisselen. Eenvoudiger en gebruiksvriendelijker kan bijna niet.

Laat u zich als security manager niet gek maken over alternatieven zoals PGP. Dit soort software is voor uw IT-afdeling lastiger te beheren dan een certificaat in Outlook. Ook qua 'sterkte' van de beveiliging doet de oplossing met een certificaat in Outlook niet onder voor PGP. Het gebruik van PGP is gebruiksonvriendelijker dan Outlook, en u moet er mee werken!! Nogmaals, Microsoft Outlook kan functioneel hetzelfde als PGP. Het is dus onzinnig om een programma als PGP hiervoor te gebruiken.

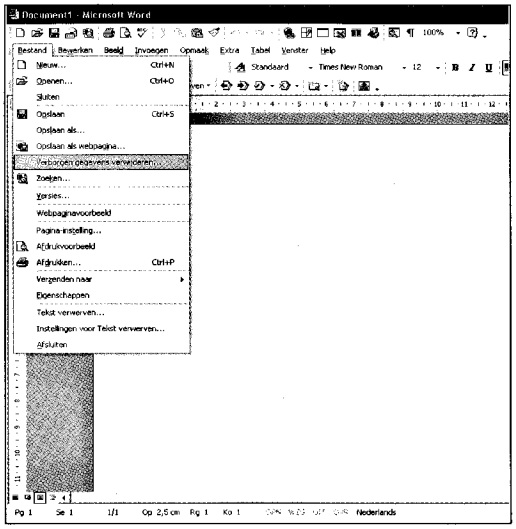
Bij het creëren van MS Word documenten en MS Excel sheets ontstaan zichtbare en onzichtbare gegevens. Het verwijderen van zichtbare gegevens hoeft in de praktijk weinig problemen op te leveren: u ziet immers wat u doet. De onzichtbare gegevens kunnen eenvoudig zichtbaar gemaakt worden. Echter verwijdering van deze gegevens is een probleem.

Dit ondervond de Britse premier Tony Blair in februari 2003 met een dossier over Irak. De verborgen gegevens vertelden namelijk een heel ander verhaal dan Blair...

In de verborgen data, ook wel metadata genoemd, worden onder meer de namen van alle auteurs die ooit aan het document werkten bewaard, net als de bedrijfsnaam, de verschillende bestandsnamen waaronder het document opgeslagen werd en de naam van de computer waarop het document werd gemaakt. Ook verborgen teksten en commentaren worden in de metadata bewaard. Wie de functie Track Changes gebuikt bewaart bovendien alle vorige versies van de tekst in hetzelfde bestand, ook al zijn deze niet meteen zichtbaar in Word. Hieronder een overzicht van alle onzichtbare metagegevens:

- Commentaren
- Eerdere auteurs en editors
- Gebruikersnaam
- Persoonlijke informatie, zoals te vinden onder Bestand >> Eigenschappen
- E-mail koppen
- Scenario commentaren
- Revisiemarkeringen

- Verwijderde woorden en tekstfragmenten
- Vorige versies en afgelegde routes
- Beschrijvingen en commentaar m.b.t. VBA-macros
- Het ID-nummer wordt gereset.



Sedert juli 2004 heeft Microsoft een gratis tool (remove hidden data) beschikbaar gesteld, waarmee de onzichtbare gegevens effectief verwijderd kunnen worden. Na het installeren van deze tool ontstaat er zowel binnen MS Word als binnen Excel een extra menu keuze met de naam 'Remove Hidden Data...'.

Outlook met X509 beveiligingscertificaat en het tool remove hidden data zijn vrij eenvoudig in uw kantoor PC aan te brengen. Het is een kwestie van downloaden en installeren. Er kan niet veel fout gaan.

Deze twee opties zijn een must-have voor elke security manager en geven een professionele uitstraling aan uw digitale werkomgeving.

PASSWORDS EN SCREENSAVERS

Een password dient om toegang te krijgen tot een netwerk, een programma of een bestand. Het mag als vanzelfsprekend worden verondersteld dat u als security manager gebruik maakt van een sterk wachtwoord op de PC. Een sterk password is tenminste 8 karakters lang. Het password bevat ten minste een getal, hoofdletters en kleine letters in willekeurige volgorde. Ook de houdbaarheid van passwords moet worden beperkt. Verval als security manager niet in de fout uw password op een onveilige manier te bewaren.

Wees u er van bewust dat er altijd mensen op jacht zijn naar de security manager, vroeg of laat pakken ze u!!

Vroeger werden screensavers gebruikt om het inbranden van een beeldscherm te voorkomen. Tegenwoordig kan een screensaver worden gezien als een nuttig stukje beveiliging. Een screensaver moet effectief zo worden ingesteld dat binnen een paar minuten na het stoppen van toetsenbordactiviteiten de screensaver aanspringt. Hierdoor wordt de PC gelockt. Wanneer men de PC opnieuw wil gebruiken dan zal de gebruiker zijn password moeten ingeven.

Bedenk dat de tijd die nodig is voor 'even koffie halen' voldoende is om scherminformatie, van een PC zonder screensaver, buit te maken. De meeste screensavers zijn ook via een menu in te schakelen. Dit menu krijgt u bij het gelijktijdig indrukken van CRTL+Alt+DEL. U krijgt dan een aantal opties, via de optie 'Lock computer ' schakelt u de screensaver met de passwordbeveiliging in. Het gebruik van een screensaver geeft een professionele indruk als even uw kamer uit rent om 'koffie te halen' voor een bezoeker of een collega.

KAMER VERSUS KANTOORTUIN

In veel moderne kantoorpanden zijn de kamers gemaakt van prefab wandjes met een slechte geluidsisolatie. Hierdoor is het goed mogelijk om in de kamer naast u te horen wat er in uw kamer besproken wordt. Als security manager gaat u om met vertrouwelijke en vaak privacygevoelige informatie. sWanneer u gehuisvest bent in een dergelijke kamer, moet u zich er van bewust zijn dat u zeer eenvoudig en zonder technische hulpmiddelen afgeluisterd kan worden.

Vanwege allerlei, soms wettelijke, criteria zijn kamers in moderne kantoorpanden voorzien van een smalle strook glas tussen de kamer en de gang. Hierdoor is het mogelijk dat er vanuit de gang van het kantoorpand de kamer in wordt gekeken. De gedachte achter deze inkijk is dat door de inkijk de sociale controle in kantoren wordt verbeterd en de kans op ongewenste intimiteiten afneemt.

Deze gedachte moet u als security manager aanspreken. Echter in bepaalde situaties, bijvoorbeeld tijdens een onderzoeksinterview, kan de inkijk voor de nodig problemen zorgen. (bijvoorbeeld in het roddelcircuit: Ik zag dat die en die laatst bij de security manager zat, zou hij wat met die diefstallen te maken hebben??). De inkijk in de kamer kan dus zorgen voor 'feelings are facts' situaties, wees u er van bewust en laat het raam mat afplakken. Informeer hier uw ondernemingsraad over. Ervaring leert dat deze nog wel eens moeilijk doen over het afplakken van het raam.

In mijn dagelijkse praktijk kom ik regelmatig security managers tegen die 'gehuisvest' zijn in een kan-

Bedenk dat de tijd die nodig is voor 'even koffie halen' voldoende is om scherm-informatie, van een PC zonder screensaver, buit te maken.

toortuin van een afdeling IT of de afdeling facilities. Als argument hoor ik dan dat de security manager tussen de mensen wil zitten. De waarheid is vaak anders, in de meeste gevallen vindt de baas van de security manager dat zijn security manager best in een kantoortuin kan zitten, een eigen kamer is alleen voor de directieleden. Dat dit een zeer slechte manier van huisvesten is, lijkt mij duidelijk. Security managers gaan immers om met gevoelige informatie welke niet zomaar door een kantoortuin mag slingeren. Vergeet niet dat een werkplek in een kantoortuin anderen in uw professionele werkomgeving opvalt en dat deze personen daardoor geen vertrouwelijke informatie met u als security manager willen delen. (Als u in een soortgelijke situatie zit dan kunt u overwegen uw baas te informeren dat u niet meer in kunt staan voor geheimhouding. Geheimhouding in een kantoortuin is onmogelijk!!!).

Bedenk dat een kantoortuin altijd oortjes heeft. Je zou kunnen stellen dat je een waardeoordeel over de graad van beveiliging van een organisatie kunt geven door te kijken naar de huisvesting van de security manager.

Bedenk dat een kantoortuin altijd oortjes heeft. Je zou kunnen stellen dat; je een waardeoordeel over de graad van beveiliging van een organisatie kunt geven door te kijken naar de huisvesting van de security manager.

CLEANDESK EN SCHOONMAKEN

Door de groeiende stroom aan informatie is het voor veel security managers een probleem om de werkplek opgeruimd te houden. Dossiers hebben vaak nog een juridische nasleep en moeten dus bewaard blijven en aparte security archieven zijn er in de meeste bedrijven niet.

U moet er op bedacht zijn dat er ook binnen uw organisatie altijd mensen zijn die even op uw bureau kijken.

Zit u in een kantoortuin dan is opruimen en uw spullen in een goed afsluitbare kast opbergen de oplossing. Deel geen kasten met anderen want dat is vragen om ellende.

In een aantal gevallen kan een eigen afsluitbare kamer een oplossing zijn. Echter, bedenk dat de kamer ook schoongemaakt moet worden dat vaak in de avonduren gebeurt. Tijdens de schoonmaak ontstaan prima gelegenheden voor ongewenst gluren. Maak dus afspraken met de schoonmaker dat deze overdag tijdens uw aanwezigheid komt. Houd toezicht wanneer uw kamer wordt schoongemaakt en loop vooral niet weg. Denk ook aan uw afval, laat een goede papiervernietiger plaatsen en gebruik deze. En goede papiervernietiger voldoet tenminste aan DIN 32757 klasse 3 of hoger.

Hoe geloofwaardig is een security manager die zich niet aan zijn eigen cleandesk beleid houdt?

HOERA EEN LAPTOP!!!

Als u als security manager de gelukkige bezitter bent van een laptop dan heeft u er een serieus security probleem bij. Naast de digitale gevaren die ook gelden voor een desktop, loopt u een verhoogde kans op fysieke diefstal van de laptop. Hierover later meer.

Naast de maatregelen zoals eerder beschreven in dit artikel, moet u nog iets doen aan encryptie van de harde schijf zodat het in geval van diefstal onmogelijk is om de op de harde schijf aanwezig informatie te gebruiken c.q. te misbruiken. U herinnert zich vast en zeker nog wel de commotie over de vermiste laptops van Shell en AIVD. Respectievelijk uit de trein en uit een auto gestolen. Als dit u als security manager overkomt dan heeft u een serieus imagoprobleem binnen uw organisatie. Zorg er dus voor dat de data op de harde schijf encrypted is opgeslagen op de schijf. Helaas heeft Microsoft hier niet een pasklare oplossing voor en zult u software moeten kopen.

Uit bestudering van incidentenrapportages blijkt dat laptops vaak onbewaakt in het zicht in de auto blijven liggen. U (her)kent het wel, even snel parkeren om iets te halen en de laptop in de auto laten liggen en foetsie is de laptop. Juist in dit soort situaties vinden diefstallen van laptops uit auto's plaats.

Voor de auto zijn overigens uitstekende laptopkluizen verkrijgbaar. Zorg dat u er één in de auto krijgt en gebruik deze kluis. De juiste preventieve maatregelen nemen en goed op uw spullen letten en nadenken is het motto.

BEKEND EN ONBEKEND

Badges om toegang te krijgen tot een gebouw is gemeengoed geworden, veel gerespecteerde bedrijven gebruiken een toegangsbadge. In veel bedrijven geldt een draagplicht van de toegangsbadge. Iedereen is verplicht zijn badge zichtbaar te dragen. Bezoekers mogen vaak niet zonder begeleiding in de gebouwen rondlopen.

Het zichtbaar dragen van uw toegangsbadge en het begeleiden van uw bezoekers naar buiten zijn handelingen waarmee u scoort als security manager.

Als security consultant overkomt het me regelmatig dat ik na een afspraak met een security manager aan mijn lot wordt overgelaten in een gebouw. Ik moet dan zelf maar de uitgang vinden. Ook bezoekers van de directie worden vaak niet begeleid naar de uitgang. Het kost immers tijd en we hebben het al zo druk, zo luiden de argumenten.

CONCLUSIE

Bedenk dat goed voorbeeld goed doet volgen, let op uw baas!!! Spreek uw baas er op aan wanneer hij de regels overtreedt, ook uw baas behoort met dit soort zichtbare zaken het goede voorbeeld te geven. Maak uw baas er op attent dat een slechte security doorstraalt in het imago van het bedrijf.

Het is van belang dat u als security manager en uw baas zich er van bewust is dat de werkomgeving veel ziet van security en de uitvoering van de security maatregelen. Ook klanten en partners in business zien heel veel van uw security. Juist dit 'zien' beïnvloedt de 'feelings' over een bedrijf. Waak er voor dat 'bad feelings' facts worden.

Ook bezoekers van de directie worden vaak niet begeleid naar de uitgang. Het kost immers tijd en we hebben het al zo druk, zo luiden de argumenten.

Identiteitsfraude: de criminaliteit van de toekomst

Flevum Forum Network/ Bart van Ratingen

Sinds de jaren negentig is een nieuw soort criminaliteit in opkomst: het stelen en misbruiken van andermans identiteit. Identiteitsfraude is geruisloos, onzichtbaar, erg moeilijk te onderzoeken en verbazingwekkend simpel uit te voeren. Identiteitsfraude is de snelst groeiende vorm van criminaliteit in en buiten Europa en aangenomen mag worden dat de schadelast de komende jaren spectaculair zal gaan stijgen. Rob van Dijk van adviesbureau Cocoon Riskmanagement BV geeft enkele praktische tips om identiteitsfraude tegen te gaan.

Eerst maar eens wat cijfers. Identiteitsfraude – lees: het stelen van persoonlijke informatie met het doel deze te misbruiken voor financieel gewin - kost het Verenigd Koninkrijk nu al bijna twee miljard euro per jaar. In de VS berekende men voor de jaren 1998 tot 2003 al een totale schadelast van zo'n 53 miljard dollar, waarvan 48 miljard dollar voor rekening van het bedrijfsleven kwam. Voor Nederland zijn geen exacte cijfers bekend, maar aangenomen mag worden dat misbruik van identiteitsbepalende gegevens ook hier tot grote schade voor het bedrijfsleven leidt.