



## 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.



## Patchmanagement (security updates)

### VOORKOMEN EN GENEZEN



- **Standaardiseer het beveiligingsonderhoud van de versies van uw bedrijfsapplicaties.**
- **Leer uw ICT-afdeling het verschil te bepalen tussen urgente en minder urgente beveiligingsupdates.**
- **Voorkom dat hackers via de werkplekken van uw medewerkers op het bedrijfsnetwerk inbreken.**
- **Geef wormen en andere malware geen kans.**

Waarschijnlijk heeft u het al gemerkt... het afgelopen jaar is het accent van de vanaf internet afkomstige aanvallen verschoven. Hackers vallen niet langer primair uw websites en mailservers aan, maar richten zich steeds vaker direct op uw gebruikers. En alhoewel deze gebruikers zich achter proxies, viruswalls, intrusion prevention systemen en firewalls bevinden, communiceren ze veelvuldig met internet. Via programma's als Office, de Java Runtime Environment, Quicktime, WMP en mediaplayers of software zoals Adobe Flash, Shockwave of Acrobat Reader verwerken uw gebruikers content (zoals video's, PDF's, presentaties, spreadsheets en muziek). Hackers besmetten deze content met trojans, virussen en andere malware met als uiteindelijk doel om de werkplek van uw gebruikers over te nemen.

Traditioneel beschermen we voornamelijk de buitenmuren van onze IT-infrastructuur en laten we

alles binnen die muren zoveel mogelijk met rust. Elke verandering kan in complexe omgevingen immers tot verstoringen leiden. En een stabiele ICT-omgeving blijft natuurlijk één van de belangrijkste doelstellingen van een ICT-beheerorganisatie. Doordat hackers zich steeds meer op kwetsbaarheden in applicaties die met internet communiceren richten, neemt de kans op verstoringen door het **niet** bijhouden van applicatieupdates echter ook steeds meer toe.

Bij softwareonderhoud met een beveiligingsdriver hebben we dus overduidelijk met een paradox te maken. Vanuit een traditionele beschikbaarheidsgedachte lijkt het verstandig om geen wijzigingen aan te brengen in een stabiele omgeving zonder veel verstoringen. Maar hoe langer we de wijzigingen uitstellen, hoe groter het risico wordt dat onze gebruikers getroffen worden door malware. Of erger nog: dat malware zich via onze gebruikers in ons netwerk weet te nestelen waardoor er risico's

# 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



ontstaan voor de beschikbaar, integriteit én vertrouwelijkheid van de complete ICT-infrastructuur.

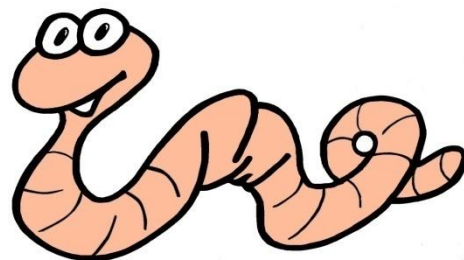
Het US-Cert (<http://www.us-cert.gov/>) is een organisatie die waarschuwingen afgeeft over de ernstigste security bedreigingen op internet. Alleen al in het eerste half jaar van 2009 is er door de

organisatie op tientallen ernstige fouten in gebruikerssoftware gewezen. Fouten die als ze misbruikt worden de betrouwbaarheid van de organisatie als geheel kunnen aantasten. Doordat de beveiligingsindustrie zich de afgelopen jaren met name heeft gericht op het verbeteren van direct vanaf het netwerk benaderbare software is de verwachting dat het aantal fouten in risicovolle werkplek applicaties de komende tijd alleen maar zal toenemen. De hoogste tijd dus om als ICT-organisatie ook op dit onderdeel de touwtjes weer in handen te krijgen.

## Randvoorwaarden

Om patchmanagement (of eigenlijk de software lifecycle) onder controle te krijgen zijn er een aantal belangrijke randvoorwaarden.

- **Ken je omgeving**  
Net als bij problem-, change- en incidentmanagement is een goede CMDB of software inventory van groot belang.
- **Ken je applicaties en werkplekken**  
Sommige softwareupdates (zoals bijvoorbeeld Java) kennen veel afhankelijkheden. Als de juiste applicatieve kennis niet wordt gecombineerd met beveiligingskennis en kennis van de kantoorautomatisering, dan neemt de kans op verstoringen toe.
- **Beschrijf en volg het patchmanagementproces**  
Een goed patchmanagementproces integreert de bovenstaande drie punten en sluit aan op de wijze waarop de organisatie met wijzigingen omgaat.
- **Ken de kwetsbaarheden**  
Niet elke kwetsbaarheid heeft eenzelfde mogelijke impact op de betrouwbaarheid. De prioriteit van het oplossen van een kwetsbaarheid kan daardoor verschillen. Om te voorkomen dat je als organisatie veel effort steekt in het oplossen van problemen die een marginaal risico wegnemen is het belangrijk om de impact van kwetsbaarheden goed in te schatten.



**Classity kan uw organisatie op verschillende fronten ondersteunen met het opzetten van een goed werkend patchmanagementbeleid en proces. Dit kan zich beperken tot het op weg helpen van een reeds samengesteld projectteam, of zich uitstrekken tot het coördineren, beschrijven en invoeren van het volledige proces.**

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

