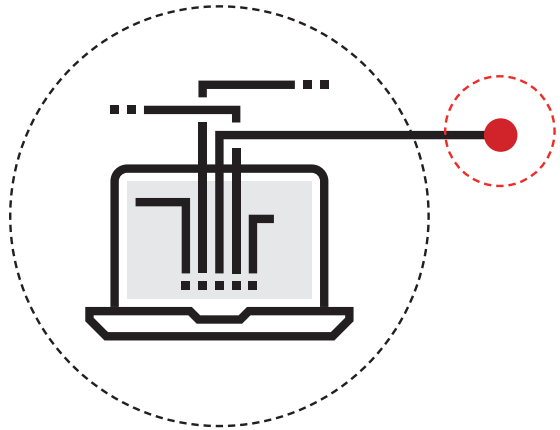
DATABEVEILIGING EN RISK MANAGEMENT

VIER STAPPEN NAAR BETERE DATABEVEILIGING

HITACHI
Inspire the Next

POWERED BY AVNET

Vanaf 1 januari 2016 bent u als organisatie verplicht om melding te maken van ieder datalek dat plaatsvindt binnen uw organisatie. Dat is vastgelegd in de nieuwe Wet Meldplicht Datalekken, onderdeel van de Wet Bescherming Persoonsgegevens. Helaas zijn niet alle organisaties goed op de hoogte of onderschatten zij de risico's. Een datalek kan naast hoge boetes ook leiden tot imagoschade en productieverlies. Het is nu belangrijker dan ooit om uw data en processen goed te beveiligen, iets wat alleen maar relevanter wordt wanneer u gebruikmaakt van de cloud.



BENT U BEKEND MET DE RISICO'S?

Zoals eerder aangegeven zijn niet alle bedrijven goed voorbereid op een datalek. U raakt bij een datalek namelijk niet enkel gegevens kwijt. Hieronder worden de belangrijkste risico's van een datalek besproken:

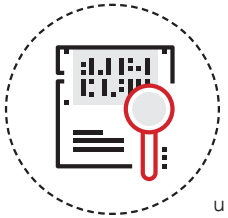
- Imagoschade: geen enkele organisatie wil op de voorpagina staan om de verkeerde redenen. Wanneer uw (potentiele) klanten lezen dat hun gegevens niet veilig zijn in handen van uw organisatie, zullen zij niet snel overgaan tot een nieuwe aankoop. Imagoschade leidt tot omzetverlies en misschien wel een faillissement.

- Onderbreking van dagelijkse werkzaamheden: bent u gegevens verloren die u niet terug kunt halen? Ook dan is er sprake van een datalek. Als u geen persoonsgegevens verliest, valt het datalek niet onder de Wet Bescherming Persoonsgegevens en daarmee ook niet onder de Meldplicht Datalekken. Dat wil niet zeggen dat een verlies van data in dat geval niet schadelijk is. Wanneer u gegevens over bijvoorbeeld leveringen of bestellingen kwijtraakt, kan het namelijk moeilijk zijn om uw dagelijkse werkzaamheden voort te zetten. Weet u nog wel hoeveel u moet produceren? Of waar en wanneer uw producten geleverd moeten worden?

- Hoge boetes: wanneer u persoonsgegevens verliest, bent u dus verplicht om dit te melden bij de Autoriteit Persoonsgegevens. Wanneer u dit niet doet, kan de boete oplopen tot wel €500.000,-. Dit is enkel de boete voor het niet melden van het lek, want de boete voor het datalek zelf kan tot wel €810.000,- bedragen. Deze boetes kunnen grote impact hebben op de organisatie.

VIER STAPPEN NAAR EEN BETERE BEVEILIGING

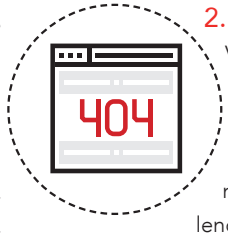
Deze risico's zijn dus wel degelijk aanwezig en moeten niet onderschat worden. De beste manier om te voorkomen dat u een boete krijgt of omzet verliest, is door uw data goed te beschermen tegen cybercriminelen en datalekken. U kunt een datalek voorkomen met behulp van deze vier stappen.



1. ANALYSE:

Allereerst is het belangrijk om een inventarisatie te maken van de data die u bezit. Welke data is cruciaal voor uw bedrijfsprocessen? Hoeveel data bezit u? Waar slaat u deze data op? Het is hierbij goed om eens kritisch te kijken naar de persoonsgegevens die u beheert. Heeft u alle gegevens die u vraagt aan uw klant of leverancier echt nodig? Gegevens die u niet vraagt en niet beheert, hoeft u tenslotte ook niet te beveiligen.

In deze fase kunt u bijvoorbeeld gebruikmaken van dataclassificatie. Daarbij wordt bepaald hoe belangrijk verschillende soorten data zijn voor de organisatie. Er wordt dus een bepaalde waarde toegekend aan de data. Dat kan gebaseerd zijn op verschillende voorwaarden en oogpunten. Welke data moet bijvoorbeeld te allen tijde beschikbaar blijven? Welke data is vertrouwelijk? Classificatie van data is cruciaal om te bepalen wat op welke manier beveiligd moet worden. Ook het lokaliseren is hierbij van groot belang. Waar is welke data opgeslagen? Gebruikt u een cloudomgeving of bewaart u alles on-premise? Door te bekijken waar al uw data opgeslagen staat, kunt u de beveiliging hierop aanpassen.



2. UITWERKEN:

Vervolgens is het belangrijk om te bekijken welke risico's deze data met zich meebrengt. Verschillende soorten data leiden tot verschillende risico's. De nieuwe Wet Meldplicht Datalekken gaat enkel over persoonsgegevens, dit is dan ook data die het meest risicovol is om te bewaren. Persoonsgegevens zijn gegevens die te herleiden zijn tot een persoon. Het gaat om voor de hand liggende gegevens zoals adressen en telefoonnummers, maar ook gegevens omtrent gezondheid en godsdienst.

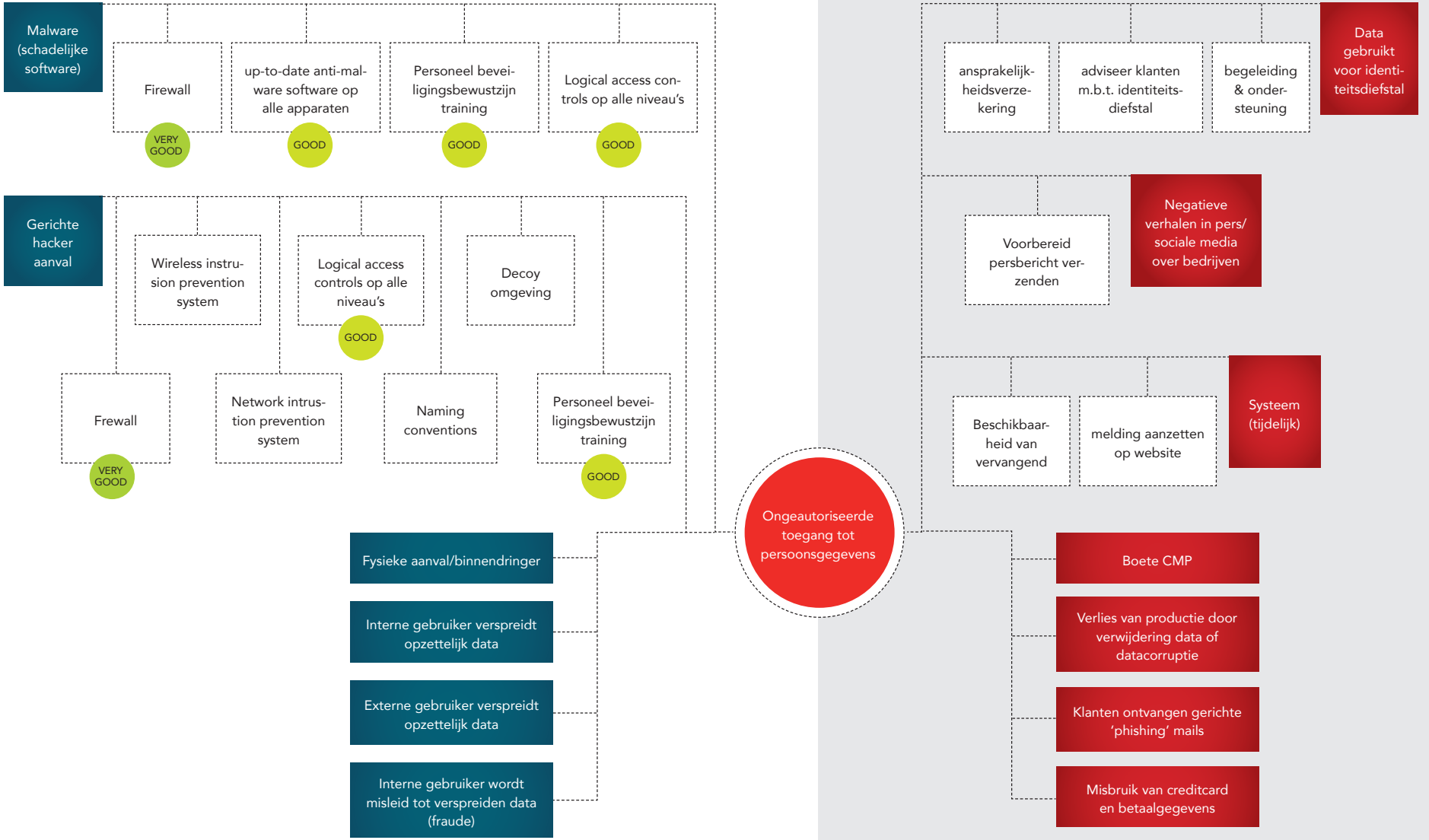
In deze fase van het proces gaat u de mogelijke risico's verder uitwerken. Dit kunt u bijvoorbeeld doen door gebruik te maken van de BowTie-methode. Hierbij is het belangrijk om de gebeurtenis die u wilt voorkomen centraal te stellen, bijvoorbeeld ongeautoriseerde toegang tot persoonsgegevens. Vervolgens maakt u een inventarisatie van de oorzaken en gevolgen van deze gebeurtenis.

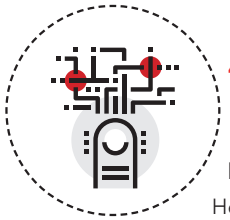
3. OPLOSSEN:

Nadat u de oorzaken en gevolgen in kaart heeft gebracht, kunt u gaan kijken naar mogelijke oplossingen voor het probleem. Dit doet u door de oorzaken één voor één te elimineren met behulp van geschikte maatregelen. Is een gerichte aanval van een hacker één van de mogelijke oorzaken? Dan zou access control bijvoorbeeld een goede maatregel zijn om toe te passen. Andere maatregelen waar u aan zou kunnen denken zijn bijvoorbeeld het versleutelen van uw data of het toepassen van encryptie.

Tijdens stap twee heeft u ook de gevolgen van een datalek geïnventariseerd. Mocht er onverhoopt toch een datalek plaatsvinden, wilt u voorbereid zijn op deze eventuele gevolgen. Wanneer u verwacht dat het datalek bijvoorbeeld leidt tot imagoschade, kunt u nu alvast een goed persbericht schrijven. Bent u bang dat uw website en systemen tijdelijk onbereikbaar zijn? Zorg dan dat er een foutmelding getoond kan worden op de website of dat er vervangend materiaal beschikbaar is.

Wanneer u oplossingen heeft gespecificeerd voor zowel oorzaken als gevolgen, heeft u een compleet overzicht van uw beveiliging en uw zwakke plekken. Wanneer u de BowTie-methode toepast, kan dit bijvoorbeeld leiden tot onderstaand schema.





4. IMPLEMENTEREN:

Nadat u een helder beeld heeft van de beveiligingsmaatregelen die nodig zijn binnen uw organisatie, kunnen deze maatregelen geïmplementeerd worden. Het implementeren van een firewall is daarbij minder ingewikkeld dan het toepassen van procedures. Het is belangrijk om daarbij te zorgen voor draagvlak bij de werknemers die de procedures uit moeten gaan voeren of data veilig moeten gebruiken. De BowTie-methode geeft de problemen en maatregelen visueel weer, waardoor deze gemakkelijker te onthouden en begrijpen zijn. Een afbeelding zegt tenslotte meer dan duizend woorden. Het is dan ook een goed idee om het schema binnen de organisatie te verspreiden. Daarnaast moet het gehele proces worden opgenomen in een zogenaamde Plan-Do-Check-Act methode, waarbij gestreefd wordt naar continue verbetering van het proces. Door de BowTie methode bij ieder proces of nieuw project te beoordelen, worden de veiligheidsprocedures steeds beter. Tot slot, kunt u bijvoorbeeld ook denken aan een security awareness training.

GOED BEVEILIGD MET IO4U & HITACHI

Deze vier stappen bieden houvast, maar er is nog steeds veel kennis en ervaring nodig om ze goed te doorlopen en de juiste oplossingen te kiezen. Met onze werkwijze en Hitachi Content Platform kunnen we risico's analyseren, maatregelen implementeren en data lokaliseren, classificeren en beveiligen. Onze methode visualiseert de risico's en maatregelen. Dit verhoogt de acceptatie en het draagvlak binnen organisaties.

HEEFT U ADVIES NODIG OP HET GEBIED VAN RISK MANAGEMENT EN PROTECTION? WIJ HELPEN U GRAAG VERDER.

WWW.DATAINDECLOUD.COM/RISKMANAGEMENT

OF NEEM CONTACT MET ONS OP: T 020 49 50 228 E INFO@IO4U.NL

HITACHI
Inspire the Next

POWERED BY AVNET