



## BEVEILIGING

Classity is gespecialiseerd in informatiebeveiliging. Of het nu gaat om beveiligingsoplossingen gebaseerd op gespecialiseerde technische kennis die nodig is voor het uitvoeren van security scans en technische audits, of om het vertalen van businesswensen naar passende informatiebeveiligingsoplossingen: bij Classity bent u aan het juiste adres.

## SECURITY MGMT

Classity kan met een interim security officer ondersteunen met: risico beheer, het verkrijgen van grip op dreigingen en kwetsbaarheden, informatiebeveiliging binnen outsourcingtrajecten, het adviseren over informatiebeveiliging binnen projecten/wijzigingen en het binnen uw bedrijf in begrijpelijke taal uitdragen van het nut en de noodzaak van informatiebeveiligingsmaatregelen.



## Beveiligingsbeleid, audits en advies VOORKOMEN EN GENEZEN



- **Beleid en baseline**  
Uitgangspunten voor informatiebeveiliging
- **Beveiligingsadvies**  
Ondersteuning bij specifieke beveiligingsvraagstukken
- **ICT audit**  
Beveiligingstoets van systeem, LAN of internet
- **Penetratietest**  
Hacker-test van uw website of applicatie

Bij informatiebeveiliging wordt veelal gedacht aan antivirus software, een firewall, een goed wachtwoord, het slotje in de browser en aan beveiligingsupdates. Terechte aandachtspunten, maar een goede beveiligingsinrichting eindigt niet bij een goed ingerichte technische infrastructuur. Een veilige dienst is alleen te realiseren als er binnen alle onderdelen van het proces dat nodig is om een dienst te leveren aandacht voor betrouwbaarheid is.

Deze betrouwbaarheid bestaat voor Classity uit het aantoonbaar op het *juiste moment* voor de *juiste personen* beschikbaar zijn van *juiste informatie*. Om dit te realiseren kijken wij samen met u naar kwetsbare punten in uw processen en/of systeemlandschap en kiezen ervoor om op basis van bedreigingen en business impact weloverwogen met risico's om te gaan. Beveiligingsoplossingen betekenen voor ons dus niet per definitie een opeenstapeling van dure producten en

diensten die de complexiteit van een omgeving (veelal onnodig) vergroten. En daarmee ook de project- en exploitatiekosten doen stijgen.

Bij een veilige infrastructuur (of dienst) staan een aantal zaken centraal.

### Beleid

Er moeten afspraken zijn hoe er met informatiebeveiliging wordt omgegaan. Hoe borgen we bijvoorbeeld dat ook onze leveranciers en hun onderaannemers betrouwbare diensten leveren? Wat vragen we van ons personeel en hoe brengen we informatiebeveiliging op een goede manier onder de aandacht? Wat zijn de minimale eisen die we aan de inrichting van ons netwerk stellen? Hoe trainen we onze applicatiebeheerders om op een goede manier met autorisaties om te gaan? En hoe zorgen we ervoor dat onze software ontwikkelaars betrouwbare applicaties ontwikkelen?

# Kwetsbaarheden bedreigen werkplek en netwerk

## OOK VOOR AUDITS

### INTERNET

Heeft u net een **nieuwe website**? Of wilt u van een bestaande site zeker weten dat het voor hackers niet mogelijk is om deze te misbruiken? Na een website penetratietest weet u het zeker.

### INTERN

Met een **interne netwerkscan** helpen wij ICT afdelingen met het verkrijgen van inzicht in de belangrijkste technische beveiligingsaandachtspunten. Met slim gecombineerde technische middelen onderzoeken we in korte tijd een groot deel van uw interne netwerk. Vanuit een kantoor netwerk perspectief wordt onderzocht wat binnen het LAN de gevaarlijkste kwetsbaarheden zijn.

**Classity**  
Informatiebeveiliging  
Zonnedauw 88  
7322EE APELDOORN

**Meer Informatie:**  
M. Hartsuijker  
+31-6-19671854  
info@classity.nl  
www.classity.nl

### Uitvoering

In het beleid gedefinieerde uitgangspunten hebben enkel bestaansrecht als medewerkers bereid zijn om ze op te volgen. Beveiligingsbewustzijn en training is hierbij erg belangrijk. Daarnaast is het belangrijk dat informatiebeveiliging niet op zichzelf komt te staan, maar wordt geïntegreerd in bestaande (beheer)processen en de standaard projectaanpak.

## Ondersteuning

Classity biedt ondersteuningsmogelijkheden voor de inrichting van zowel beleid, uitvoering als controle.

- **Beleid**

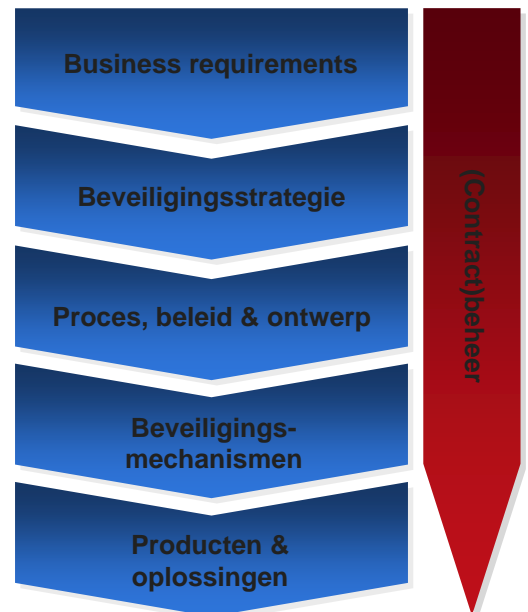
Informatiebeveiligingsbeleid  
ICT richtlijnen , policies en procedures  
Beveiliging binnen outsourcing & RFP's  
Beveiliging binnen projecten & ICT wijzigingen

- **Uitvoering**

Bedreigingen en kwetsbaarheden analyse  
Business Impact Analyse  
Security architectuur  
Beveiligingsmaatregelen binnen FO's en TO's  
Authenticatie en autorisatie frameworks  
Patchmanagement

### Controle

Om vast te stellen of de beveiligingsopzet (het beleid) en de uitvoering ervan goed functioneren, is het belangrijk om de werking regelmatig te controleren. Een goed controleprogramma heeft een gezonde balans tussen self-assessments en onafhankelijke audits.



- **Controle**

Hardening en systemscan  
Netwerk kwetsbaarheden scan  
Internet kwetsbaarheden scan  
Website penetratietest  
Effectiviteit van het patchmanagementproces  
Effectiviteit van wachtwoordpolicy

**Classity kan uw organisatie op verschillende fronten ondersteunen met het verbeteren van uw informatiebeveiliging. We zijn gespecialiseerd in gedetailleerde technische controles, zoals netwerkscans, website pentests en infrastructuur audits. Maar als u liever bij de basis begint helpen we u ook graag met een bij uw business passend beveiligingsbeleid.**

**In alle gevallen profiteert u maximaal van de kennis en ervaring van Classity.**

