juni 2020

+ Cybersecurity-lexicon voor kmo's

Missie 'gemoedsrust'

Onderzoeksrapport cybersecurity bij Belgische kmo's

It just takes
one mailicious email

proximus
enterprise

Inhoud

1. Methodologie

2. Onderzoeksresultaten

   2.1. Cybersecurity = topprioriteit

   2.2. Aantal en soorten aanvallen

   2.3. Zware gevolgen

   2.4. Security aanpak

3. Beveilig uw bedrijf in 4 stappen

4. Het aanbod-op-maat van Proximus

Bijlagen

Cybersecurity-lexicon

Bronnen

Vooraf

Wereldwijd stijgt het aantal cyberaanvallen van jaar tot jaar. Ook kmo's ondervinden meer en meer last van cybercriminaliteit.

*Internationale onderzoeksbureaus bestuderen geregeld het cybersecuritylandschap. Maar hun cijfers zijn niet altijd representatief voor Belgische kmo's. Daarom organiseerde Proximus twee eigen studies: een kwalitatief en een kwantitatief onderzoek bij **122 Belgische bedrijven.***

3 key facts uit het onderzoek

1. **Negen op de tien** Belgische kmo's is **bezorgd** over mogelijke aanvallen.
2. **Phishing**-aanvallen komen het vaakst voor.
   Eén op de vier malware-aanvallen draait om losgeld.
3. Belgische kmo's zijn zeer **heterogeen** in hoe ze hun beveiliging aanpakken.

Methodologie

Doelgroep

De ondervraagde kmo's hadden 25 tot 250 medewerkers en kwamen uit uiteenlopende sectoren met uitsluiting van ICT-diensten.

Respondenten

De respondenten waren CEO's, CIO's en andere medewerkers met beslissingsmacht.

Datacollectie

Mix van kwalitatieve face-to-face diepte-interviews van 60 minuten en een online enquête.

Steekproefomvang

122 Belgische kmo's namen deel aan het kwalitatief en kwantitatief onderzoek.

- 63% uit het Vlaams Gewest
- 29% uit het Waals Gewest
- 8% uit het Brussels Hoofdstedelijk Gewest

Onderzoeksperiode

Proximus onderzocht van november 2019 tot februari 2020 de cybersecurity bij Belgische kmo's.

‘Je kan zoveel securitytoepassingen installeren als je wil. Als de gebruikers hun verstand niet gebruiken, heeft dat geen zin.’

respondent a

Onderzoeksresultaten

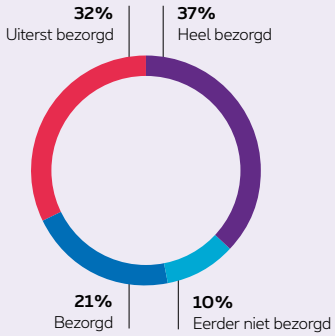
Cybersecurity = topprioriteit

Kmo’s zijn vaak minder goed beveiligd dan grotere bedrijven, maar beschikken evengoed over gevoelige data, zoals klantgegevens van personen of bedrijven, intellectuele eigendomsrechten enzovoort. **In 2018 steeg de schade door cyberaanvallen tegen Belgische kmo’s met maar liefst 194 (!) procent,** becijferde Vanbreda Risk & Benefits in haar Cyberstudie 2019.

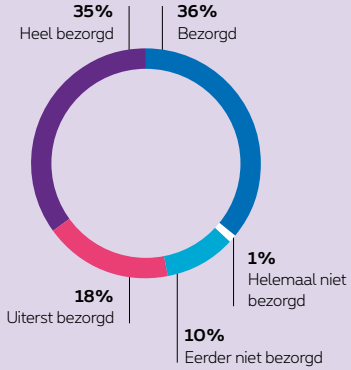
- Alle respondenten gaven aan dat cybersecurity een **topprioriteit** is.
- De meest voorkomende beveiligingsrisico’s die de respondenten zien, zijn **gebruikers** en **mobiele toestellen**.
- Belgische kmo’s liggen wakker van **gegevensbeveiliging** (datalekken) en **bedrijfsstoringen** (bedrijfscontinuïteit) door cyberaanvallen.

Negen op tien kmo’s zijn bezorgd om aangevallen te worden. Het valt op dat kmo’s die in het verleden al te maken kregen met een cyberaanval meer bezorgd zijn voor een nieuwe aanval dan kmo’s die aangeven dat ze nog niet aangevallen zijn.

Hoe bezorgd bent u over de mogelijkheid opnieuw slachtoffer te worden van een cyberaanval?



Hoe bezorgd bent u over de mogelijkheid slachtoffer te worden van een cyberaanval?



Eén op de vijf ondervraagde Belgische kmo's slachtoffer.

Aantal en soorten aanvallen

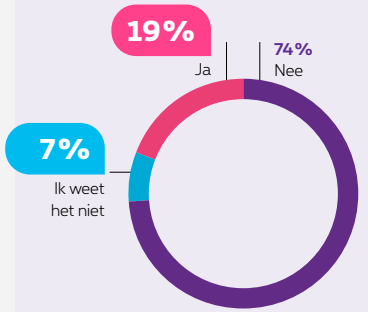
Begin 2020 lagen verschillende Belgische bedrijven weken stil door een cyberaanval. Gelukkig is lang niet elke aanval zo ingrijpend. Het Amerikaanse Ponemon Institute berekende dat **56 % van de kmo's in de Benelux – al dan niet bewust – een cyberaanval onderging in 2019.**

Eén op de vijf ondervraagde Belgische kmo's getroffen.

- **19 procent** van de Belgische kmo's geeft aan in 2019 **slachtoffer** van een cyberaanval te zijn geweest. [1]
- **7 procent** (!) van de ondervraagde kmo's **weet niet** of ze werden aangevallen of niet.
- Van de kmo's die aangeven niet aangevallen te zijn, is maar 22 procent daar heel zeker van. (20 procent antwoordt het niet zeker te weten.)
- Ook opvallend: 16 procent van de respondenten weet niet zeker hoe lang de aanval al gestart was voor ze hem ontdekten.

1. Dat is veel minder dan de 56 procent uit het onderzoek van het Ponemon Institute. Mogelijk ondervonden Belgische kmo's geen hinder van de aanvallen of weten ze niet dat ze aangevallen werden.

Is uw onderneming in 2019 slachtoffer van een cyberaanval geweest?



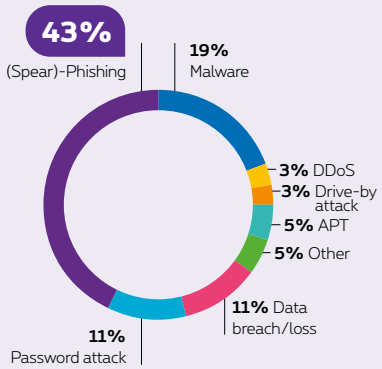
Veel phishing maar ook malware-aanvallen

- **Phishing** is de meest voorkomende soort aanval met 43 procent. Daarna volgen **malware (19%)** en **paswoordhacks (11%)**.

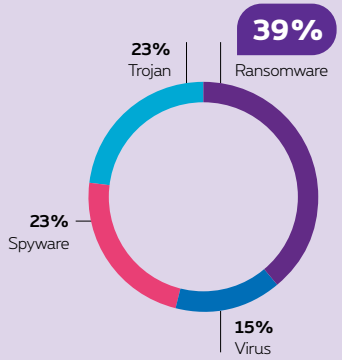
- **Vier malware-aanvallen op de tien** draaien om **losgeld** (ransom).

Om phishing en ransomware te voorkomen, is een beveiligingsstrategie voor de **smartphones** van uw medewerkers onontbeerlijk. Op een kleiner scherm is de kans nog groter dat medewerkers op een onbetrouwbare url klikken en hackers met één voet binnen raken. Combineer minstens een platform voor mobile device management met voldoende opleiding en sensibilisering voor uw medewerkers.

Om welke soort aanval ging het?



In geval van malware, welke malware?



‘Datadiefstal is een nachtmerrie. Soms lig ik echt wakker van de mogelijke gevolgen daarvan.’

respondent b

‘Ik mag er niet aan denken dat je alles moet stilleggen. Dat kost je duizenden euro’s per uur.’

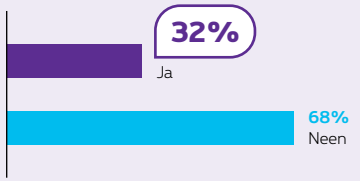
respondent c

Zware gevolgen

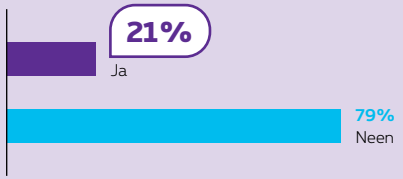
Een cyberaanval kan verstrekkende gevolgen hebben voor bedrijven. Verzekeringsmaatschappij Hiscox berekende dat de **gemiddelde kost** van cyberaanvallen op Belgische ondernemingen in 2019 gemiddeld **441.000 euro** (of 486.000 dollar) bedroeg.

- **32 procent** van de respondenten geeft aan dat hun medewerkers **niet meer konden werken** als gevolg van de cyberaanval.
- Bij **21 procent** van de ondervraagden gingen er **bedrijfsgegevens** verloren of werden er bedrijfsgegevens ontoegankelijk gemaakt.

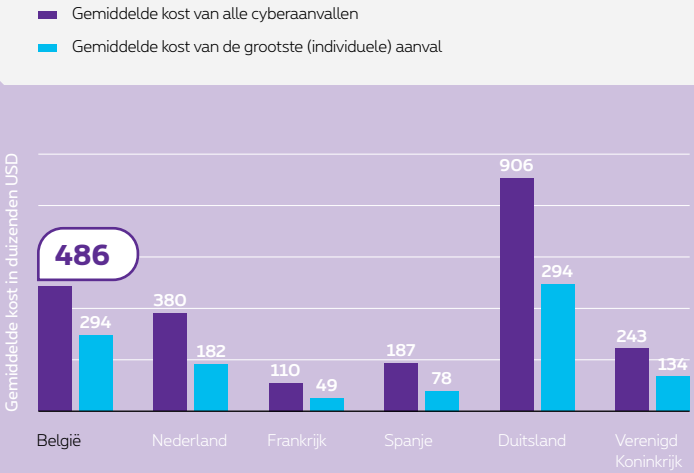
Was de aanval van die aard dat de medewerkers van uw bedrijf niet meer konden werken?



Gingen er gegevens verloren of werden er gegevens geblokkeerd?



486.000 dollar. Dat is de gemiddelde kost van alle cyberaanvallen bij Belgische bedrijven in 2019.



Bron: Onderzoek van Hiscox: Forrester Research, 2019

Security aanpak

Wel een firewall, geen encrypted hard drive

De meeste kmo's hebben een degelijk beveiligde voordeur, maar een goede huisvader gaat een stuk verder om ongewenste gasten te voorkomen. Voor welke beveiligingsoplossingen kiezen kmo's om het **veilig** maar ook **betaalbaar** te houden? Heel wat slimme ingrepen beveiligen uw ICT-infrastructuur zonder dat ze grote investeringen vergen.

Hoe beschermt u zich?

Bijna altijd geïmplementeerd	Soms geïmplementeerd	Zelden geïmplementeerd
• firewalls	• spam- en reputatiefilters	• managed security services
• backups	• advanced threat protection	• Multi-factor authentificatie
• antivirus	• wifi guest netwerk	• encrypted hard drives
		• proxy server
		• ethical hacking
		• cyberverzekering

‘Ik ben helemaal geen computerwetenschapper en ik heb er soms weinig tijd voor, maar cybersecurity hoort bij mijn verantwoordelijkheden.’

respondent d

Veel doe-het-zelvers

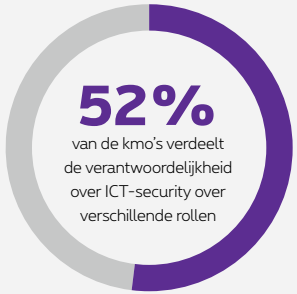
De ICT-kennis en het vertrouwen in externe partners bepalen hoe een kmo haar cybersecurity regelt.

Kmo’s organiseren het beheer en de monitoring van hun security omgeving op zeer uiteenlopende manieren.

- 41 procent beheert en monitort volledig **zelf** zijn security infrastructuur.
- Een derde van de kmo’s verdeelt de securitytaken over **eigen medewerkers** en een ICT **partner**.
- Een kwart van de kmo’s besteedt het beheer uit aan een **ICT partner**.

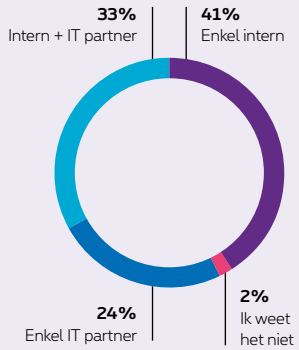
Versnipperde verantwoordelijkheid

Bij iets meer dan de helft (52%) van de kmo’s zit de verantwoordelijkheid over cybersecurity verdeeld over verschillende profielen binnen het bedrijf.

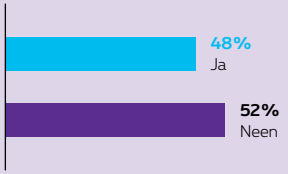


bron: Untangle 2019 SMB IT Security Report

Wie monitort en beheert uw security infrastructuur?



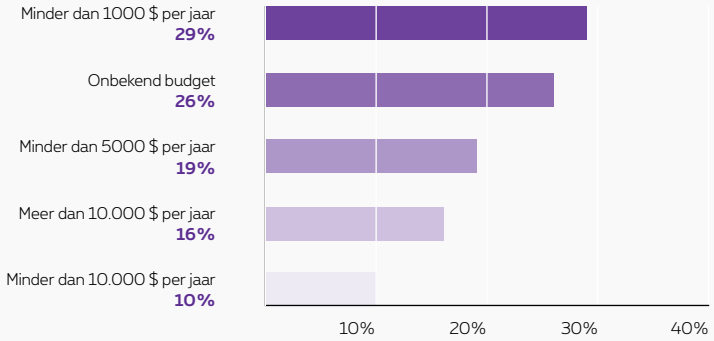
Is er één verantwoordelijke aangeduid voor cybersecurity binnen uw kmo?



Bescheiden budgetten

29 procent spendeert minder dan 1000 euro per jaar aan cybersecurity.

Welk budget spendeert uw kmo jaarlijks aan cybersecurity?

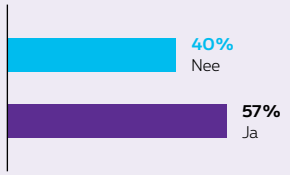


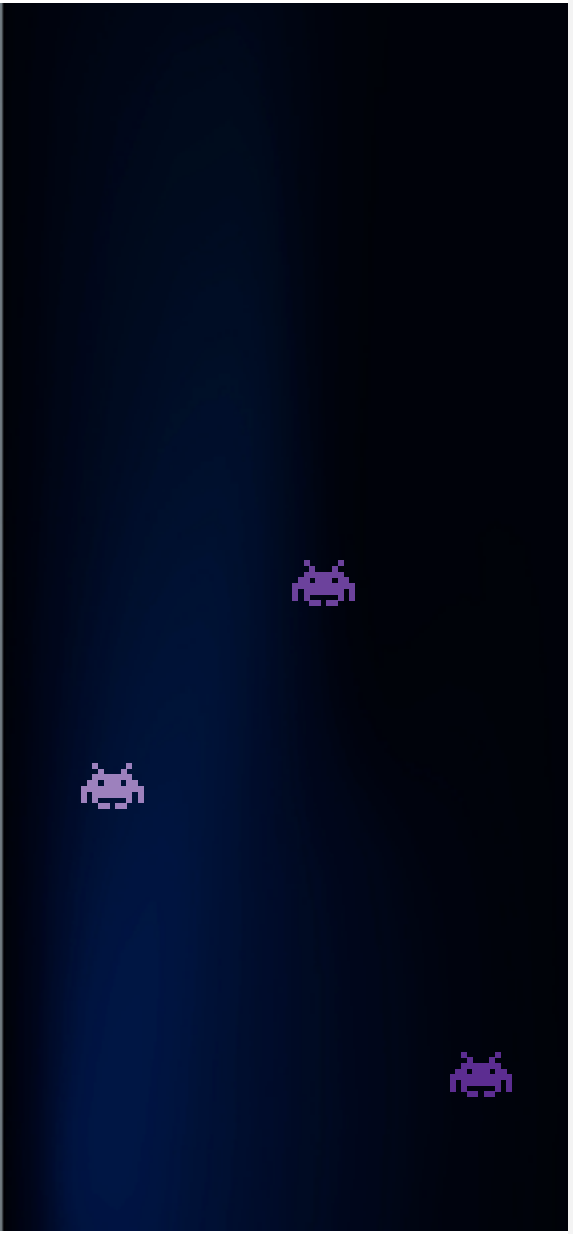
bron: Untangle 2019 SMB IT Security Report

Eén kmo-werknemer op de drie krijgt geen security-opleiding

Een ketting is maar zo sterk als haar zwaktste schakel. Een bedrijf mag dan over een gesofisticeerd alarmsysteem beschikken, als een medewerker de achterdeur vergeet te sluiten, heeft dat weinig impact. **Menselijk handelen** geldt als de **zwakste factor** in cybersecurity. Medewerkers bewustmaken van cyberrisico's is een essentieel onderdeel van elke beveiligingsaanpak.

Krijgen uw medewerkers opleidingen over hoe ze het best omgaan met de digitale toestellen en gegevens van uw onderneming?





Beveilig uw bedrijf in 4 stappen

En u? Hoe stelt u uw plan voor gemoedsrust op?

1. Bepaal uw profiel

Kies wat kritisch is en wat minder kritisch:	› Weeg voor elk onderdeel de beveiligingskost af tegenover de mogelijke impact van een aanval.
Maak een lijst van de kritieke **operaties** en vitale **bedrijfsmiddelen** die u moet beschermen:	› Welke **systemen, netwerken, ICT-toestellen, ICT-toepassingen en data** zijn essentieel voor uw onderneming? › Inventariseer alle **kantoren, toestellen en gegevens** die u moet beveiligen. › Breng in kaart waartoe **medewerkers toegang** moeten hebben en waartoe niet. › Denk ook aan **fysieke beveiliging**: zorg bijvoorbeeld dat niet eender welke bezoeker zomaar uw serverlokaal kan binnenstappen.
Beslis wat u **intern** wil doen en wat **extern**. Beschikt u over voldoende knowhow en mankracht om alles zelf op te volgen? Denk hierbij aan:	› design en implementatie van je veiligheidsinfrastructuur (zie hieronder) › opvolging en incidentenbeheer (zie hieronder) › tests en opleidingen (zie hieronder).

2. Design en zet uw beveiliging op

- **Ontwerp** zelf of met een partner uw volledige 360° veiligheidsinfrastructuur. Teken bijvoorbeeld uit hoe u uw interne netwerk het best opsplitst. Tussen welke netwerken plaatst u extra firewalls? Wie heeft toegang tot wat? Enzovoort. Vergeet zeker ook niet een systeem voor e-mailbeveiliging, ook al hebt u Office 365. Ook multi-factor authenticatie en een goede back-up strategie mogen niet ontbreken.
- Stel een **stappenplan** op voor de implementatie van nieuwe infrastructuur. Houd er ook rekening mee dat u voor sommige installaties uw dienstverlening moet onderbreken.
- **Documenteer** alle instellingen, serienummers, soft- en hardewareversies, locaties in het gebouw, kabels enz.

3. Volg op en maak een incidentenplan

- Stel procedures in om **7 dagen** per week en **24 uur** per dag beveiligings-waarschuwingen op te volgen.
- Zorg dat iemand geregeld de **status** en **logs** van uw beveiligingsoplossingen nakijkt.
- Leg vooraf vast wat u gaat doen bij een incident. **Wie reageert, hoe snel, met welke middelen**? Wie brengt u op de hoogte? Wie heeft de eindverantwoordelijkheid?

4. Test, leid op en boek succes

- Organiseer een oefencase om je incidentenplan te testen.
- Leid medewerkers op om slim om te gaan met toestellen en gegevens van uw bedrijf.
- Geniet van gemoedsrust dankzij een 360°-bescherming en bouw uw business verder uit.

Het aanbod-op-maat van Proximus

Ontdek de 360°-aanpak van Proximus voor de cybersecurity van uw kmo. Kies zelf wat u wil: van volledige ontzorging tot specifieke security services.

Een degelijke basisbeveiliging hoeft niet duur te zijn.
Ga voor onze 360°-benadering:

Voorspel

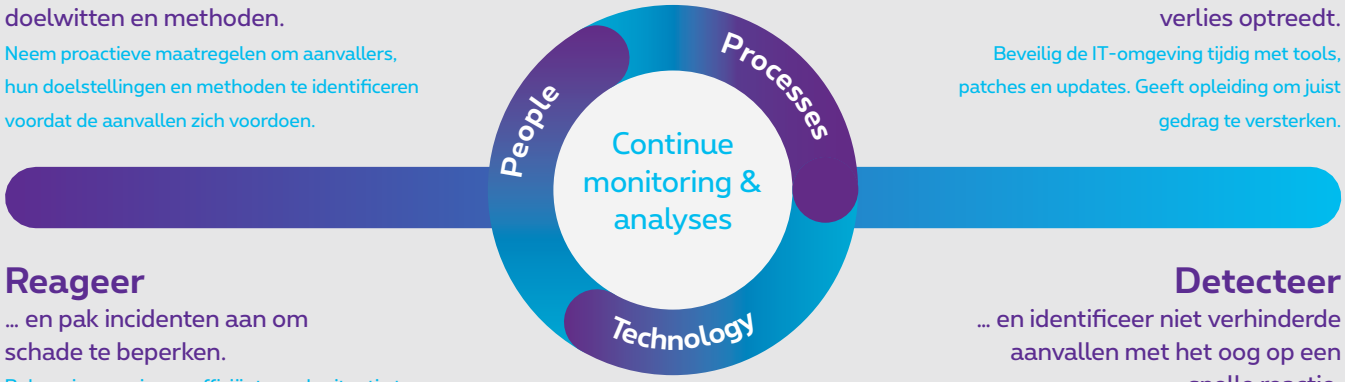
... de meest waarschijnlijke aanvallen, doelwitten en methoden.

Neem proactieve maatregelen om aanvallers, hun doelstellingen en methoden te identificeren voordat de aanvallen zich voordoen.

Voorkom

... of belet aanvallen zodat er geen verlies optreedt.

Beveilig de IT-omgeving tijdig met tools, patches en updates. Geeft opleiding om juist gedrag te versterken.



Reageer

... en pak incidenten aan om schade te beperken.

Beheer inspanningen efficiënt om de situatie te bedewingen en te herstellen zodat de IT-omgeving terug normaal kan functioneren.

Detecteer

... en identificeer niet verhinderde aanvallen met het oog op een snelle reactie.

Controleer belangrijke activiteiten op aanvallen. Identificeer tijdig problemen, lekken en aanvallen.

Audit of verbetertraject. We analyseren uw aanpak en stellen acties voor om uw beveiliging te verbeteren.

Consultancy en design. We geven advies en ontwerpen een veilige digitale omgeving voor uw bedrijf. We brengen risico's en kosten in kaart en stippelen samen uw beveiligingsbeleid uit.

Opvolging en advies. Onze beveiligingsconsultants volgen uw digitale omgeving op en evalueren geregeld uw beveiligingsverslagen. Ze formuleren advies en verbetervoorstellen.

JA,
ik wil een verkennend adviesgesprek

Oplossingen op maat die we voor u kunnen implementeren:

- Netwerkbeveiligingsoplossingen zoals hypergeavanceerde firewalls, netwerktoegangscontrole en webbeveiliging.
- Advanced Threat Protection-oplossingen zoals intrusiepreventiesystemen, DDoS-beveiliging, geavanceerde malwarebescherming en SSL encrypted traffic visibility.
- Web application firewalls, XML-gateway, preventie van gegevensverlies, e-mailbeveiliging en strong authentication.
- Endpoint protection-oplossingen die bescherming bieden voor (mobiele) eindpunten en (virtuele) servers
- 'Managed Security Services': Remote services om de belangrijkste beveiligingscomponenten van een ICT omgeving op te volgen en te beheren.
- Remote Operations Center (ROC) dat 24 uur per dag en 7 dagen per week de nieuwste dreigingen opvolgt en indien nodig proactief ingrijpt.

Bronnen

www.proximus.be
www.ictportal.nl/ict-lexicon/cybersecurity-woordenboek

Proximus & cybersecurity

De Proximus-groep is de Belgische marktleider in telecom- & IT-diensten. De groep is actief in de Benelux en bedient residentiële klanten, ondernemingen en openbare diensten. Proximus heeft de ambitie om bedrijven te begeleiden op hun weg naar digitale transformatie, door de beste connectiviteitsmiddelen (bv. fiber, 5G, ...) te verenigen met expertise in domeinen zoals Cloud, het Internet of Things (IoT), Big Data en Cyber Security om zo tot oplossingen met een doorslaggevende impact te komen.

Proximus is een vertrouwde partner om te helpen bij het uitwerken en implementeren van een evenwichtige beveiligingsstrategie.

- Samen met haar filialen beschikt Proximus over meer dan 350 werknemers die gespecialiseerd zijn in cyber security.

  - Davinsi Labs
  - Spearit
  - Telindus Luxemburg
  - Telindus Nederland

- Proximus heeft meer dan 20 jaar ervaring in cybersecurity:

- Proximus is lid van verschillende cyber security verenigingen voor het uitwisselen van best practices: Cyber Security Coalition, ETIS, Beltug, enz. Hierdoor zijn we steeds op de hoogte van de allerlaatste nieuwigheden. Deze kennis wenden we aan om onze klanten nog beter te beschermen.

Wenst u meer informatie?

Surf naar www.proximus.be/security of neem contact op met één van onze security experten.

Cybersecurity-lexicon

Of u de cybersecurity van uw kmo nu zelf opvolgt of niet: dankzij deze 25 securitytermen kunt u uw bedrijf beter beveiligen. Praat mee met interne of externe security specialisten en til uw gemoedsrust naar een hoger niveau.

1. **Advanced Threat Protection** (ATP) Software die beveiliging biedt tegen onveilige bijlagen en schadelijke koppelingen naar onveilige websites.

2. **Audit log** Bestand waarin is vastgelegd wanneer, wie, wat heeft gedaan in je computersysteem.

3. **Bot** Een computerprogramma dat zelfstandig taken kan uitvoeren. Bot is een afkorting van robot.

4. **Captcha** Afkorting van “Completely automated public turing test to tell computers and humans apart”. Manier om te controleren of de gebruiker een mens is.

5. **CEO/CFO-fraude** Vorm van fraude waarbij een aanvaller e-mails stuurt aan een financiële afdeling uit naam van de CEO of CFO van een bedrijf. De aanvaller wil hiermee een medewerker overtuigen of onder druk zetten om geld over te maken.

6. **Cloud Access Security Broker** (CASB) Een beveiligingsoplossing voor toepassingen in de cloud waarbij men een schakel plaatst tussen het bedrijfsnetwerk en de cloud.

7. **Cyberverzekering** Verzekering die betaalt voor financiële schade als gevolg van een cyberaanval. De verzekering betaalt niet alleen voor schade bij de organisatie zelf, maar ook voor de schade die je aan anderen moet vergoeden.

8. **Distributed Denial of Service** (DDoS) Aanval om een dienst onbeschikbaar te maken door een server, applicatie, netwerk, enz. met nutteloos dataverkeer te overspoelen.

9. **Firewall** Een verzameling computerprogramma’s of -apparatuur die een netwerk beschermt.

10. **Insider threat** Dreiging die haar oorsprong heeft binnen de organisatie. Bijvoorbeeld doordat medewerkers, oud-medewerkers en leveranciers bij informatie kunnen komen.

11. **Managed security service** Het op afstand beheren en monitoren van de security-omgeving van een bedrijf door een derde partij.

12. **Meerfactor authenticatie** Methode om vast te stellen of een gebruiker of digitaal systeem wel is wie of wat hij zegt te zijn. U gebruikt hiervoor verschillende manieren. Bijvoorbeeld een wachtwoord en een code die de gebruiker per sms krijgt.

13. **Mobile device management** (MDM) Zorgt dat mobiele apparaten in een organisatie goed beheerd en beveiligd worden. Bijvoorbeeld door een pincode in te stellen voor smartphones en tablets. Of door te zorgen dat u op afstand gegevens op die apparaten kunt wissen.

14. **Netwerktoegangs – beheer** Manier om een netwerk beter te beveiligen door alleen bekende en geautoriseerde apparaten op het netwerk toe te laten.

15. **Phishing** Aanval waarbij de aanvaller iemand verleidt om belangrijke informatie te geven, zoals inlog- of creditcardgegevens. Phishing gebeurt vaak via e-mail, maar ook via telefoon, sms of een ander bericht.

16. **Privacy Impact Assessment** Onderzoek waarmee een organisatie inzicht krijgt in de privacyrisico's.

17. **Ransomware** Goed voorbereide aanval waarbij gegevens geëncrypteerd worden of ontoegankelijk gemaakt worden. De aanvaller belooft je een sleutel om je gegevens te "bevrijden" in ruil voor "losgeld" (ransom).

18. **Remote Operations Center** Afdeling die 24 uur per dag en 7 dagen per week de nieuwste dreigingen opvolgt. Zo kan ze snel en proactief reageren om risico's af te wenden.

19. **Role based access control** Bepaalt of een gebruiker bij een computersysteem mag komen. Men kijkt daarbij naar de rol die de gebruiker of een groep gebruikers heeft. Voorbeelden van rollen zijn viewer, editor en manager.

20. **Rule based detection** Methode om een cyberaanval te ontdekken. U bepaalt vooraf welke patronen of tekens in data op een netwerk verdacht kunnen zijn. Daarna zoekt het systeem naar die patronen of tekens.

21. **Sandbox** Afgeschermd deel in een digitaal systeem. Software die op deze plek werkt, kan geen andere processen in de computer verstoren. Men gebruikt een sandbox om software in te draaien die vaak aangevallen wordt. Of om te testen of iets malware is en wat het dan doet.

22. **Single sign on** (SSO) Eindgebruikers loggen één keer in en kunnen daarna in verschillende applicaties en onderdelen van het netwerk werken. Ze hoeven dus niet meer elke keer opnieuw inloggegevens in te voeren.

23. **Spamfilter** Software die spam en computervirussen probeert te herkennen en te verwijderen.

24. **Spoofing** De aanvaller verbergt zijn identiteit of doet zich voor als een andere gebruiker / iemand anders (masquerading, source routing).

25. **Spyware** Vorm van malware. Spyware is software waarmee men ongemerkt informatie verzamelt en doorstuurt. Vaak gaat het om toetsaanslagen, screenshots, e-mailadressen, surfgedrag of persoonlijke informatie zoals een creditcardnummer.

Bronnen

www.proximus.be

www.ictportal.nl/ict-lexicon/cybersecurity-woordenboek


proximus
enterprise