

THE POWER OF BEING UNDERSTOOD

AUDIT | TAX | CONSULTING

IT INSIGHTS

CYBERSECURITY: HOE VERMIJDT UW BEDRIJF CYBERAANVALLEN?



Zoals u wellicht weet is het aantal cyberaanvallen de laatste maanden toegenomen. Zo werd afgelopen weekend het woonzorgcentrum in Willebroek getroffen en eerder deze maand het productiebedrijf Picanol.

Ook Asco is nog steeds niet hersteld van de aanval in juni 2019. De producent van vliegtuigonderdelen is destijds niet ingegaan op de eis om het losgeld te betalen en verkoos om het probleem zelf op te lossen. Het herstel van de aangetaste productiesystemen is na 6 maanden nog steeds bezig. Dit heeft zware financiële gevolgen voor Asco.

Naar aanleiding van deze verschillende cyberaanvallen delen we u graag enkele **best practices** mee om aanvallen op uw bedrijf te voorkomen.

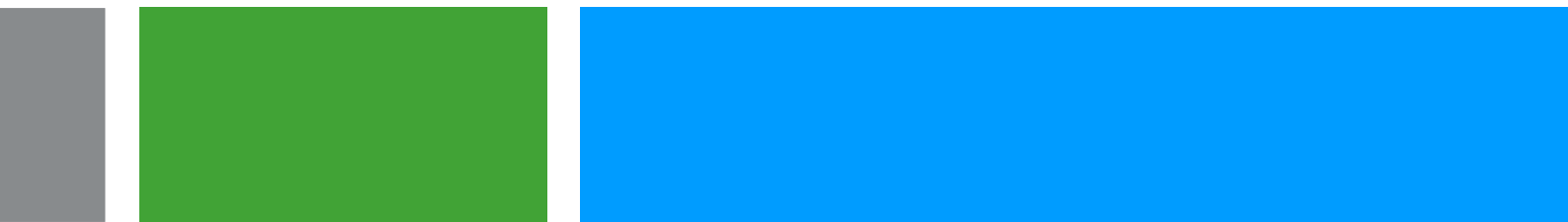
Binnen uw office 365 omgeving:

- Implementeer **multi-factor authenticatie** om in te loggen.
- Blokkeer **mail forwarding** zodat hackers niet ongezien gevoelige informatie kunnen doorsturen en meelesen.
- Monitor onsuccesvolle inlogpogingen en blokkeer automatisch na vb. 5 onsuccesvolle pogingen het Office 365 account.
- Controleer regelmatig de foutmeldingen in het Office 365 administrator account

Naast deze specifieke configuratie, raden wij u aan om:

- Uw IT systemen regelmatig te laten testen op eventuele veiligheidsrisico's.
- Uw personeel continu bij te scholen door het geven van **awareness** training over oa **phishing, ransomware, enz.** De oorzaak van een cyberaanval ligt vaak in een vergetelheid of menselijke fout.
- Minimaliseer het gebruik van mobiele toestellen, vb. USB sticks, draagbare harde schijven, geheugenkaarten enz.
- Het inperken van **single sign one (SSO)**, vooral voor toegang tot bedrijf kritische systemen.
- Het afschermen van kritische machines in een aparte VLAN met beperkte of geen toegang tot het internet of intern netwerk.
- Zorg ervoor dat al uw systemen bv. Firewall, PC's,.. tijdig de laatste security updates hebben.
- Uw anti-virus heeft bij voorkeur "**containerized**" mogelijkheden waardoor email bijlagen niet lokaal, maar standaard eerst in de **cloud** worden geopend. **Ransomware** zal minder kans krijgen om zich lokaal in uw netwerk te verspreiden.
- Het afsluiten van een cyber verzekering om u gedeeltelijk in te dekken tegen de financiële risico's.

Hebt u hulp nodig met de implementatie van bovenstaande topics, aarzel niet om contact op te nemen met RSM IT Advisory. Vraag naar onze gratis brochure ivm met **penetration testing** van uw website, **ethical hacking** en 24/7 **treath detection & response services**.



RSM IT Advisory organiseert regelmatig workshops omtrent Digitale transformatie, Cyber Security en GDPR, klik [hier](#) om u te abonneren op onze nieuwsbrief zodat u op de hoogte bent van de volgende workshop.

U kan zich alvast inschrijven voor onze Cyber Insurance workshop op itadvisory@rsmbelgium.be

CONTACTGEGEVENS:

Steven VERMEULEN
Partner IT Advisory
s.vermeulen@rsmbelgium.be

☎ +32 494 51 86 03

☎ +32 3 449 57 51

ZAVENTEM

Lozenberg 22 b 2 - B 1932 Zaventem
T +32 (0)2 725 50 04 - F +32 (0)2 725 53 41

ANTWERP

Posthofbrug 10 b 4 - B 2600 Antwerp
T +32 (0)3 449 57 51 - F +32 (0)3 440 68 27

BRUSSELS

chaussée de Waterloo 1151 - B 1180 Brussels
T +32 (0)2 379 34 70 - F +32 (0)2 379 34 79

CHARLEROI

rue Antoine de Saint-Exupéry 14 - B 6041 Gosselies
T +32 (0)71 37 03 13 - F +32 (0)71 37 01 39

MONS

boulevard Saintelette 97 b - B 7000 Mons
T +32 (0)65 31 12 63 - F +32 (0)65 36 37 07

AALST

Korte Keppestraat 7 bus 52 - B 9320 Erembodegem
T +32 (0)53 75 12 20

interaudit@rsmbelgium.be
interfiduciaire@rsmbelgium.be
intertax@rsmbelgium.be
interpay@rsmbelgium.be
itadvisory@rsmbelgium.be

WWW.RSMBELGIUM.BE

RSM Belgium is a member of the RSM network and trades as RSM. RSM is the trading name used by the members of the RSM network.

Each member of the RSM network is an independent accounting and consulting firm, each of which practices in its own right. The RSM network is not itself a separate legal entity of any description in any jurisdiction.

The RSM network is administered by RSM International Limited, a company registered in England and Wales (company number 4040598) whose registered office is at 50 Cannon Street, London, EC4N 6JJ.

The brand and trademark RSM and other intellectual property rights used by members of the network are owned by RSM International Association, an association governed by article 60 et seq of the Civil Code of Switzerland whose seat is in Zug.

© RSM International Association, 2019