Achter Het Nieuws

In deze rubriek geven enkele iB-redacteuren in een kort stukje hun reactie op recente nieuwsitems over informatiebeveiliging. Dit zijn persoonlijke reacties van de auteurs en deze geven niet noodzakelijkerwijs het officiële standpunt weer van hun werkgever of van PvIB. Vragen en/of opmerkingen kun je sturen naar ibmagazine@pvib.nl.

De mens wel/niet de zwakste schakel in informatiebeveiliging

Zodra we het hebben over informatiebeveiliging, gaat het over houding en gedrag van mensen. Dat is logisch, want vaak komen de grootste fouten in onze digitale wereld voort uit onachtzaamheid en nonchalance. En wat definieert dan een fout? Eigenlijk altijd, enkel en alleen, het resultaat. Of dit nu 'positief' is (gezien vanuit de hacker: doorbreking van een beveiliging) of 'negatief' (gezien vanuit ons als slachtoffer: de ongeoorloofde overboeking van een bedrag, wat direct een verlies betekent!).

Chris de Vries | Fook Hwa Tan | Nicole van Deursen | Tom Bakker

Praat erover en leer van elke fout van jezelf en die van een ander.

De keten is zo sterk als haar zwakste schakel en in elke digitale keten is dat altijd de mens! Natuurlijk moeten wij het in de informatiebeveiliging dus hebben over dat falend wezen, die domoor/sufferd/…, wiens catastrofale handeling iedereen natuurlijk voorzien had (vanuit het standpunt dat je altijd 'achteraf de koe in de kont kijkt'). Of niet soms? Wij hebben onze redactieleden gevraagd wat zij vinden van deze automatische reactie. Hoe staan zij tegenover deze onachtzame en nonchalante 'dader'? Hebben zij weleens in diens schoenen gestaan? Zo niet, wat zien zij als reden dat zij het goed hebben gedaan. Daarom een reflectie uit de zielen van de redactie.

Chris de Vries - Geluk, geluk, geluk en bedachtzaamheid

De enige keer dat ik ooit waargenomen heb dat mijn computer besmet was geraakt, betrof een eenvoudig macrovirus in een Wordperfectprogramma (voorloper van MS Word) en dat moet ergens midden de jaren 80 geweest zijn. Waargenomen, want hoe vaak ben ik niet besmet geweest, terwijl ik onwetend bleef? Dat dank ik, vermoed ik, aan drie factoren: geluk was aan mijn zijde, mijn bankiersachtergrond en mijzelf opgelegde vertragingen.

Geluk is het belangrijkste, maar dat kan bevorderd worden door discipline. Discipline die in mijn eerste arbeidsjaren als bankier werd gevoed door de noodzaak van vertrouwelijkheid, zorgvuldigheid en bedachtzaamheid. Als faillissementenbeheerder ga je om met het leven van anderen. Dat heb ik altijd als een grote verantwoordelijkheid ervaren en dus legde ik mij op vele acties vertraagd door te voeren; lees: te overdenken en de reflex te beheersen! Dat is weleens fout gegaan, ik bleek mens te zijn….

Daarnaast mijn filosofische aanleg en herkenning van veel in de deugden van de Stoïcijnen. Dat zijn er vier: moed, matigheid, rechtvaardigheid en wijsheid. Met deze beschikbare werktuigen benader ik mijn handelingen, mijn werk, mijn leven. Daar komt mijn begrip voor de mens als 'zwakste' schakel uit voort en voorkwam ik de grootste fouten in informatiebeveiliging.

Nicole van Deursen - Mensen zijn sterke schakels

Ik zal niet snel zeggen dat mensen zwakke schakels zijn. Ik hou niet van negatief geformuleerde boodschappen in ons vak. Mensen zijn niet altijd zwak, een hacker is niet per definitie een crimineel en techniek is niet per se moeilijk. We maken allemaal weleens een fout of we zien iets over het hoofd. Waar het om gaat is hoe je daarna handelt: ga je het herstellen en ervan leren, of geef je een ander de schuld? Veel fouten komen voort door gebrek aan digitale geletterdheid, werkdruk of interesse. Als je niet goed weet hoe iets werkt, als je onder te veel stress moet werken (lichte stress schijnt juist weer goed te zijn), of je vindt het niet echt interessant, dan kan het zijn dat je op een verkeerd linkje klikt of een instelling over het hoofd ziet. Meestal blijven mensen wel weg van zaken waar ze geen verstand van hebben. Maar er is bijna geen beroep meer waar je om computers heen kunt. Je moet dus wel gaan bijleren en 'zin maken'. Digitale geletterdheid begint al op school en ik hoop dat de volgende generaties van hun (beroeps)opleidingen komen met betere digitale vaardigheden dan mijn generatie. Werkgevers hebben ook een verantwoordelijkheid naar (nieuwe) medewerkers. Die weten niet vanzelfsprekend alles van de systemen waarmee je ze laat werken en vinden het ook niet altijd leuk om zich daar in te verdiepen. Train ze goed in de basis van het gebruik van een systeem voordat je veilig gedrag verwacht. En zorg dat ze zich veilig voelen om te rapporteren wanneer ze toch de mist in zijn gegaan. Praat erover en leer van elke fout van jezelf en die van een ander. Zo maken we onszelf weerbaar.

Fook Hwa - Mensen zijn je belangrijkste verdediging

Binnen informatiebeveiliging bouwen en beschermen we een organisatie door verschillende lagen van beveiliging op te richten. Dit betekent, dat we door maatregelen te nemen in processen en technologie en mensen daarover te leren, we het moeilijker maken voor criminelen om een organisatie binnen te komen om iets mee te nemen of schade aan te richten.

De mens wordt vaak gezien als de zwakste schakel. Maar is dit wel zo? Processen worden ingericht om te zorgen dat er geen ongeautoriseerde activiteiten worden uitgevoerd. De wereld is echter erg veranderlijk en vergt een hoge mate van flexibiliteit. Dit betekent dat ongeacht hoe goed een proces is bedacht er altijd situaties zijn waarbij je zou willen afwijken omdat de situatie dit noodzaakt. Technologie vindt men sterk, omdat het geen 'menselijke fouten' kan maken. Het is echter door mensen gemaakt en bevat vaak kwetsbaarheden. We zijn bezig met zelfhelende systemen, maar op dit moment zijn we nog

Fouten maken is zo menselijk. Er is geen training opgewassen tegen per ongeluk het verkeerde doen.

niet zover en kunnen we niet alleen op systemen vertrouwen. Dan krijg je nog de menselijke barrière die je kunt opwerpen. Dit doen we door training en bewustwording om te zorgen, dat personen binnen en buiten de organisatie geen rare dingen doen om de organisatie open te stellen voor onnodige inbreuken. Het is natuurlijk wel zo dat een fout heel menselijk is.
Organisaties werken hard om mensen niet op linkjes te laten klikken, bijlagen te openen en geen inloggegevens achter te laten. Dit doen we door e-learning, trainingen en andere gedrag beïnvloedende maatregelen. We komen er echter achter, dat we het vaak niet tot nul kunnen brengen. Fouten maken is zo menselijk. Wanneer iemand emotioneel is, haast heeft of anderszins is afgeleid dan is er geen training opgewassen tegen per ongeluk het verkeerde doen. Maar ik geloof dat wanneer we alle drie lagen van proces, technologie en mens op een hoger niveau krijgen, het mogelijk is een mix te creëren waarbij de verdediging van de organisatie optimaal is, oftewel: Intelligent Security Operation.

Tom Bakker - De mens als de sterkere schakel

De mens zou de sterkste schakel moeten zijn maar helaas in de praktijk blijkt het tegendeel. Er zijn allerlei redenen waarom de mens de zwakste blijkt. Naast de 'domme' fouten (vergissingen) die men soms maakt, is het zo dat criminelen steeds doortastender worden om mensen te verleiden ongewenste en verkeerde dingen te laten doen. Blijkbaar vinden zij ook dat de mens de zwakste schakel is. Daartoe gebruiken ze allerlei middelen om hun doel te bereiken.
Hoogleraar psychologie en marketing Robert Cialdini ontwikkelde zes principes om mensen te beïnvloeden en te manipuleren (Schaarste, Social Proof, Autoriteit, Sympathie, Wederkerigheid, Consistentie) (1). Later is daar Eenheid (groepsgedrag/-gevoel) als zevende aan toegevoegd. Het zijn eigenlijk marketingprincipes maar ook prima te gebruiken voor social engineering. De CEO-fraude is een voorbeeld van het autoriteit-principe. Wederkerigheid: ik heb iets voor jou gedaan en nu moet je iets voor mij doen. Relatiegeschenken zouden hier ook onder kunnen vallen. Zo zie je die principes terugkomen in allerlei ellende.

In 2010 verscheen in iB-Magazine (voorheen InformatieBeveiliging) acht artikelen van auteur Jan de Boer over deze principes toegepast op Social Engineering testen (o.a. Mystery Guest) (ze staan nog in het archief op de PvIB-website (2)). Wellicht een idee om deze principes in awarenessprogramma's op te nemen zodat men 'bewust bekwaam' wordt en verandert van de zwakste in een sterkere schakel. Iedereen kan het overkomen in die principes te trappen. Los van hacking en hackers. Alleen al in de supermarkt trap je er telkens weer in met die 'speciale aanbiedingen die je snel vandaag moet kopen'. Want op=op (schaarste).

(1) https://en.wikipedia.org/wiki/Robert_Cialdini
(2) https://www.pvib.nl/actueel/ib-magazines/archief?pagina=11