**Security-by-Design is het middelpunt van uw informatiebeveiliging**

*Organisaties moeten zich in duizend bochten wringen om te voldoen aan eisen aan informatiebeveiliging van bijvoorbeeld klanten, wetgevers, toezichthouders en andere stakeholders. Tot voor kort bekommerde zich in feite nooit iemand echt om beveiliging. Het gevolg daarvan is, dat beveiliging nu doorgaans neerkomt op het aanrukken van dozen met pleisters en dan maar plakken.* Maar pleisters laten wel eens los, kunnen het bloeden niet altijd stelpen of veroorzaken jeuk en worden dan losgetrokken. Bovendien is een wond niet ineens genezen als je er een pleister op plakt. Helaas richt de aandacht van leveranciers, adviseurs en toezichthouders zich vaak op de kwaliteit van de pleisters en het plakwerk. Voor hen de gemakkelijkste manier om werk te houden. Maar uw organisatie schiet er weinig mee op. Want vaak ontstaan er steeds weer nieuwe wondjes die afgeplakt moeten worden. Kortom, er is sprake van symptoombestrijding. En dat draagt weinig bij aan de oplossing van het echte probleem. Dat probleem blijft dan maar aandacht vragen, blijft geld kosten, blijft irriteren.

**Security by design is vooral gebaseerd op het scheiden van dingen**

Security by design is een modewoord. Het is door allerlei ICT- en security bedrijven geannexeerd als marketingterm om er hun waren mee aan te prijzen. Zelfs Wikipedia gaat daarin mee. Maar Security by design werd al toegepast in het stenen tijdperk. Het is de beste en de goedkoopste manier van beveiligen. Maar alleen als je er van meet af aan voor kiest. Security by design (vroeger vaak logische informatiebeveiliging genoemd) is primair gebaseerd op het scheiden van dingen. Laten we aan de hand van een fysiek voorbeeld uitleggen hoe dat werkt.
Al sedert de oudheid hebben mensen de behoefte om hun eigendommen te beveiligen tegen de boze buitenwereld. Ze doen dat door die eigendommen van de buitenwereld af te schermen. Eerst ging men daartoe in holen wonen en later bouwde men huizen. De muren van een huis vormen de belangrijkste scheiding van de buitenwereld. Daarnaast zijn er nog andere verdedigingslinies. Zo staat er misschien om uw tuin een hek of een schutting of heeft u om uw land sloten gegraven. En vroeger hadden steden stadsmuren en stadsgrachten en zat er een grens om Nederland, die werd bewaakt. Maar er is meer dan beveiliging. Om van binnen naar buiten te kunnen komen of kijken, werd de muur verzwakt door er deuren en ramen in te maken. Hierdoor werd het ook voor de buitenwereld mogelijk om binnen te komen, gevraagd of desnoods ongevraagd. Er was dus een probleem ontstaan. De oplossing voor dit probleem werd gevonden in goed hang en sluitwerk. Anders gezegd, er werd een pleister geplakt. Hierdoor kregen vooral ongenode bezoekers het wel moeilijker om binnen te komen, maar als ze dat echt wilden, kon het nog steeds. Sommigen installeerden bewegingssensoren of complete beveiligings- en alarmeringssystemen. Een volgende pleister dus, die veel geld kost een heel hinderlijk is. Want hij veroorzaakt hoofdzakelijk loos alarm.
Veel hinderlijke verdedigingslinies werden ook weer afgebroken, om toch maar weer gemakkelijke over de scheidingen te kunnen komen. Zo werd in de EU bepaald, dat de landsgrenzen open moesten. Dat was beter voor de economie. Maar tegelijkertijd werd het uiteraard onveiliger. Mensen met kwade bedoelingen konden op deze manier immers gemakkelijker bij hun doel komen. En er werden weer de nodige pleisters geplakt. De overheid voerde een identificatieplicht in, dwong providers om toegang te geven tot vertrouwelijke informatie en nam nog tal van andere maatregelen, die inbreuk betekenen op de privacy van burgers. Privacy is eigendom van de burgers. Dus in feite is hier sprake van diefstal, alleen is deze diefstal legaal gemaakt.

**Security by design is terug naar de basics**

Laten we de zaak nu eerst eens van de andere kant bekijken, vanuit de invalshoek van de risico's. We willen tenslotte niet in een vicieuze cirkel terechtkomen, waarin iedereen gelijk heeft, maar niemand gelijk krijgt.

Vanuit de boze buitenwereld geredeneerd moet er aan twee punten worden voldaan om die buitenwereld belang te laten hebben bij één van uw eigendommen:

- Het eigendom moet waarde hebben.
- Het eigendom moet te krijgen zijn met een beperkte inspanning en een lage pakkans.

En ook vanuit dit perspectief is scheiding weer de beste remedie is. Zaken met weinig waarde, zoals bijvoorbeeld uw tuinmeubelen, uw planten enzovoort laat u 's nachts gewoon in uw weinig beveiligde tuin staan. Meer waardevolle zaken zoals gereedschap overnachten in een iets beter beveiligd tuinhuisje. Uw laptop gaat 's nachts mee naar binnen in het huis. En als u beschikt over zeer waardevolle zaken (uw kroonjuwelen), dan legt u die in een brandkast. Met deze gelaagde beveiliging beschermt u uw eigendommen adequaat en beperkt u de overlast voor uzelf.
En dat werk prima. Het gaat pas fout als u niet de discipline heeft om bijvoorbeeld 's nachts uw laptop binnen te zetten en die gewoon op de tuintafel laat staan. U moet dan niet gek kijken dat hij de volgende ochtend verdwenen is. Het spreekwoord zegt niet voor niets: 'De gelegenheid maakt de dief'.
Als u die discipline echt niet wilt opbrengen en toch de laptop wilt beschermen, dan bent u wel genoodzaakt om hoge muren om uw tuin te bouwen, zodat de beveiliging van uw tuin wordt opgetrokken tot het niveau van uw huis. Dit is weer een vorm van pleisters plakken. En dat kost uiteraard geld en leidt tot irritatie.

**Security by design bij het beveiligen van informatie**

Als het gaat om fysieke dingen, dan snappen de meeste mensen uitstekend hoe de relatie tussen waarde en beveiliging in elkaar steekt. Als het echter gaat om informatie, dan zien we, dat vaak niemand zich daar meer om bekommert en alle informatie gewoon opslaat op dezelfde plek, bijvoorbeeld in een directory structuur. Als hier waardevolle informatie tussen zit, dan betekent dit, dat je in feite een hoge muur moet bouwen om je directory structuur (zeg maar de stadswal) tegen indringers van buiten. En iedereen wil toch ook zijn eigen tuintje beschermen, zodat er bovendien stevige schuttingen met een beveiligde toegang nodig zijn, omdat er anders teveel mensen toegang hebben tot dat eigen tuintje. En dus zijn er weer een heleboel pleisters nodig. Alleen maar omdat we niet even nadenken hoe we iets het beste kunnen opslaan.
En dat gaat nog verder. Bedrijven hebben van iedere medewerker een dossier. De privacy wet schrijft voor dat bijzondere gegevens (over ras, geloof, medische situatie, BSN, VoG, wangedrag) gescheiden moeten worden van identificerende gegevens. (Zie ook 'Toegevoegde waarde van een Privacy Officer of FG'.) De meeste HR-applicaties slaan deze gegevens dan ook netjes gescheiden op. Niets aan de hand dus. Maar vervolgens zien we dat alle gegevens van een medewerker worden geprint en in een mapje worden gestopt, dat in een la wordt bewaard. Of dat een HR-medewerker of een manager de gegevens van een medewerker bij elkaar harkt en in een Word- (pdf) of een Excelbestand plakt om dit vervolgens uit te printen of op te slaan in zijn directory structuur. En natuurlijk wordt dit printje niet direct na gebruik vernietigd en ook het Word- of Excelbestand wordt niet direct verwijderd. Kortom, er zijn kopieën gemaakt van informatie die door scheiding in de database weinig waarde had en dus ook niet goed beveiligd hoefde te worden en de scheiding tussen de identificerende gegevens en de bijzondere persoonsgegevens is doorbroken, waardoor er informatie is ontstaan, die wel een hoge waarde heeft (inbreuk op de privacy). Deze informatie, waarvoor dus een hoger beveiligingsniveau nodig is, wordt ook nog eens bewaard. Kortom, er zijn weer heel veel pleisters nodig. En als dan vervolgens zo'n documentje met informatie als pdf ook nog eens wordt gemaild naar een externe relatie, dan ontstaat er ineens ook nog een serie kopieën van dit kostbare document. Denk aan de eigen mailbox met verzonden items, de eigen mailserver, de mailserver van de provider, de mailserver van de ontvanger, de inbox van de ontvanger, die tevens kopieën stuurt naar zijn laptop, zijn tablet en zijn telefoon. En als het tegenzit, dan print die

ontvanger het documentje nog uit en slaat hij het op in zijn eigen directory. Om de waardevolle informatie uit dit ene mailtje te beschermen moeten er weer dozen met pleisters worden geplakt.

**Security by design: niet slepen met informatie**

Heel vaak denken we niet na bij de waarde van informatie, die bepalend is voor hoe je met de beveiliging van die informatie omgaat. In het laatste voorbeeld is er geen nieuwe informatie gemaakt. Er is alleen informatie verplaatst. De informatie was gescheiden en adequaat beveiligd beschikbaar in het HR-systeem. De scheiding is doorbroken en de informatie is vervolgens gekopieerd naar een groot aantal plekken, die dus allemaal beveiligd moeten worden om te voorkomen dat er in strijd met de privacywet wordt gehandeld. Kortom, allemaal overbodige beveiliging, kosten en dus irritatie, alleen omdat er ondoordacht is gehandeld.
Security by design begint dus bij het maken van scheidingen om te voorkomen dat de stadsmuren en stadsgrachten van vroeger weer opgetrokken moeten worden. Databases met gescheiden data zijn heel eenvoudig te beveiligen. Dit betekent wel, dat iedereen zich daarvan bewust moet zijn en dus niet gaat slepen met informatie. Natuurlijk is kennisdeling essentieel voor vrijwel iedere organisatie. (Zie ook 'Informatiebeveiliging en kennisdeling vragen om nieuwe oplossingen'.) Maar dat betekent niet dat informatie ongecontroleerd moet worden verspreid.
De basis is dat je gecontroleerd toegang geeft tot informatie. De informatie blijft dan op zijn plek en je kunt ook nog zien wie de informatie heeft bekeken. En als dit van buitenaf is, werk dan met een token of iets dergelijks. En als je vertrouwelijke informatie toch moet verzenden, versleutel dan de informatie of beveilig  het bestandje minimaal met een wachtwoord. Dan voorkom je dat overal en nergens ook weer pleisters moeten worden geplakt.
Juist doordat veel mensen zich niet bezighouden met de basisbeginselen van de beveiliging van informatie, moet er zoveel beveiligd worden, dat het irritant wordt en handenvol geld kost. Maar als je wilt dat medewerkers veilig werken, dan moet je het die medewerkers natuurlijk wel gemakkelijk maken om dat te doen en dat is iets wat veel ICT'ers en beveiligers weer niet snappen. (Zie ook 'Informatiebeveiligers verpesten iedere awareness'.)
Security by design is geen technische oplossing. Het is primair het logisch principe van scheiding dat toegepast moet worden in de fysieke, technische, organisatorische en juridische beveiliging.