vanroey.be

wat is JOUW opstelling?

PRAKTISCHE GIDS OM JE **ICT OMGEVING** TE **BEVEILIGEN**

“Vaak moet er iets gebeuren voordat er iets gebeurt.”

- Johan Cruijff

Hackers en malware gebruiken uiteenlopende tactieken om jouw organisatie aan te vallen. Hoe bescherm je jezelf best?
De juiste oplossingen kiezen is aartsmoeilijk en wachten is geen optie.

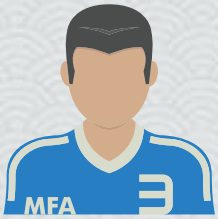
Cybersecurity is een complexe materie. Het wordt al een stuk duidelijker wanneer we de vergelijking met voetbal maken. Eén sterspeler betekent weinig zonder teamgenoten. Dit geldt ook voor security oplossingen.

Het juiste team, geruggensteund door de juiste strategie bepaalt of je de situatie machtig bent.

WE STELLEN **ONZE OPLOSSINGEN** GRAAG VOOR **ALS TEAMSPELERS** DIE WE TACTISCH INZETTEN:

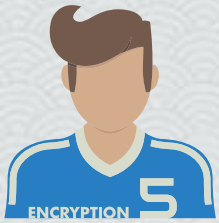
ANTIVIRUS + ANTISPAM + FIREWALL + BACK-UP + PATCHMANAGEMENT

SECURITY AWARENESS TRAINING



MULTI FACTOR AUTHENTICATION

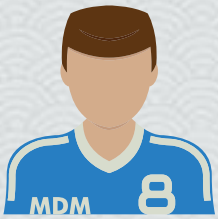
PASSWORD POLICY



ENCRYPTION

PRINTING SECURITY

CLIENT SECURITY



MOBILE DEVICE MANAGEMENT

NETWORK ACCESS CONTROL

WIRELESS SECURITY

REVERSE PROXY

USER ENTITY BEHAVIOUR ANALYTICS

CLOUD ACCESS SECURITY BROKER

MANAGED SERVICES

JOUW COACH VANROEY.BE

"Je beveiliging is maar zo goed als de zwakste schakel: de eindgebruikers."

#1 ANTIVIRUS, ANTISPAM, FIREWALL, BACK-UP, PATCH-MANAGEMENT

Of je nu een organisatie bent met een beperkt of eerder een groot aantal kantoorgebruikers, de basics moeten sowieso op orde zijn:

- Een degelijke hardware firewall, antivirus en antispam houden het gros van de bedreigingen tegen.
- Gaat het toch een keer mis? Dan kan een betrouwbare back-up je alsnog uit de nood helpen.
- Overweeg zeker ook Sandboxing, hiermee worden bestanden en e-mails uitvoerig getest, nog voor ze eindgebruikers bereiken.
- En last but not least: patchmanagement! Windows-updates, updates van individuele programma's en firmware van alle apparatuur in het netwerk moeten te allen tijde up-to-date zijn om voor de hand liggende hacks te voorkomen.

2: MANAGED SECURITY AWARENESS TRAINING

Je beveiliging is maar zo goed als de zwakste schakel: de eindgebruikers. Hoe snel klikt iemand riskante bijlagen open of vult deze gevoelige gegevens in? Via onze Managed Security Awareness Training krijg je inzicht in de alertheid van je personeel en ontdek je wie vatbaar is voor valse mails of websites. We stellen hen regelmatig op de proef met valstrikken en wijzen hen op de fouten en mogelijke risico's.

3: MULTI FACTOR AUTHENTICATION

Een sterk wachtwoord van een gebruiker ontfutselen is eenvoudiger dan gedacht. Daarom bieden we oplossingen om bovenop het wachtwoord, een unieke tijdsgebonden code in te voeren die naar de gebruiker wordt ge-sms't.

4: PASSWORD POLICY

Gebruiken je medewerkers krachtige, unieke wachtwoorden of gebruiken ze steeds hetzelfde, zwakke wachtwoord? Een goed beleid kan met hulp van tools complexe wachtwoorden verplichten, genereren, veilig doorgeven en beheren.

5: ENCRYPTION

Een gestolen laptop of smartphone bevat een schat aan informatie. Om te voorkomen dat dieven aan deze informatie geraken is het versleutelen van deze gegevens van uitermate belang.

6: PRINTING SECURITY

Net als PC's beschikken printers over netwerktoegang, geheugen, een harde schijf en een processor. Waarom zou je hen dan onbeveiligd in je netwerk zetten? Bescherm bv. het BIOS om de integriteit te verzekeren zodat niemand de prints kan uitlezen. Ook onbewaakte documenten die blijven liggen vormen grote beveiligingsrisico's.

7: CLIENT SECURITY

Wanneer werknemers zeer gevoelige informatie op hun apparaten dragen is de keuze van het toestel van groot belang. Versterk de beveiliging met ingebouwde vingerafdruklezers, smartcard readers of een privacy guard. Maar het gaat ook verder dan dat: geavanceerde malware nestelt zich vaak buiten het besturingssysteem of harde schijf, bv. het BIOS of RAM- geheugen. Met HP Sure Start en Sure Run heb je de garantie op de integriteit van BIOS en software. De systemen zijn zelfhelend, dus van uitval is er geen sprake.

9: NAC

Met Network Access (of Admission) Control kunnen bezoekers geen connectie maken met bv. losliggende netwerkkabels of een gelekt WiFi-wachtwoord om zo toegang te krijgen tot de infrastructuur van uw organisatie. Enkel geverifieerde devices krijgen toegang.

11: REVERSE PROXY

Een reverse proxy heeft vele functies. Voorbeelden hiervan zijn:

- Het beschermt je domein of website door externe requests eerst te analyseren en te filteren alvorens ze je perimeters (beperkt) mogen bereiken;
- Het voorkomt DDoS aanvallen;
- Je voorkomt dat externe partijen inzicht krijgen in je intern netwerk.
- Vergeet ook niet dat infrastructuur in de cloud evenzeer beveiliging nodig heeft. Een Windows Server in de cloud dien je, net zoals een server on premise, van de nodige security te voorzien.

8: MOBILE DEVICE MANAGEMENT

Via Mobile device Management dwing je (beveiligings)policies af op de mobiele toestellen van werknemers (iOS, Windows en Android). Verplicht hen vergrendeling te configureren, stel enkele applicaties als standaard in, vergrendel of wis apparaten, data of apps vanop afstand enzovoort.

10: WIFI SECURITY

Uiteraard dien je je eigen netwerk goed af te schermen van het publieke netwerk. WPA2 encryptie is een minimum, alsook een grondige controle of er via het gastnetwerk geen toegang te verkrijgen is tot vitale bedrijfsopslag of -databases. Ook hier is een goede firewall met URL filtering en een acceptatie van specifieke gebruiksvoorwaarden van groot belang om te vermijden dat mensen illegale activiteiten verrichten vanop je IP-adres.

Zorg er ook voor dat WiFi SSID's via een policy naar apparaten worden gepusht en er automatisch verbinding gemaakt wordt of zelfs dat de SSID helemaal verborgen wordt. Zo voorkom je dat een hacker zich op de parking kan begeven met een hotspot die hetzelfde SSID als dat van jouw bedrijf uitzendt.

“Ook hier is een goede firewall met URL filtering en een acceptatie van specifieke gebruiksvoorwaarden van groot belang om te vermijden dat mensen illegale activiteiten verrichten vanop je IP-adres.”

"Het beheer van ICT is aartsmoeilijk en de ontwikkelingen gaan razendsnel. Laat ons team van high-level experts zich bekommeren over je ICT-infrastructuur."

12: USER ENTITY BEHAVIOUR ANALYTICS

Helaas is er altijd een klein percentage personeelsleden met kwaad opzet... UEBA kan, mede dankzij artificiële intelligentie en algoritmes, afwijkend gedrag identificeren en hierdoor beveiligingsrisico's beperken. Denk aan medewerkers die de klantendatabase downloaden en deze op een USB stick zetten of naar een Dropbox uploaden. Of een gehackte collega die normaal gesproken steeds vanuit Antwerpen werkt en nu 'opeens' vanuit Oekraïne inlogt op de documentbibliotheken.

13: CLOUD ACCESS SECURITY BROKER

Cloud Access Security Broker (CASB) zorgt voor een beveiligingslaag tussen het bedrijfsnetwerk, de gebruikers en de verschillende cloudtoepassingen zoals bv. Office 365, Salesforce of Google. Zo krijg je dezelfde laag van beveiliging binnen, maar ook buiten je bedrijfsnetwerk.

Binnen het bedrijfsnetwerk zal het aanmelden vlot en eenvoudig verlopen. In een internetcafé in Shanghai zal je een extra verificatie moeten doorstaan om te bewijzen dat jij het bent. Daarnaast kan het ook op inhoud controleren en detecteren wanneer gevoelige inhoud als Visakaartnummers gedeeld wordt. Indien nodig kunnen beheerders een apparaat of app vergrendelen of wissen vanop afstand.

14: MANAGED SERVICES

Het beheer van ICT is aartsmoeilijk en de ontwikkelingen gaan razendsnel. Laat ons team van high-level experts zich bekommeren over je ICT-infrastructuur. We voorkomen hacks door geautomatiseerd patchmanagement en minimaliseren downtime door preventieve monitoring en 24/7 ondersteuning. Zo kunnen interne ICT medewerkers zich focussen op strategische taken ipv brandjes blussen en het uitpluizen van raadselachtige issues die wij dagelijks oplossen.

COACH VANROEY.BE

Met ruim 25 jaar ervaring, een team gecertificeerde Level 3 security experts en de hoogst mogelijke partnerships bij topmerken zoals Fortinet, Microsoft, HP en HPE, is VanRoey.be de ideale coach om samen met de klant de ideale opstelling te gaan bepalen. Tal van tevreden klanten bevestigen deze stelling.

”Als wij de bal hebben, kunnen hun niet scoren”

- Johan Cruijff

vanroey.be

ALS COACH ZORGT **VANROEY.BE** VOOR DE JUISTE **SECURITY OPSTELLING** VOOR JOUW ORGANISATIE. DIT STEEDS AANGEPAST AAN DE ACTIVITEITEN EN GROOTTE VAN JE ONDERNEMING.

VOORBEELDSTRATEGIE:
RETAILER

Een keten van kledingzaken met verschillende vestigingen en webshop.

De klanten en het personeel maken continu gebruik van de aanwezige wifi, die tevens dient als analysetool om het gedrag van de shoppers op te volgen. Elke shop is uitgerust met touchscreens waarop klanten meteen kunnen bestellen.

ONZE OPSTELLING:

#1 KEEPER
#10 WIFI SECURITY
#5 ENCRYPTION
#7 CLIENT SECURITY
#4 PASSWORD POLICY
#14 MANAGED SERVICES
#13 CLOUD ACCESS SECURITY BROKER
#9 NETWORK ACCESS CONTROL
#2 SECURITY AWARENESS TRAINING
#3 MULTIFACTOR AUTHENTICATION
#11 REVERSE PROXY

WETEN WELKE SPELERS VOOR JOUW ORGANISATIE BELANGRIJK ZIJN?

Ontvang onmiddellijk een **uitgebreid security-voorstel** op maat via:

VANROEY.BE/**STRATEGIE**

EEN AANTAL VAN ONZE TEVREDEN KLANTEN:

TORFS SCHOENEN MET NAAM · P&V · FLUXYS EXCELLENCE IN GAS TRANSPORT · imelda ZIEKENHUIS · az turnhout · UZ LEUVEN · Van Lanschot · SFZ

“Gedetailleerde offertes, een doordacht project management en een professioneel specialisten team: de ideale cocktail tot een goede samenwerking.”

Raf De Leu, IT-manager Torfs

TRUST **DIGITAL**
CREATE
WONDERFUL
THINGS

ONZE PARTNERS

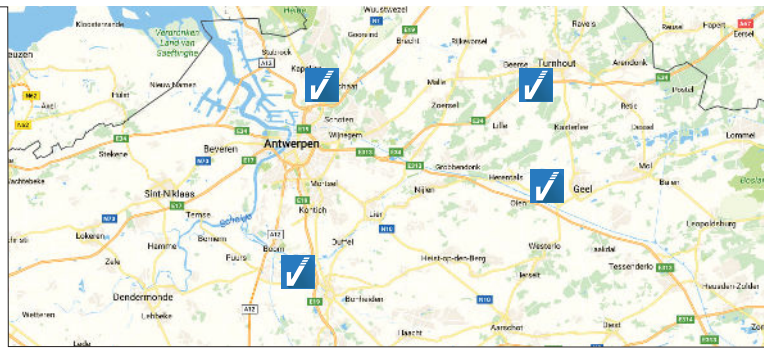
Specialisten die maximaal gecertifieerd zijn en met bewezen technologie werken.

FORTINET PLATINUM PARTNER & PARTNER OF EXCELLENCE
aruba a Hewlett Packard Enterprise company
Symantec. Gold Partner
Microsoft Gold Partner
Hewlett Packard Enterprise
Business Expert Partner
exabeam
Entrust Datacard sms|passcode
RUCKUS an ARRIS company

Contacteer VanRoey.be

+32 14 470 605 (algemeen)
business@vanroey.be
www.vanroey.be

vanroey.be
TRUST DIGITAL, CREATE WONDERFUL THINGS



Turnhout

Kempenlaan 2
B-2300 Turnhout

Geel

Antwerpseweg 116h
B-2440 Geel

Mechelen

Motstraat 30
B-2800 Mechelen

Antwerpen

Sint-Pietersvliet 7
2000 Antwerpen