juin 2020

+ lexique de la cybersécurité

Mission ‘Tranquillité d’esprit’

Le rapport de l’étude ‘Les PME belges et la Cybersécurité’

proximus
enterprise

Contenu

Préface

Dans le monde, les cyberattaques s'intensifient d'année en année. Elles ciblent de plus en plus les PME.

Les bureaux d'études internationaux analysent régulièrement le paysage de la cybersécurité. Malheureusement, leurs chiffres ne sont pas toujours représentatifs des PME belges. Pour combler cette lacune, Proximus a mené une double étude – qualitative et quantitative – ***auprès de 122 petites et moyennes entreprises belges.***

En voici les 3 conclusions majeures :

1. **Pour 9 PME belges sur 10,** les cyberattaques sont **une source de préoccupation.**
2. Les attaques par **phishing** sont les plus fréquentes. Une rançon est demandée dans 1 cyberattaque sur 4.
3. Les PME belges ont une approche très **hétérogène** de leur cybersécurité.

Méthodologie

Groupe cible

Les PME interrogées comptent entre 25 et 250 collaborateurs. Elles sont actives dans de multiples secteurs (à l'exception des services ICT).

Répondants

Les répondants sont les CEO, CIO et autres décideurs de l'entreprise.

Collecte des données

Combinaison entre une enquête via internet et des entretiens approfondis de 60 minutes en face-à-face.

Échantillon

Quelques 122 PME belges ont participé à l'étude quantitative et qualitative.

- 63% en Flandre
- 29% en Wallonie
- 8% à Bruxelles

Période

Proximus a étudié la cybersécurité dans les PME belges entre novembre 2019 et février 2020.

‘Vous pouvez installer toutes les applications de sécurisation du monde, cela ne sert à rien si vos utilisateurs ne font pas preuve de bon sens.’

répondant a

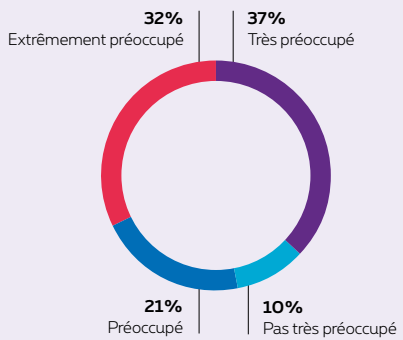
Les résultats

Cybersécurité = priorité absolue

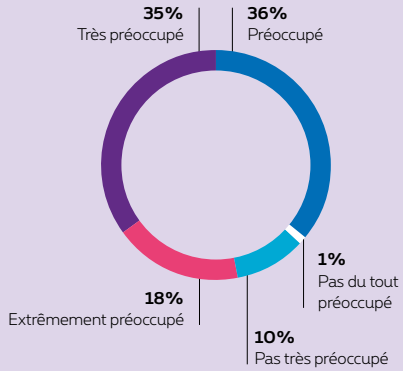
- Les PME sont généralement moins bien protégées que les grandes entreprises, mais possèdent également des informations sensibles, telles que les données clients (personnes ou entreprises), des droits de propriété intellectuelle, etc. **En 2018, les dommages occasionnés par les cyberattaques ciblant des PME en Belgique ont augmenté de 194% !** (source : Cybersurvey 2019, Vanbreda Risk & Benefits).
- Tous les répondants indiquent que la cybersécurité est **une priorité absolue.**
- Les deux sources de risques les plus fréquemment citées sont **les utilisateurs** et **les appareils mobiles.**
- Les PME belges sont surtout préoccupées par **la protection des données** (fuites) et **la continuité de leurs activités** (perturbations) engendrées par les cyberattaques.

9 PME sur 10 sont préoccupées par le risque de cyberattaque. À noter : les entreprises qui ont déjà été victimes d’une attaque sont davantage soucieuses des risques que les PME qui n’ont encore jamais subi une cyberattaque.

Êtes-vous préoccupé par la possibilité d’être à nouveau victime d’une cyberattaque ?



Êtes-vous préoccupé par la possibilité d’être victime d’une cyberattaque ?



1 PME belge interrogée sur 5 a été touchée

Nombre et types de cyberattaques

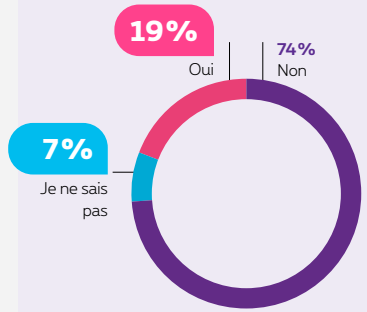
Au début 2020, une cyberattaque a contraint plusieurs entreprises belges à interrompre leurs activités pendant plusieurs semaines. Heureusement, toutes les attaques n'ont pas de telles conséquences. Le Ponemon Institute (USA) a calculé que **56% des PME du Benelux ont subi une cyberattaque en 2019, à leur insu ou non.**

1 PME belge interrogée sur 5 a été touchée

- 19% des PME belges indiquent avoir été **victimes** d'une cyberattaque en 2019.[1]
- **7%** (!) des PME interrogées **ne savent pas** si elles ont été attaquées ou non.
- Parmi les entreprises indiquant ne pas avoir été attaquées, seulement 22% en sont sûres. (20% ne peuvent répondre avec certitude)
- Autre observation marquante : 16% des répondants indiquent ne pas savoir quand l'attaque a commencé (avant d'être découverte).

1. Ce pourcentage est nettement inférieur aux 56% de l'étude du Ponemon Institute. Explications possibles : peut-être les PME belges ne savent-elles pas qu'elles ont été attaquées et/ou peut-être n'en ont-elles subi aucun préjudice.

Votre entreprise a-t-elle été victime d'une cyberattaque en 2019 ?



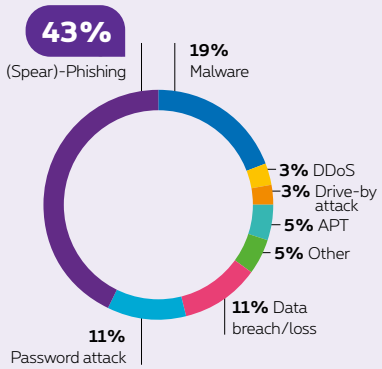
Beaucoup de phishing, mais aussi du malware.

- Le **phishing** est le type d'attaque le plus fréquent, avec **43%.** Viennent ensuite les **malwares (19%)** et les **passwordhacks (11%).**

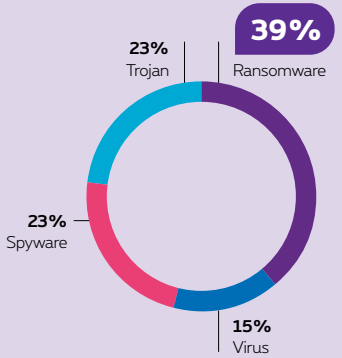
- **4 attaques malware sur 10** débouchent sur une demande de **rançon.**

Pour prévenir le phishing et le ransomware, la sécurisation des appareils mobiles de vos collaborateurs (smartphones, tablettes, PC portables) est une composante cruciale de votre stratégie. Lorsque l'écran est de petite dimension (smartphone) et n'affiche les informations que de manière simplifiée, le risque est encore plus grand de voir vos clients cliquer sur un lien malveillant, et de permettre ainsi aux hackers d'accéder à vos systèmes. Pour prévenir cette menace, deux éléments au moins doivent être combinés : la sensibilisation/formation de vos collaborateurs, ainsi que le déploiement d'une plateforme de gestion des appareils mobiles dotée d'une Threat Protection.

De quel type d'attaque s'agit-il ?



En cas de malware, quel type de malware?



‘Le vol de données est un vrai cauchemar. Quand je pense aux conséquences potentielles, je n’en dors plus’

répondant b

‘Tout arrêter ? Je n’ose pas l’imaginer. Ça nous coûterait des milliers d’euros à l’heure.’

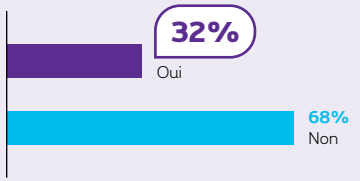
répondant c

De lourdes conséquences

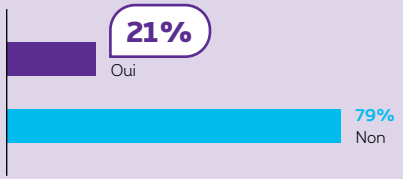
Les cyberattaques peuvent avoir de lourdes conséquences pour les entreprises. La compagnie d’assurances Hiscox a calculé que **le coût moyen** des cyberattaques subies par les entreprises belges en 2019 se montait à **441.000 euros.**

- **32%** des répondants indiquent que leurs collaborateurs n’ont **plus été en mesure de travailler** en raison de la cyberattaque.
- Pour **21%** des répondants, la cyberattaque s’est soldée par **la perte de données de l’entreprise,** ou par l’impossibilité d’encore accéder à ces informations.

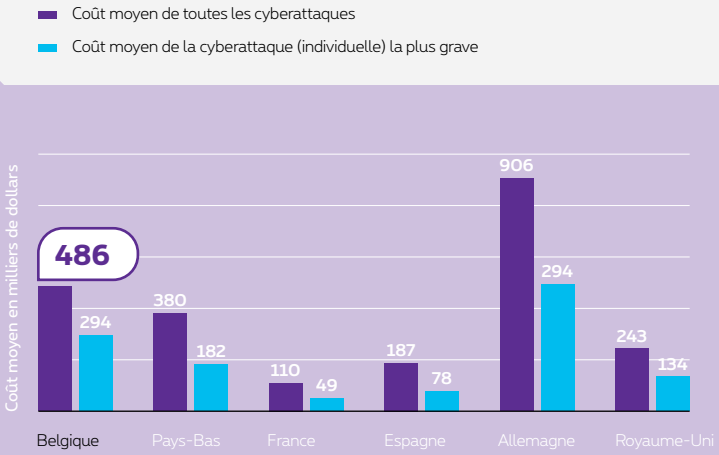
La cyberattaque a-t-elle empêché vos collaborateurs de continuer à travailler ?



Des données ont-elles été perdues ou sont-elles devenues inaccessibles ?



486.000 dollars. Voilà le coût moyen des cyberattaques sur les entreprises belges en 2019.



Source : étude Hiscox, Forrester Research, 2019

Comment sécuriser ?

Un pare-feu, pas de disque dur crypté

La plupart des PME protègent efficacement l'accès depuis l'extérieur mais, pour sécuriser réellement leurs activités, elles doivent aller plus loin. Quelles sont les solutions de sécurisation choisies par les PME, qui sont à la fois **efficaces** et **financièrement abordables** ? Ici, retenez que de très nombreuses solutions de sécurisation de votre infrastructure ICT ne requièrent pas d'investissement substantiel.

Comment vous protégez-vous ?

Presque toujours mis en œuvre

- Pare-feu
- Sauvegardes
- Antivirus

Parfois mis en œuvre

- Filtres anti-spam et de réputation
- Advanced threat protection (ATP)
- Réseau de 'guest wifi'

Rarement mis en œuvre

- Système de sécurité géré
- Authentification multifactorielle
- Disques durs cryptés
- Proxy server
- Piratage éthique
- Cyber assurance

‘Je ne suis pas expert en informatique et je n’ai pas toujours le temps de m’en occuper, mais la cybersécurité fait partie de mes responsabilités.’

répondant d

Do-it-yourself à l’honneur

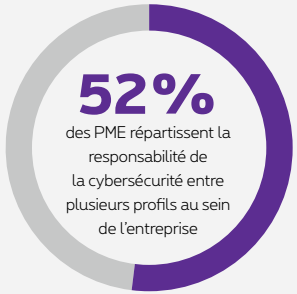
L’approche de la cybersécurité par les PME dépend de leur maîtrise ICT et de leur confiance dans des partenaires extérieurs.

Les PME organisent de multiples manières la gestion et le monitoring de leur environnement de sécurité.

- 41% d’entre elles gèrent et supervisent **elles-mêmes** leur infrastructure de sécurité.
- 33% des PME répartissent leurs missions sécuritaires entre **leurs propres collaborateurs** et **un partenaire ICT externe.**
- 25% des PME externalisent ces missions et les confient à **un partenaire ICT.**

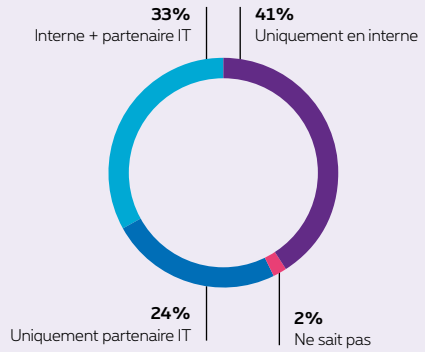
Responsabilités morcelées

Dans plus de la moitié des PME (52%), la responsabilité de la cybersécurité est répartie entre plusieurs profils au sein de l’entreprise.

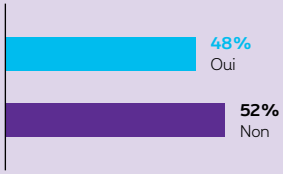


Source: Untangle 2019 SMB IT Security Report

Qui gère et supervise votre cybersécurité ?



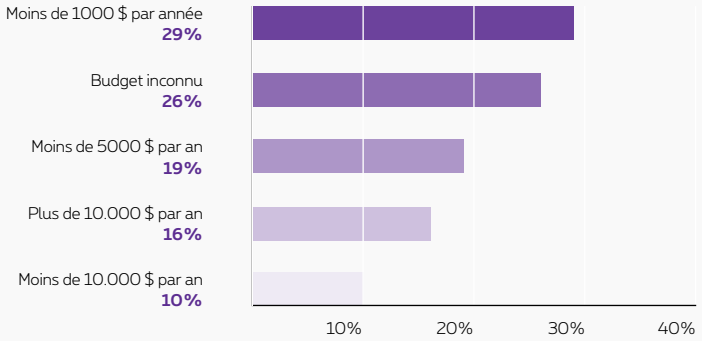
Dans votre PME, y a-t-il officiellement un seul responsable de la cybersécurité ?



Des budgets modestes

29% des PME consacrent moins de 1.000 euros par an à leur cybersécurité.

Quel est le budget annuel consacré par votre PME à la cybersécurité ?

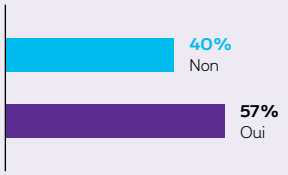


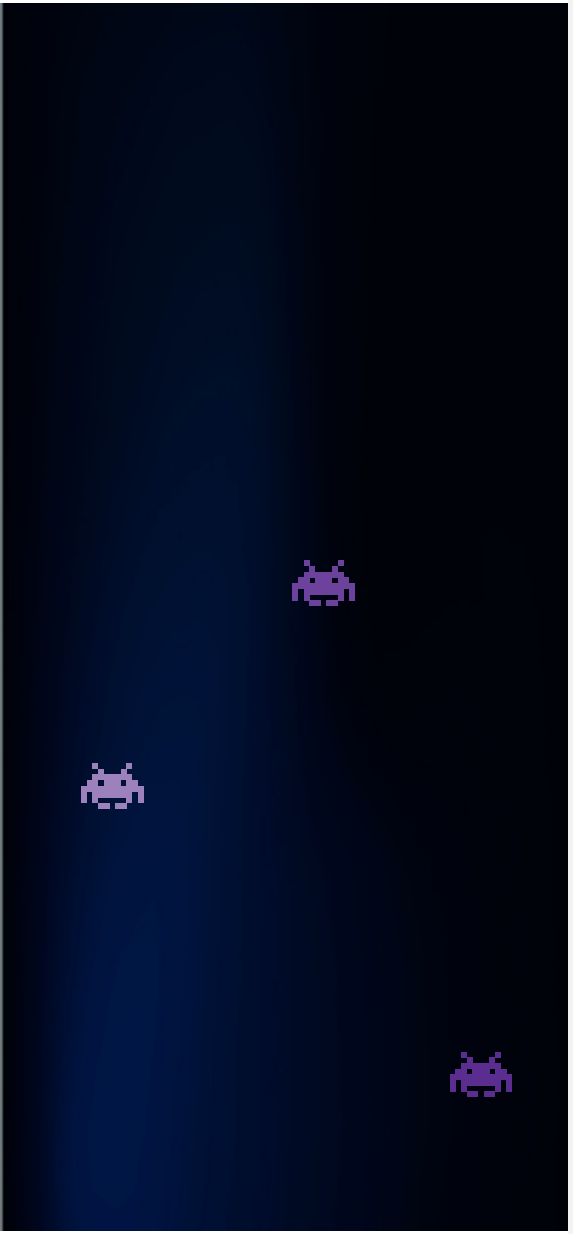
Source : Untangle 2019 SMB IT Security Report

1 collaborateur sur 3 ne bénéficie d'aucune formation en cybersécurité

'La résistance d'une chaîne est celle de son plus faible maillon', a-t-on coutume de dire. Une entreprise a beau disposer d'un système d'alarme sophistiqué, ce système ne sert à rien si un collaborateur oublie de fermer la porte en sortant. Très souvent, **le facteur humain est le maillon le plus faible** de la cybersécurité. La sensibilisation du personnel aux cyberrisques est une des clés de voûte de toute approche de la sécurité informatique.

Vos collaborateurs bénéficient-ils de formations à l'utilisation des appareils numériques et des données de votre entreprise ?





Protégez votre entreprise en 4 étapes

Et vous ? Comment mener à bien votre 'Mission Cybersécurité ?

1. Définissez votre profil

Inventoriez les éléments critiques (et non critiques).	› Pour chacun de ces éléments, calculez le coût de la sécurisation par rapport aux conséquences potentielles d'une attaque.
Inventoriez **vos processus critiques** et **vos ressources vitales** à protéger.	› Quels sont les **systèmes, réseaux, appareils ICT, applications ICT et données** qui sont essentiels aux activités de votre entreprise ? › Inventoriez tous les **bureaux** et **appareils** à protéger. › Déterminez les éléments auxquels vos collaborateurs doivent **avoir accès**, ou non. › Pensez aussi à **la sécurisation physique**. Exemple : vos visiteurs ne doivent pas pouvoir accéder à la pièce où est installé votre serveur.
Choisissez les missions de sécurité à gérer **en interne**, et celles qui peuvent/doivent être **externalisées**. Demandez-vous si vous disposez des ressources (personnel et savoir-faire) suffisantes pour vous charger de toutes les missions en interne. Pensez notamment à :	› La conception et le déploiement de votre infrastructure de sécurité (voir ci-dessous) › La gestion et le suivi des incidents (voir ci-dessous) › Les tests et la formation (voir ci-dessous)

2. Concevez et déployez votre système de sécurité

- **Concevez** vous-même ou avec l'aide d'un partenaire votre infrastructure globale de sécurité. Quelle sera la configuration de votre réseau interne ? Entre quels réseaux installerez-vous des pare-feu ? Qui a accès à quoi ? Même si vous disposez d'Office 365, n'oubliez pas de sécuriser votre courrier électronique. Enfin, pensez à l'autorisation à facteurs multiples et à votre stratégie de sauvegarde/restauration.
- Élaborez **un échéancier de déploiement** de votre nouvelle infrastructure. N'oubliez pas que certaines installations ne pourront se faire sans interrompre vos services et activités.
- **Documentez** tous les paramétrages, numéros de série, versions logicielles et matérielles, implantations dans le bâtiment, câblages, etc.

3. Supervisez et élaborez un plan de gestion des incidents

- Définissez des procédures de suivi des incidents, **24 heures sur 24 et 7 jours sur 7.**
- Confiez à un de vos collaborateurs la supervision régulière du **statut** et des **registres** de vos solutions de sécurisation.
- Définissez à l'avance ce que vous ferez en cas d'incident : **qui doit réagir, dans quel délai, avec quels moyens ?** Qui est chargé de vous informer ? Qui est le responsable final ?

4. Testez, formez et performez

- Organisez un exercice, afin de tester l'efficacité de votre plan de gestion.
- Formez vos collaborateurs à la gestion de votre infrastructure.
- Bénéficiez d'une tranquillité d'esprit maximale grâce à une sécurisation tous azimuts, et concentrez-vous sur votre cœur de métier.

La solution sur mesure de Proximus

Découvrez la solution globale de Proximus pour assurer la cybersécurité de votre PME. Choisissez l'option qui vous convient : tranquillité d'esprit totale ou services sécuritaires spécifiques.

Une solide Cybersécurité ne doit pas nécessairement être coûteuse. Optez pour notre approche tous azimuts :

Anticipez

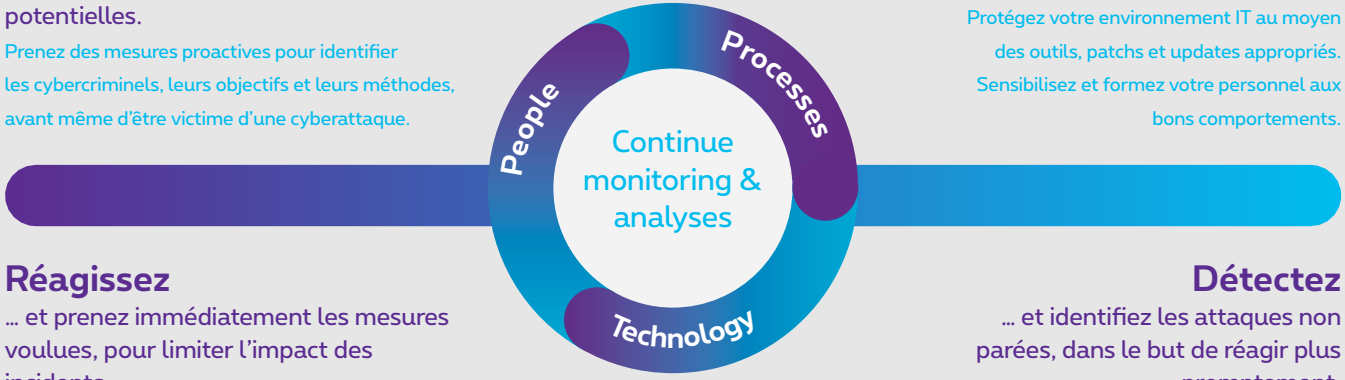
... les attaques, cibles et méthodes potentielles.

Prenez des mesures proactives pour identifier les cybercriminels, leurs objectifs et leurs méthodes, avant même d'être victime d'une cyberattaque.

Prévenez

... et évitez les cyberattaques.

Protégez votre environnement IT au moyen des outils, patchs et updates appropriés. Sensibilisez et formez votre personnel aux bons comportements.



Réagissez

... et prenez immédiatement les mesures voulues, pour limiter l'impact des incidents.

Coordonnez la réaction en cas d'incident, pour en limiter les conséquences et revenir au plus vite à la normale.

Détectez

... et identifiez les attaques non parées, dans le but de réagir plus promptement.

Contrôlez la cybersécurité de vos activités cruciales. Détectez à temps les problèmes, fuites et attaques.

Audit ou trajet d'optimisation. Nous analysons votre approche et vous proposons des mesures/actions de protection.

Consultance et design. Nous vous donnons des conseils et concevons un environnement numérique optimal pour votre entreprise. Nous analysons les risques et les coûts, et définissons ensemble votre politique de cybersécurité.

Suivi et conseil. Nos experts en cybersécurité assurent le suivi de votre environnement et évaluent régulièrement vos rapports de sécurité. Ils formulent des conseils et des propositions d'optimisation.

Solutions sur mesure, que nous pouvons mettre en œuvre pour vous :

- Solutions de protection de réseau telles que pare-feu ultrasophistiqués, contrôle d'accès au réseau et sécurisation web.
- Solutions d'Advanced Threat Protection, telles que les systèmes de prévention d'intrusion, protection DdoS, protection de pointe contre les malwares et SSL encrypted traffic visibility.
- Web application firewalls, XML-gateway, prévention des pertes de données, sécurisation du courrier électronique et *authentification forte*.
- Solutions d'Endpoint Protection, qui sécurisent les points terminaux (mobiles) et les serveurs (virtuels).
- Managed Security Services : téléservices de suivi et de gestion des composantes sécuritaires essentielles d'une IAS (Internet Access Street) ou d'un datacenter.
- Remote Operations Center (ROC), qui supervise 24/7 les nouvelles menaces, et qui agit proactivement si nécessaire.

OUI,
j'aimerai m'entretenir avec vous de la cybersécurité de ma PME !

Sources

www.proximus.be

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

Proximus & cybersecurity

Le groupe Proximus est le n°1 belge des télécoms et des services IT. Le groupe est actif dans le Benelux et sert les particuliers, les entreprises et les services publics. Proximus a pour ambition d'accompagner les entreprises dans leur transformation numérique, en conjuguant les meilleures solutions de connectivité (fibre optique, 5G...) à son expertise dans de multiples domaines – le Cloud, l'Internet of Things (IoT), les Big Data et la Cyber Security – dans le but de faire la différence par l'excellence.

Proximus est votre partenaire à haute fiabilité pour l'élaboration et le déploiement de votre stratégie de cybersécurité.

- Avec ses filiales, Proximus peut compter sur la compétence de plus de 350 experts en cybersécurité.

  - Davinsi Labs
  - Spearit
  - Telindus Luxemburg
  - Telindus Nederland

- Proximus possède plus de 20 ans d'expérience en cybersécurité.

- Proximus est membre de plusieurs associations d'échange de pratiques d'excellence en cybersécurité, telles que Cyber Security Coalition, ETIS, Beltug, etc. Grâce à ces contacts, nous sommes en permanence à la pointe de la nouveauté. Cette expertise est mise à la disposition de nos clients, pour les protéger encore mieux.

Vous souhaitez de plus amples informations ?

Surfez sur www.proximus.be/security ou prenez contact avec un de nos experts.

à conserver

Le lexique de la cybersécurité

Que vous supervisiez vous-même la cybersécurité de votre PME ou non, ces 25 termes vous aideront à mieux sécuriser votre entreprise. Examinez-les avec vos experts internes et externes, et passez à la sécurité supérieure.

1. **Advanced Threat Protection** (ATP) Logiciel de protection contre les annexes malveillantes et les liens vers des sites internet dangereux.

2. **Audit log** Fichier qui enregistre toutes les opérations intervenues dans vos systèmes informatiques : qui, quand, quoi, comment.

3. **Bot** Un programme informatique capable d'effectuer des tâches de manière autonome (abréviation de 'robot').

4. **Captcha** Abréviation de "Completely automated public turing test to tell computers and humans apart". Outil permettant de s'assurer que l'utilisateur est un humain.

5. **CEO/CFO fraud** Cyberarnaque consistant à envoyer des e-mails au département financier, au nom du CEO ou du CFO d'une entreprise, dans le but de convaincre ou de contraindre le destinataire à verser de l'argent.

6. **Cloud Access Security Broker** (CASB) Méthode de sécurisation des applications dans le cloud, qui consiste à intercaler un maillon entre le cloud et le réseau de l'entreprise.

7. **Cyberassurance** Police d'assurance qui couvre le préjudice financier résultant d'une cyberattaque. Ce type d'assurance couvre non seulement les dommages occasionnés à l'entreprise, mais aussi aux tiers.

8. **Distributed Denial of Service** (DDoS) Cyberattaque consistant à submerger un serveur/application/réseau au moyen de flux de données inutiles, afin de rendre le service inopérant.

9. **Pare-feu** Ensemble de programmes et/ou matériels qui ont pour fonction de protéger un réseau.

10. **Insider threat** Menace provenant de l'intérieur même d'une organisation, par exemple lorsque des collaborateurs, ex-collaborateurs ou fournisseurs ont accès à des informations.

11. **Managed security service** Télégestion et télémonitoring par un tiers de l'environnement de sécurité d'une entreprise.

12. **Authentification à facteurs multiples** Méthode permettant de contrôler l'identité d'une personne ou d'un système. Cette méthode recourt à des 'facteurs' multiples, tels qu'un mot de passe et un code reçu par SMS.

13. **Mobile device management** (MDM) Solution de gestion et de sécurisation des appareils mobiles d'une organisation. Cette gestion comprend par exemple le paramétrage des codes d'accès aux smartphones et tablettes, ou l'échange de données à distance entre ces appareils.

14. **Gestion d'accès réseau** Optimisation de la sécurisation d'un réseau, en n'autorisant la connexion qu'à des appareils connus et agréés.

15. **Phishing** Cyberattaque consistant à demander à une personne de communiquer des informations personnelles, telles qu'un code d'accès ou des données de carte de crédit. Le phishing (encore appelé 'hameçonnage') se produit le plus souvent par e-mail, mais aussi par téléphone, SMS ou autre type de messagerie.

16. **Privacy Impact Assessment** Analyse des risques auxquels une organisation est exposée, en termes de respect de la vie privée.

17. **Ransomware** Cyberattaque consistant à crypter l'appareil cible ou à le rendre inutilisable, et à exiger le versement d'une somme d'argent ('rançon') pour le réactiver.

18. **Remote Operations Center** Département qui assure 24/7 le suivi des nouvelles menaces. Ce département est ainsi en mesure de proagir et de réagir instantanément en cas d'attaque.

19. **Role based access control** Solution d'autorisation d'accès à un système, fondée sur des 'rôles' assignés à chaque (groupe de)

collaborateur(s) de l'organisation, tels que consultation, modification ou gestion.

20. **Rule based detection** Méthode de détection d'une cyberattaque. Le gestionnaire détermine au préalable les profils ou schémas de données suspects. Ensuite, le système recherche et détecte systématiquement ces profils et schémas.

21. **Sandbox** Espace protégé au sein d'un système, dans lequel des données ou programmes peuvent être utilisés tout en restant isolés du reste du système. Ce 'bac à sable' est généralement utilisé pour tester des logiciels suspects ou des malwares, afin d'analyser leurs effets.

22. **Single sign on** (SSO) Système d'accès unique permettant ensuite à l'utilisateur de travailler dans de multiples applications et composantes du réseau, sans avoir à réintroduire à chaque fois son identifiant/mot de passe.

23. **Filtre antispam** Logiciel d'identification et de suppression des virus informatiques et du courrier indésirable.

24. **Spoofing** Le cybercriminel dissimule son identité ou se fait passer pour un autre utilisateur (masquerading, source routing).

25. **Spyware** Un malware logiciel consistant à collecter et à transmettre des informations à l'insu de l'utilisateur. Ces informations sont généralement des suites de frappes au clavier, des captures d'écran, des adresses e-mail, des habitudes de surf ou des informations personnelles, telles qu'un numéro de carte de crédit.

Sources

www.proximus.be

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


proximus
enterprise