Stichting NIOC en de NIOC kennisbank

Stichting NIOC (www.nioc.nl) stelt zich conform zijn statuten tot doel: het realiseren van congressen over informatica onderwijs en voorts al hetgeen met een en ander rechtstreeks of zijdelings verband houdt of daartoe bevorderlijk kan zijn, alles in de ruimste zin des woords.

De stichting NIOC neemt de archivering van de resultaten van de congressen voor zijn rekening. De website www.nioc.nl ontsluit onder "Eerdere congressen" de gearchiveerde websites van eerdere congressen. De vele afzonderlijke congresbijdragen zijn opgenomen in een kennisbank die via dezelfde website onder "NIOC kennisbank" ontsloten wordt.

Op dit moment bevat de NIOC kennisbank alle bijdragen, incl. die van het laatste congres (NIOC2023, gehouden op donderdag 30 maart 2023 jl. en georganiseerd door NHL Stenden Hogeschool). Bij elkaar bijna 1500 bijdragen!

We roepen je op, na het lezen van het document dat door jou is gedownload, de auteur(s) feedback te geven. Dit kan door je te registreren als gebruiker van de NIOC kennisbank. Na registratie krijg je bericht hoe in te loggen op de NIOC kennisbank.

Het eerstvolgende NIOC vindt plaats op donderdag 27 maart 2025 in Zwolle en wordt dan georganiseerd door Hogeschool Windesheim. Kijk op www.nioc2025.nl voor meer informatie.

Wil je op de hoogte blijven van de ontwikkeling rond Stichting NIOC en de NIOC kennisbank, schrijf je dan in op de nieuwsbrief via

www.nioc.nl/nioc-kennisbank/aanmelden nieuwsbrief

Reacties over de NIOC kennisbank en de inhoud daarvan kun je richten aan de beheerder:

R. Smedinga kennisbank@nioc.nl.

Vermeld bij reacties jouw naam en telefoonnummer voor nader contact.

Risicofactor Mens bij informatiebeveiliging

Stephen E. Querido - Academie voor ICT&Media / De Haagse Hogeschool

Stephen Querido

Bij informatiebeveiliging denken we vaak in eerste instantie aan het technisch beveiligen van systemen. We komen dan op toegangscontrole, wachtwoorden, intranetbeveiliging, autorisaties, beveiligde mainframe-ruimtes, etc. Toch vinden op dat terrein veel minder ongelukken plaats dan bij de schakel mens in dit ver-haal. Onderzoeksbureaus zoals Gartner, leren ons dat ca. 80% van fouten bij informatiebeveiliging worden veroorzaakt door verkeerd of niet handelen. 6% van de incidenten zijn bewust onrechtmatige acties. 66% van de beveiligingsproblemen wordt veroorzaakt door eigen medewerkers. In dit artikel wordt een schets gegeven van verschillende (inter-)persoonlijke processen, die niet in het voordeel van Informatiebeveiliging werken.

Keywords

informatiebeveiliging, risico, bewustwording, mentaliteits-verandering, security management, bedrijfscultuur.

Het beveiligen van informatie; waar hebben we het over?

Als we informatie beschouwen als betekenisvolle gegevens, en beveiliging daarvan als een set van technische en niet technische maatregelen om te voorkomen dat informatie in verkeerde handen komt, aan integriteit inboet of niet meer kan stromen, dan hebben we het kader te pakken. Het is handig om hier geen onderscheid te maken tussen digitale informatie en bij voorbeeld papier. Immers, wij printen veel zaken uit en digitaliseren teksten en plaatjes. Een bekend voorbeeld is een plakkertje met het wachtwoord op de computer; hiermee wordt als het ware een sleutel open en bloot neergelegd.

Zijn we bewust of onbewust nalatig?

Bewustwording is een sleutelbegrip bij de huidige beveiligingsproblematiek. Naast de medewerker dient juist het management zich meer van haar verantwoordelijkheid bewust te zijn. We kunnen stellen, dat de meeste mensen niet bewust nalatig zijn of kwade bedoelingen hebben. Als niemand vertelt wat er gebeurt bij overbelasting van een server, gaan ze rustig filmpjes downloaden. En dan nog; het is erg verleidelijk te denken dat toch niet veel mensen dat doen, dus die van mij kan wel. Pas als de server uitvalt, gaan we morren.

We hebben ook de neiging risico's verkeerd in te schatten. 'Het zal zo'n vaart niet lopen.' Dat lijkt iets van onze cultuur. We doen een boodschapper liever af als een nar. Managers kunnen bewust een ingecalculeerd risico willen lopen. De kosten van de beveiliging wegen niet op tegen het geringe aantal incidenten of men schat de gevolgen in als aanvaardbaar. Het op een site plaatsen van bepaalde informatie kan -nog los van privacyissues- een veiligheidsrisico voor individuele medewerkers of het hele bedrijf tot gevolg hebben. Het scheelt al een slok op een borrel, wanneer mensen snappen waarom er een regel of richtlijn is, en wat mogelijke consequenties zijn van het niet naleven ervan. Er is weinig gepubliceerd over de invloed van de werksfeer op informatiebeveiliging of de verschillen in bedrijfscultuur tussen branches. Van huis uit is men in het bankwezen voorzichtiger dan bij maatschappelijke organisaties. Hierin komt langzaamaan verandering. Niet in de laatste plaats door Wet- en regelgeving en incidenten.

De verleiding weerstaan

We laten ons graag verleiden. Sowieso tot het negeren van voorschriften. Interne drijfveren daarvoor zijn bijvoorbeeld: het gevoel boven de Wet te kunnen staan, 'more equal' te zijn dan anderen (in Huxley's termen), de spanning te voelen van het in overtreding zijn en het al dan niet betrapt worden. Maar ook minder onverantwoordelijke beweegredenen zijn ons niet vreemd: 'die website zag er betrouwbaar uit', 'op die site stond een linkje met gratis wallpapers', 'ik las toevallig de mail van m'n collega, die z'n systeem niet gelocked had', 'een kennis vroeg een bericht over een heel kwaadaardig virus door te sturen naar al mijn contactpersonen'. Wie al eens een computercrash heeft gehad en een dag of meer (naast alle eigen documenten, instellingen, mailtjes en adressenboek) kwijt was aan een hersteloperatie, zal waarschijnlijk beter opletten.

Onlangs deed een Engelse beveiligingsexpert een onderzoek naar het effect van waarschuwingen op een site. Op zijn site plaatste hij een waarschuwing in de trant van 'hier niet klikken; verdachte link'. U raadt het al; binnen korte tijd kon hij ruim 400 bezoekers registeren, die ondanks de waarschuwing (misschien juist daardoor) de verleiding niet konden weerstaan. Fout is lekker!

Bevoegd of onbevoegd?

Wie kwaad wil, kan via het internet stukjes informatie eenvoudig aan elkaar koppelen en analyseren; wat de AIVD kan, kunt u ook! Zo zijn de digitale sociale netwerken een rijke bron van informatie. Is het verstandig om netwerkende (meestal hoogopgeleide) medewerkers te attenderen op de risico's van deze kanalen? Mag de werkgever in deze überhaupt eisen stellen of regels opleggen?

Het is zinvol om na te gaan hoe gevoelig informatie is; dat wil zeggen welke schade zou als gevolg van beschikbaarheid van deze informatie kunnen ontstaan (uitgedrukt in geld en omvang). Defensie hanteert een indeling naar kwetsbaarheid tegenover externe leveranciers. Een dergelijke indeling zou men ook ten aanzien van bedrijfsinformatie kunnen hanteren. Dit is ook goed te koppelen aan autorisatieniveaus voor medewerkers. Een voorbeeld zijn n.a.w.-gegevens van medewerkers. Behalve de afdeling personeelszaken, behoort niemand van buiten of binnen die te kunnen opvragen (vaak vormt de direct leidinggevende daarop een uitzondering).

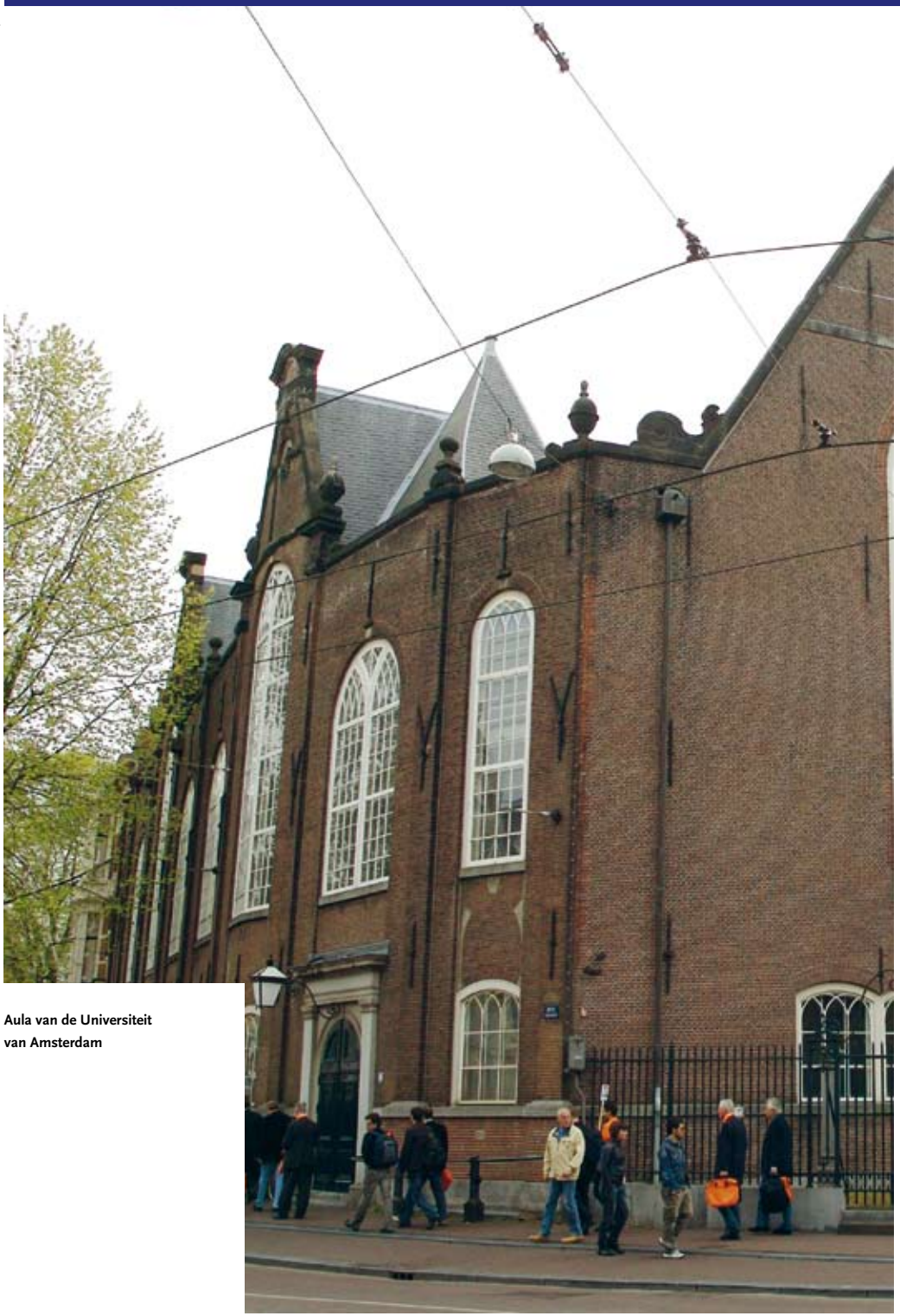
Waar ligt de verantwoordelijkheid?

Verschillende partijen hebben in dit verhaal hun eigen verantwoordelijkheid. Bovenaan zou ik het management willen plaatsen. Zij gaan over de plaats van informatiebeveiliging op de agenda, het budget, het beleid (inclusief sancties). Controle en de organisatie van de uitvoering van het beleid zou mogen liggen bij de IT-manager of meer specifiek de security officer. Dan hebben we de ICT-afdeling, waar medewerkers de eerste beveiligingslijn vormen (papieren of mondelinge informatie daargelaten).

Ten slotte de interne eindgebruikers. Het lijkt er op, dat men zowel van boven als van onder op meent dat informatiebeveiliging vooral bij en door de afdeling ICT geregeld moet worden, zonder hierin naar de eigen bijdrage te kijken. Gegevens of ideeën over risico's of incidenten zouden naar beide richtingen mogen stromen. Welke rol zou de bedrijfscultuur hierin kunnen spelen?

De rol van bedrijfscultuur

Weer een voorbeeld. Ongeveer 15 jaar geleden heeft Defensie aardig geïnvesteerd in mentaliteitsveranderingprogramma's. Jan Soldaat en de lagen er boven, zouden beter moeten leren omgaan met minderheidsgroeperingen binnen de organisatie. Hoe marginaal de effecten hiervan zijn, is ons inmiddels bekend. Een belangrijke oorzaak hiervoor is beslist gelegen in het incidentele karakter van een dergelijke operatie. Belangrijke boodschappen moeten voortdurend herhaald worden. Helaas is een onbedoeld effect daarvan, dat men door gewenning de boodschap niet meer zo ontvangt als hij bedoeld was. Op hoeveel



Aula van de Universiteit van Amsterdam

agenda's voor werkoverleg staat het aspect informatiebeveiliging standaard, of überhaupt? Hoe men met regels omgaat, is nauw verbonden met de heersende bedrijfscultuur. Ongeveer een kwart van de MKB-bedrijven heeft volgens de onderzoekers van Dynamic Marketing een gedragscode voor internetgebruik. Dat wil niet zeggen dat werknemers die ondertekenen of er naar handelen. Hoe komt het dat mensen bewust zich niet aan regels en instructies houden, en een manier hebben gevonden om dit gedrag goed te praten.

Sociale invloed

Met het kijken naar persoonlijke (interne) processen is de schets nog niet kompleet. Een aantal interpersoonlijke en intergroepsprocessen is minstens zo interessant om te beschouwen. Het vakgebied sociale psychologie leert ons dat het uitmaakt of we alleen zijn, met een ander of een groep anderen. Ook maakt het uit wie die anderen zijn. Als we ons in de context van dit artikel beperken tot 'het kantoor', dan is de vraag welke invloed een collega of groep collegae heeft, of juist de afwezigheid van hen. Een directe collega kan stimulerend of remmend werken op ons gedrag. De behoefte om bij een groep te horen kan ons er toe brengen niet-authentiek gedrag te vertonen. De behoefte ons te onderscheiden kan juist afwijkend gedrag tot gevolg hebben. U kunt het zelf aan- en invullen.

Communiceren over informatiebeveiliging

Bedrijfscommunicatie is een vak. Binnen dit gebied wordt er dankbaar gebruik gemaakt van psychologie. De functionaris PR & Communicatie weet hoe een boodschap moet worden verpakt en gebracht. Er worden bij grote bedrijven en instellingen aanzienlijke budgetten verspijkerd aan voorlichting. Elk schooljaar verzinnen bijvoorbeeld Hogescholen en Universiteiten aandachttrekkers om de nieuwe ICT-gebruikers te attenderen op de do's en dont's. Het is lastig om het effect hiervan op het gedrag van studenten te meten. Alleen gegevens die gelogd worden zijn te verzamelen, maar dan nog is de interpretatie ervan lastig.

In weinig bedrijven communiceert men over de status van de beveiliging. Medewerkers weten dus niet wat er op dat gebied gebeurt. Ook niet welke incidenten er zijn, hoeveel en wat de gevolgen daarvan zijn. Juist met deze informatie kan het management een volwassen beroep doen op de eigen verantwoordelijkheid van medewerkers. Stel je voor, dat ze er ook over gaan meedenken! Ook andersom zou het nuttig zijn gegevens hierover te delen. Wat te denken van cijfers over het geringe aantal incidenten, of een afname ervan in vergelijking met een voorgaand jaar of in vergelijking met cijfers binnen de zelfde bedrijfstak? Vanuit trots komen andere processen tot stand dan vanuit schaamte of in een cultuur van strenge regelgeving en sancties.

Een mentaliteitsverandering?

Zelfs wanneer we op de hoogte zijn van regels en hun achtergrond; in de dagelijkse praktijk storen we ons er niet of soms niet aan. Zo lang we niet rechtstreeks geconfronteerd worden met de gevolgen, laten we bijvoorbeeld ons surfplezier op het internet niet vergallen.

Eén van de ruim tachtig sessies tijdens NIOC 2007

Sterker nog, wie zijn mond daarover opendoet is een watje. Wat te denken van leidinggevenden, die zelf het verkeerde voorbeeld geven? Als mentaliteit afhankelijk is van personen, groepen van personen en de manier waarop men in de organisatie zaken benadert (de mores), zou een mix van maatregelen en gedragingen de richting van het gewenste gedrag kunnen aangeven.

Dat betekent onder andere gewenst gedrag stimuleren, belonen en een cultuur bevorderen, waarbinnen men zich vrij voelt om het bespreekbaar te maken. Hierbij luistert het nauw hoe leidinggevenden zich hierin opstellen. In plaats van een uitbrander geven, zou deze met de medewerker in kwestie kunnen nagaan waardoor de fout ontstond of hoe deze en wellicht ook anderen met de regels of voorschriften omgaan. Wellicht blijkt dat aanwijzingen in praktische zin lastig uitvoerbaar zijn (bijvoorbeeld in tegenspraak met andere regels). Een te groot aantal regels kan ook een afnemend effect tot gevolg hebben. Vaak zit de kunst in het naar boven krijgen van een werkbaar aantal. Dikwijls worden directe gebruikers niet betrokken bij de totstandkoming ervan.

Conclusie

Informatiebeveiliging is mogelijk met behulp van een aantal aangrijpingspunten. Wanneer we het bottom-up benaderen, kijken we naar individueel en groepsgedrag van medewerkers. Met een beetje pech ben je als bedrijf dan bezig een afdeling 'controle en sancties' op te tuigen. Top-down kan betekenen dat het management zich bewust is van de problematiek en deze stevig belegt bij een aangewezen functionaris. Deze doet beleidsvoorstellen en initieert de praktische invulling daarvan. Onderdeel daarvan zijn technische maatregelen, aanwijzingen, informatieverstrekking en -uitwisseling; het vooral op de agenda houden van IB-vraagstukken en het betrekken van de juiste mensen bij het ontwerp van maatregelen en het toezicht erop. Losgemaakt van informatiebeveiliging zouden deze suggesties ook opgaan voor vrijwel elk ander aspect van de bedrijfsvoering. De verantwoordelijke voor informatiebeveiliging kan hard maken, dat als dit aspect goed geregeld is, waarschijnlijk ook andere bedrijfsaspecten goed kunnen lopen. Het is maar welke kapstok je gebruikt.