



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 outsourcingstrajecten, het adviseren over informatiebeveiliging binnen projecten/wijzigingen en het binnen uw bedrijf in begrijpelijke taal uitdragen van het nut en de noodzaak van informatiebeveiligingsmaatregelen.

Meer Informatie:

M. Hartsuijker
+31-6-19671854
info@classity.nl
www.classity.nl



Security Scan

METEN IS WETEN

Indien binnen de ICT infrastructuur wijziging op wijziging volgt, is het eenvoudig om het overzicht kwijt te raken. In een CMDB is informatie over hardware en applicaties vaak nog wel terug te vinden, maar hoe weet u zeker dat deze systemen ook vrij zijn van beveiligingsfouten? Fouten maken is menselijk en de ervaring leert dan ook dat omvangrijke ICT omgevingen bijna altijd genoeg (vaak eenvoudig te verhelpen) fouten bevatten om een hacker kritieke informatiesystemen te laten misbruiken. Na een [security scan](#) van Classity weet u waar de belangrijkste fouten van uw infrastructuur zich bevinden, hoe u ze kunt wegnemen en wat u kunt doen om ze in de toekomst te voorkomen. Classity levert een aantal standaard security scans, zoals een [internet security scan](#), [netwerk scan](#) of [website penetratietest](#). Maar een security scan / technische audit "op maat", die aansluit op uw auditprogramma, TPM of SAS70 is uiteraard ook mogelijk.



- **Internet security scan**
Voor een veilige internetverbinding en DMZ
- **Netwerk security scan**
Voor een veilig intern netwerk
- **Technische audit**
Gedetailleerd systeemonderzoek
- **Website penetratietest**
Kunnen hackers op uw website inbreken?

Alhoewel we inhoudelijk vaak spreken van security audits, penetratietesten, scans en beveiligingscontroles, is uiteraard het einddoel het belangrijkste: zeker zijn dat onze informatie veilig is. Een security audit geeft invulling aan deze controleerbaarheid en is een middel om aantoonbaar te maken dat er (gelet op factoren als kwetsbaarheden, dreiging en waarde) voldoende maatregelen zijn getroffen om het juiste beschikbaarheids-, integriteits- en vertrouwelijkheidsniveau te kunnen garanderen.

Op het technische vlak helpt Classity hiermee met de hierboven genoemde security scans. Hieronder volgt een korte toelichting op deze scans.

- **De internet security scan**
Deze scan richt zich primair op de netwerk(en) die de systemen bevatten die vanaf internet worden benaderd. Na de internet security scan weet u of uw firewall goed is ingesteld, uw systemen up to date zijn en er geen rare configuratiefouten zijn gemaakt die een hacker toegang geven tot uw internet servers of interne bedrijfsnetwerk.
- **De interne netwerkscan**
Tijdens de interne netwerk scan wordt uw interne netwerk in kaart gebracht en uitgebreid getest op kwetsbaarheden. De belangrijkste kwetsbaarheden, waar u intern de grootste verbetering mee kunt realiseren, worden uitgewerkt in concrete aanbevelingen. uw systeembeheerders weten direct waar ze moeten beginnen.
- **De website penetratietest**
De website penetratietest gaat verder waar de internet security scan ophoudt. Elk beetje van de website wordt tijdens de penetratietest omgedraaid. Als uw website fouten bevat zoals Cross Site Scripting, SQL Injection of andere aan gebruikersinput gerelateerde fouten, dan komt dit in de resultaten van de penetratietest naar voren.
- **Technische audit**
Tijdens de technische audit worden normen rondom logische toegangsbeveiliging, security updates, hardening, backup en recovery, monitoring, beheer, etc. getoetst. Classity kan hierbij gebruik maken van uw interne normen en richtlijnen, maar ook toetsen op basis van een best-practise normenset.