IT-SECURITY: een hele uitdaging

Weet u waar het met de ICT van uw organisatie naartoe moet? Zo ja, weet u ook hoe u daar moet geraken? Een duidelijke strategie kan een antwoord bieden op beide vragen. Dat is de opzet van Realdolmens ICT Infrastructure Roadmap. Samen met de sleutelpersonen uit uw organisatie bepalen we de toekomst van uw ICT. Op basis daarvan schetsen we een roadmap waarop we scherp gedefinieerde en gebudgetteerde projecten plaatsen. We schetsen de horizon en de weg ernaartoe. Afgestemd op uw business.

IT-SECURITY: een hele uitdaging

Iedereen is vandaag een doelwit

Het internet is een geweldige vooruitgang, maar tegelijk een geweldig wapen tegen individuen, overheden en bedrijven. Het aantal cyberincidenten in België is in één jaar tijd verdubbeld (Smartbiz, maart 2015). Cybercrime is vandaag duidelijk big business. Kmo's zijn net zo vaak als multinationals het doelwit van hackers. Logisch, eigenlijk. Want hackers weten dat kleinere organisaties vaak minder goed beveiligd zijn. En als ze uw beveiliging hebben gekraakt, hebben ze gemakkelijker toegang tot de ICT van de (grote) bedrijven waar u zaken mee doet.

Uit onderzoek blijkt dat er in veel gevallen geen hooggespecialiseerde kennis of speciale middelen nodig zijn om bij een bedrijf binnen te dringen. In meer dan 80% van de gevallen hebben de criminelen in enkele minuten hun doel al bereikt. Ondernemingen maken van gegevensbeveiliging duidelijk nog onvoldoende een prioriteit. Dat heeft zeker te maken met de kosten van die beveiliging, die bedrijven liever niet willen maken. Nochtans kunnen de gevolgen van één incident enorm zijn, zowel voor de werking van het bedrijf, de financiële situatie als het imago.

Nieuwe mogelijkheden, nieuwe risico's

De invoering van cloud computing, de explosieve groei van big data en het integreren van mobiele devices bieden uw organisatie heel wat nieuwe mogelijkheden en voordelen. Maar ze zorgen ook voor nieuwe security-uitdagingen. Het aantal cyberincidenten neemt niet alleen toe, cybercriminelen gebruiken ook steeds nieuwe aanvalsmethoden. Hierdoor komen uw (virtuele) servers, mainframes, endpoints en vooral uw netwerk enorm onder druk te staan. Traditionele netwerkbeveiliging is vaak onvoldoende om de stroom aan cyberaanvallen een halt toe te roepen, waardoor diefstal van vertrouwelijke en gevoelige bedrijfsinformatie op de loer ligt.

Mensen blijven de zwakste schakel.

De hacker gaat altijd op zoek naar de zwakste schakel in een systeem. Meestal is dat de mens. Werknemers die hun pc in de wagen laten liggen, die te eenvoudige paswoorden gebruiken of ingaan op phishing. Mensen blijven maar klikken op links en buttons zonder zich veel vragen te stellen. Nog verontrustender voor bedrijven is de trend van spear phishing en zelfs phone phishing. Vandaag werken criminelen via callcenters om toegang te krijgen tot de interne systemen van een organisatie. Wie medewerkers bewuster maakt van de problematiek, kan al snel meer veiligheid in zijn onderneming tot stand brengen.

MET EEN
ANTIVIRUS
KOM JE
ALTIJD
TE LAAT!

- Elke dag worden in Europa bijna **150.000 COMPUTERS** besmet met een virus.
- Symantec raamt de schade van cybercriminaliteit over de hele wereld op 290 miljard euro/jaar.
- Uit de Eurobarometer-enquête over cyberbeveiliging blijkt dat **18% VAN DE INTERNETGEBRUIKERS** minder snel via internet koopt wegens zorgen over cyberbeveiliging.
- Volgens Eurostat heeft maar **een kwart van de bedrijven** een duidelijk ICT-beveiligingsbeleid.

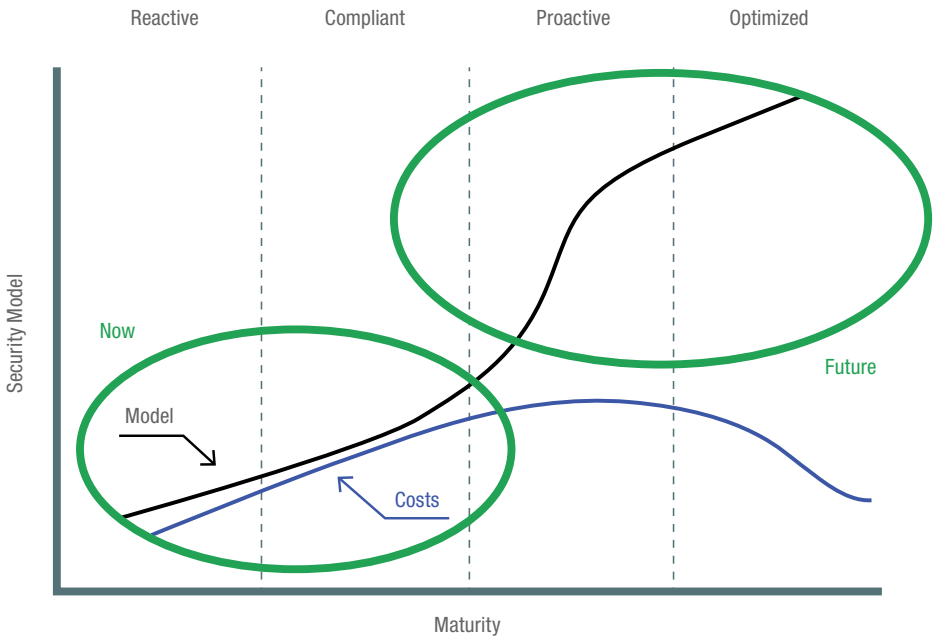
Bron: europa.eu

REALDOLMENS security-aanpak

Van reactief naar proactief

Terwijl beveiligingsaanvallen vandaag het voorpaginanieuws halen, menen de meeste bedrijven beschermd te zijn met traditionele tools zoals antivirus of een firewall. Vaak zijn die producten echter niet geïntegreerd en niet up-to-date. Bovendien zijn ze vaak niet aangepast aan de nieuwe types aanvallen. Vandaar het belang om de belangrijkste bedrijfsprocessen, applicaties en bedreigingen in kaart te brengen zodat u de nodige maatregelen kunt treffen om die optimaal te beveiligen. Voorkomen is beter dan genezen. Een goed uitgebouwde security-omgeving helpt bij het tijdig signaleren van een cyberaanval waardoor zo snel mogelijk kan worden gereageerd en hersteld. Om goed bestand te zijn tegen een cyberaanval is het van belang de cyclus, van het identificeren tot en met detectie en reactie, volledig voor te bereiden.

Wilt u inzicht krijgen in de beveiliging van uw organisatie? Wenst u meer zekerheid over de security van uw omgeving en zo uw klanten beschermen en een vertrouwensbreuk voorkomen? Dan bieden de Realdolmen Vulnerability Assessment en Penetration Testing een oplossing.



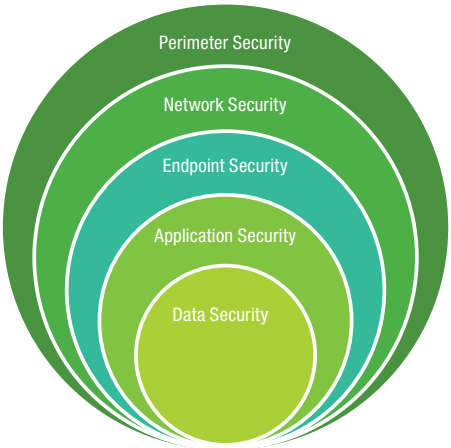
Gelaagd securitymodel

Door de informatiebeveiliging op verschillende lagen van uw IT-systemen in te zetten, biedt gelaagde beveiliging de nodige redundantie als een van de controles faalt. Bovendien laat het organisaties toe om op een progressieve manier tools te implementeren die toelaten om zowel data als applicaties te beveiligen. Kortom, een aanpak die de big bang vermijdt.

Bovendien kunt u op uw eigen ritme evolueren zonder abstractie te moeten maken van de producten die u al gebruikt. Realdolmen heeft immers partnerships afgesloten met diverse leveranciers die alle beveiligingslagen kunnen dekken. We zijn er immers van overtuigd dat beveiliging veel meer is dan louter producten en vertrekken altijd vanuit een architectuurbenadering.

Managed Security Services

Organisaties hebben door de complexiteit van IT mogelijk niet meer de kennis en mankracht om bedreigingen van hun IT-infrastructuur op tijd te detecteren en hier dan nog snel op te reageren. Managed Security Services bieden hier een oplossing. U krijgt ondersteuning van een team beveiligingsspecialisten die uw netwerk monitoren, malware en cybercriminelen detecteren en op de gepaste wijze reageren. Om deze dienst aan te leveren werken we vanuit Realdolmen samen met partners zoals Symantec. Zij analyseren elke maand meer dan een 275 miljard log-entries, identificeren meer dan 40.000 beveiligingsincidenten en detecteren meer dan 4.000 gevalideerde ernstige incidenten.



IT-security:
een hele uitdaging

Mail naar info@realdolmen.com.

We contacteren u zo snel mogelijk. Natuurlijk kunt u ook terecht bij uw accountmanager.

REALDOLMEN
to get there, together