cybersécurité
pour **tous**

digital wallonia .be

La sécurité de votre EPN
✓ bonnes pratiques et
✓ protection des données

protéger les usagers, renforcer la confiance

proximus

Wallonie

Osons le numérique
osonslenumerique.be

Agence du Numérique

31 mars 2026

Programme du jour

1. Comprendre les risques spécifiques aux EPN
2. Inventaire IT : connaître ses équipements
3. Sécurisation des accès et des comptes
4. Sécurisation du réseau
5. Sécurisation des logiciels et des postes
6. Sauvegardes & continuité
7. Sécurité physique
8. Protection des données & RGPD
9. Procédures internes & gestion des incidents
10. Menaces & techniques des cybercriminels

digital wallonia .be

1

Comprendre les risques spécifiques aux EPN

proximus

Les EPN sont des environnements ouverts avec un public varié et des machines partagées.

Environnement ouvert
Accès libre, flux constant d'usagers, profils variés.

Public vulnérable
Usagers peu formés, comportements propices aux incidents.

Machines partagées
Sessions successives, traces laissées, risques d'usurpation.

Données personnelles manipulées
Inscriptions, impressions, connexions à des comptes privés.

Risques plus élevés qu'en bureau classique
Surface d'attaque élargie, contrôle limité.

Risques techniques et liés aux usages

Infections via supports USB et téléchargements
Propagation rapide entre postes, fichiers infectés.

Logiciels obsolètes ou non autorisés
Failles non corrigées, installations risquées par les usagers.

Appareils personnels connectés
Risque d'infection croisée et d'accès non maîtrisé

Sites web douteux et phishing
Faux sites, liens piégés, pièces jointes malveillantes.

Absence d'antivirus ou de filtrage
Protection insuffisante face aux menaces modernes.

proximus

Risques techniques et liés aux usages

Comptes utilisateurs non protégés
Sessions mal fermées, mots de passe enregistrés, usurpation possible.

Réseau Wi-Fi vulnérable
Sniffing, MitM, scans réseau, faux points d'accès (Evil Twin).

Traçabilité difficile
Difficulté d'identifier l'origine d'un incident.

Données personnelles laissées sur les machines
Historique, documents, identifiants exposés.

Usage illégal du Wi-Fi
Responsabilité potentielle de l'EPN en cas d'abus.

proximus

Risques organisationnels, légaux et matériels

Absence de procédures
Incidents non signalés, réactions tardives, propagation des risques.

Obsolescence du matériel
Pas de mises à jour, failles non corrigées.

Responsabilité légale (RGPD)
Fuites de données, mauvaise gestion des traces.

Risques réputationnels
Perte de confiance des usagers, image dégradée.

Vols et dégradations
Matériel exposé, usure rapide, dommages fréquents

proximus

Inventaire IT
Connaître ses équipements

2

Pourquoi faire un inventaire ?

- **Savoir ce que l'on protège**
  Avoir une vision complète du matériel et des systèmes présents dans l'EPN.

- **Identifier les machines critiques**
  Repérer les équipements sensibles ou indispensables au fonctionnement.

- **Suivre l'état du matériel**
  Connaître l'âge, l'usure, les performances et les besoins de remplacement.

- **Préparer les budgets**
  Anticiper les achats, renouvellements, licences et maintenances.

- **Faciliter les interventions techniques**
  Permettre un diagnostic rapide en cas de panne ou d'incident.

Ce que doit contenir un inventaire

- **Liste du matériel**
  Tous les équipements : PC, imprimantes, routeurs, tablettes, périphériques.
- **Numéros de série**
  Identification unique pour le suivi, la garantie et les réparations.
- **Dates d'achat et garanties**
  Durée de vie, fin de garantie, fournisseur, support.
- **Logiciels installés**
  Systèmes d'exploitation, antivirus, suites bureautiques, logiciels métiers.
- **Configuration réseau**
  Adresses IP, type de réseau, DNS, DHCP, emplacement des nœuds.

Inventaire materiel

- **PC fixes et portables**
  Caractéristiques, OS, licences, emplacement, usage.
- **Tablettes et smartphones**
  Modèles, versions, sécurité, utilisateurs.
- **Imprimantes et scanners**
  Type, emplacement, IP, consommables, support.
- **Routeurs, switches, Wi-Fi**
  Configuration, adresses IP, emplacement, fournisseur.
- **Accessoires**
  Clés USB, casques, écrans, UPS, caméras, robots, imprimantes 3D.

proximus NXT cybersecurity

Composante Physique
Ordinateurs et équipements de communication

Ordinateurs - Desktop		
	Machine n° ☐	Machine n° ☐
Marque		
Modèle		
Numéros de série		
Emplacement		
Fournisseur		
Cout		
Date d'achat		
Garantie		
Support		
Fournisseur		
Nom du système		
Utilisation/affectation		
Adresse IP		
Fréquence processeur		
Taille mémoire RAM		
Taille disque dur		
CD/DVD		
Périphériques internes		
Périphériques externes		
Système d'exploitation & version		
Numéros de série de l'OS & clé de licence		
Numéro de patch panel réseau		
Numéros de boitier de raccordement réseau		

Inventaire logiciel

- **Systèmes d'exploitation**
  Versions, mises à jour, licences.
- **Suites bureautiques**
  Office, LibreOffice, outils collaboratifs.
- **Antivirus**
  Nom, version, renouvellement, postes couverts.
- **Logiciels métiers**
  Applications spécifiques à l'EPN ou aux usagers.
- **Licences et dates d'expiration**
  Clés, abonnements, renouvellements à prévoir.

proximus NXT cybersecurity

Composante Configurations logiciels & données

Configurations, bases de données, programmes, systèmes d'exploitation, fichiers clés, fichier images, documentation technique et utilisateurs, plan de continuité et de reprise d'activité

Configuration réseau	
Type (client server, peer-to-peer, etc)	
Range d'adresses IP	
Masque de sous-réseau	
Domaine/workgroup	
IP du serveur Windows internet name service (WINS)	
IP du serveur Domain name system (DNS)	
IP du serveur Dynamic host configuration protocol (DHCP)	
Passerelle (Gateway)	
Nombre de nœuds	
Emplacement des nœuds (et identification) Peut faire référence au diagramme réseau	1. 2. 3. 4. 5. 6. 7. 8. 9. 10.

Bases de données partagées		
Utilisé par (Quel programme)	*Emplacement (Quel ordinateur)*	*Chemin d'accès et nom de la base de donnée Ex. \\Server\C\program\...*

Bonnes pratiques d’inventaire

- **Mise à jour mensuelle**
  Actualiser les ajouts, suppressions et modifications.
- **Stockage dans un dossier partagé sécurisé**
  Accessible aux gestionnaires autorisés uniquement.
- **Version papier en cas d’incident majeur**
  Utile en cas de panne réseau ou d’indisponibilité du système.
- **Historique des modifications**
  Suivre les changements pour comprendre l’évolution du parc.
- **Responsable identifié**
  Une personne clairement désignée pour maintenir l’inventaire.

digital wallonia .be

3

Sécurisation des accès et des comptes

proximus

Les principes de base

Un compte = une personne
Chaque utilisateur doit avoir son propre compte nominatif.

Pas de partage de mots de passe
Aucun mot de passe ne doit être communiqué ou partagé.

Comptes administrateurs limités
Seulement pour le personnel autorisé, et uniquement pour les tâches techniques.

Double authentification
Activation systématique dès que possible pour renforcer la sécurité.

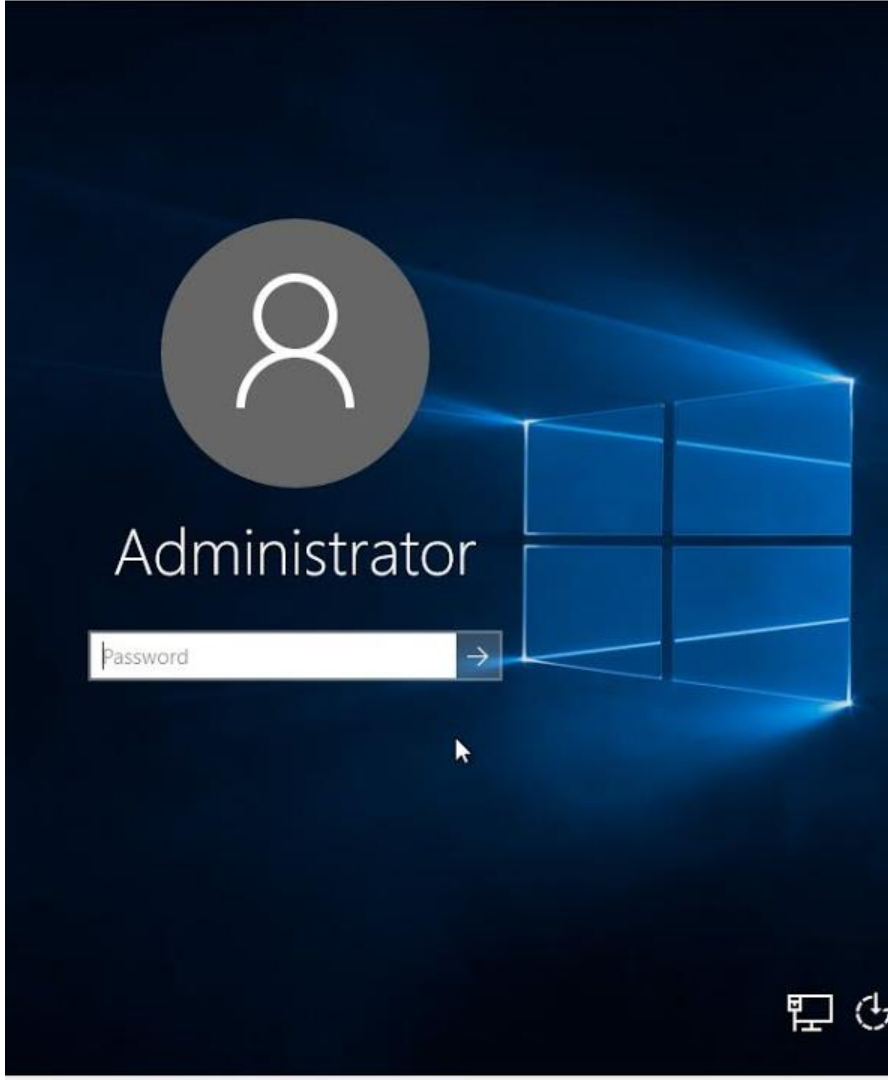
proximus

Gestion des mots de passe

- **Longs et complexes**
  Minimum 12 caractères, mélange de lettres, chiffres et symboles.
- **Gestionnaire de mots de passe recommandé**
  Permet de stocker, générer et synchroniser les mots de passe en sécurité.
- **Renouvellement régulier**
  Changer les mots de passe sensibles ou administrateurs à intervalles définis.
- **Jamais notés sur papier visible**
  Aucun post-it, cahier ou note laissée à proximité des postes.

Comptes administrateurs

- **Réservés au personnel**
  Uniquement pour les gestionnaires EPN ou techniciens autorisés.
- **Jamais utilisés pour la navigation**
  Pas d'Internet, pas d'e-mail, pas d'usage quotidien avec un compte admin.
- **Journalisation obligatoire**
  Toutes les actions administratives doivent être tracées.
- **Mot de passe renforcé**
  Plus long, plus complexe, renouvelé plus souvent que les comptes standard.



Sécurisation des sessions

- **Verrouillage automatique**
  Écran qui se verrouille après quelques minutes d'inactivité.

- **Déconnexion obligatoire**
  Fin de session systématique après usage, surtout sur les postes publics.

- **Sessions invité désactivées**
  Aucun accès anonyme ou non contrôlé.

- **Droits limités pour les usagers**
  Les utilisateurs ne doivent pas pouvoir installer, modifier ou supprimer des logiciels.

Journalisation et suivi

- **Historique des connexions** Enregistrer les connexions, déconnexions et tentatives d'accès.
- **Alertes en cas d'accès suspect** Notification automatique en cas d'activité inhabituelle.
- **Suivi des tentatives d'intrusion** Analyse régulière des logs pour détecter les anomalies.
- **Archivage sécurisé** Stockage des journaux dans un espace protégé, avec conservation sur la durée.

digital wallonia .be

Sécurisation du réseau

4

proximus

Les bases d’un réseau sécurisé

- **Routeur configuré**
  Paramètres de sécurité activés, accès administrateur protégé.

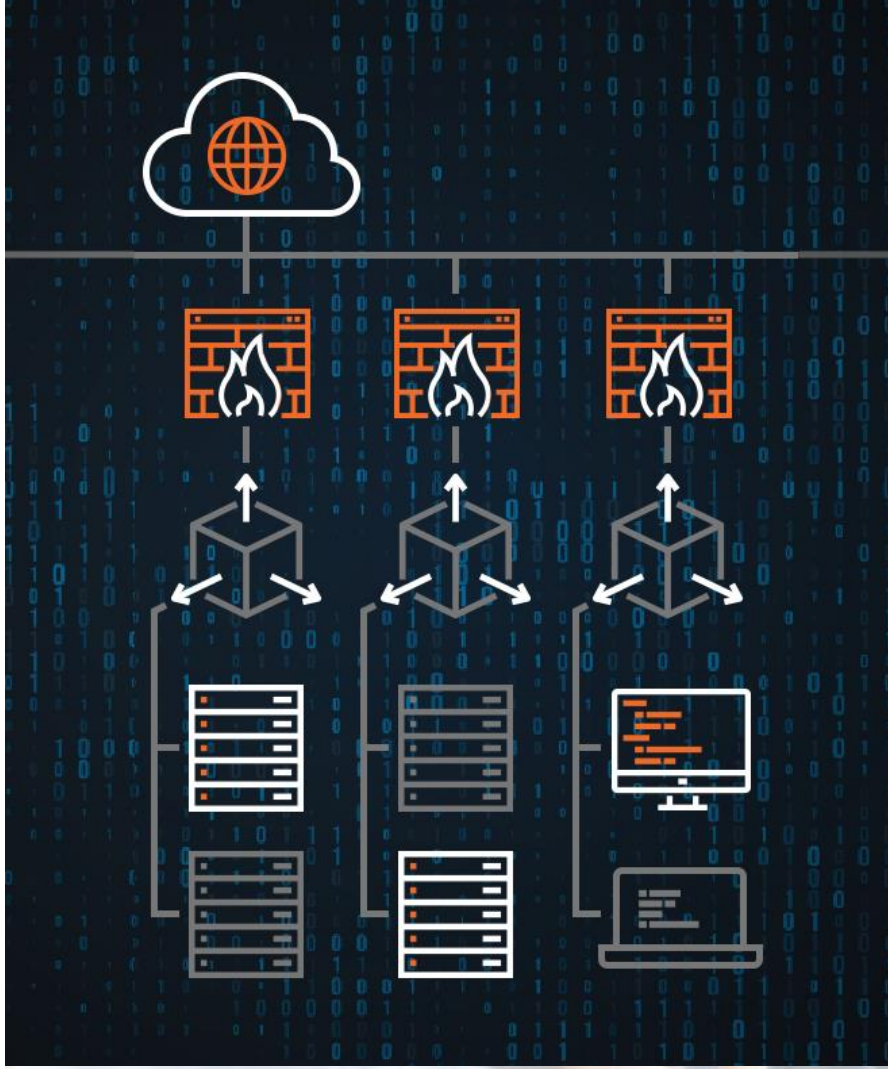
- **Pare-feu actif**
  Pare-feu local activé sur chaque machine pour bloquer les connexions non autorisées.

- **Mots de passe modifiés**
  Aucun mot de passe par défaut conservé sur le routeur ou les équipements réseau.

- **Mise à jour du firmware**
  Routeur et points d’accès mis à jour régulièrement pour corriger les failles.

Séparer les réseaux

- **Réseau interne (gestionnaires)**
  Accès réservé au personnel, protégé et isolé.
- **Réseau public (usagers)**
  Accès Internet uniquement, sans visibilité sur le réseau interne.
- **SSID invité**
  Wi-Fi séparé pour les visiteurs, avec mot de passe distinct.
- **VLAN si possible**
  Segmentation du réseau pour limiter la propagation des attaques.



Sécurisation Wi-Fi

- **WPA2 ou WPA3**
  Norme de chiffrement obligatoire pour protéger les communications.
- **WPS désactivé**
  Désactivation du bouton WPS, vulnérable aux attaques.
- **Mot de passe robuste**
  Long, complexe, changé régulièrement.
- **Filtrage MAC (optionnel)**
  Limiter l'accès à des appareils autorisés, en complément des autres protections.

Sécurisation de la passerelle

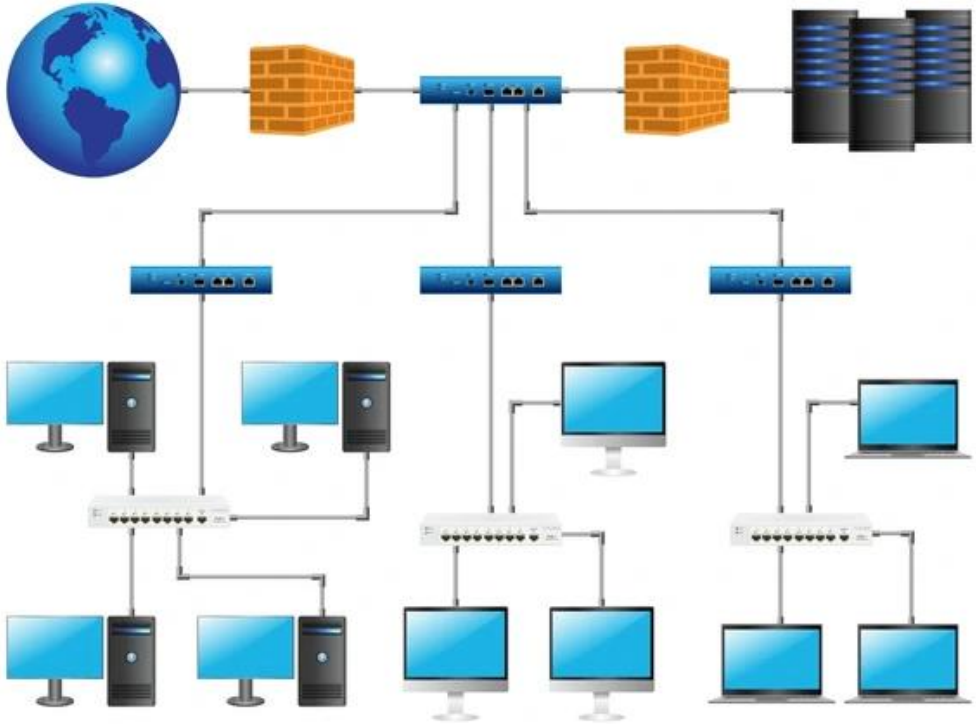
La passerelle est la porte d'entrée du réseau. La sécuriser, c'est protéger tout l'EPN

- **Filtrage web**
  Blocage des sites dangereux ou inappropriés.

- **Blocage des ports inutiles**
  Limiter les services accessibles depuis l'extérieur.

- **Surveillance du trafic**
  Analyse régulière pour détecter les comportements anormaux.

- **Alertes en cas d'anomalie**
  Notifications automatiques en cas d'accès suspect ou tentative d'intrusion



Documentation réseau

- **Schéma du réseau**
  Vue claire des connexions : routeur, switch, Wi-Fi, machines.
- **Paramètres du routeur**
  Adresse IP, identifiants, règles de pare-feu, configuration Wi-Fi.
- **Liste des appareils connectés**
  Inventaire des équipements autorisés et de leurs adresses IP/MAC.
- **Historique des modifications**
  Journal des changements pour comprendre l'évolution du réseau et faciliter le dépannage.

digital wallonia .be

5

Sécurisation des logiciels et des postes

proximus

Antivirus et protections

- **Antivirus obligatoire**
  Chaque poste doit disposer d'un antivirus actif et à jour.

- **Analyse automatique**
  Analyse régulière des fichiers, téléchargements et supports externes.

- **Mise à jour quotidienne**
  Les signatures virales doivent être mises à jour automatiquement.

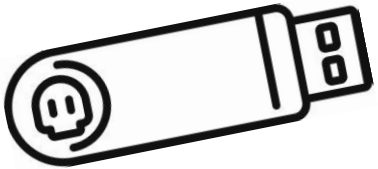
- **Protection web**
  Blocage des sites dangereux, phishing et téléchargements suspects.

✓ Installer **un logiciel antivirus** sur tous ses appareils et lancer un scan de sécurité.

Gestion des supports USB

- **Analyse automatique**
  Tout support USB doit être scanné dès son branchement.

- **Blocage des exécutables**
  Empêcher l'exécution automatique de programmes non autorisés.



- **Sensibilisation des usagers**
  Informer sur les risques liés aux clés USB et supports externes.

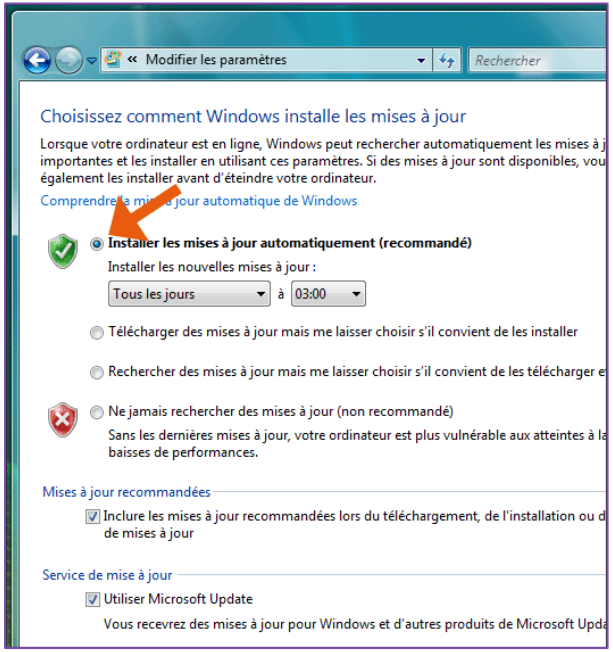
Mise à jour des systèmes

- **Windows Update activé**
  Mises à jour automatiques pour corriger les failles de sécurité.

- **Logiciels à jour**
  Applications, navigateurs et outils doivent être régulièrement mis à jour.

- **Correctifs de sécurité**
  Installation prioritaire des patchs critiques.

- **Redémarrages planifiés**
  Organisation des redémarrages pour appliquer les mises à jour sans perturber les usagers.

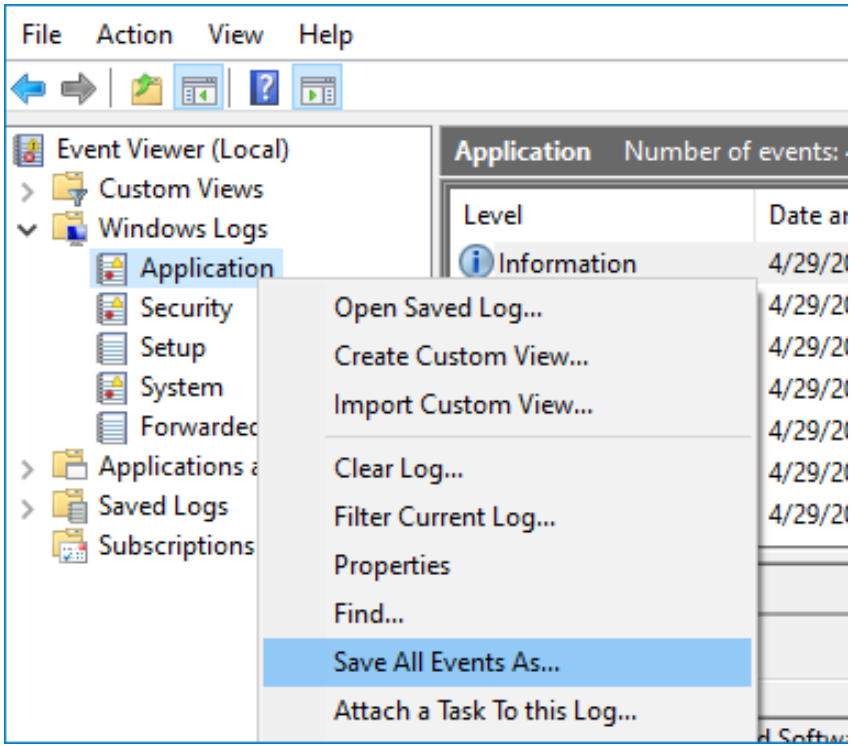


- Corrections de failles, vulnérabilités et bugs
- Meilleures performances globales de l'équipement
- Sécurité passive et active plus robuste
- Mise en conformité aux normes
- Meilleur moyen de garantir la compatibilité
- Accès aux fonctionnalités les plus récentes
- Maximise la durée de vie de votre matériel
- Réduire les coûts d'énergie et de maintenance.
- Economie de temps et des soucis plus tard

Chiffrement des disques

- **BitLocker activé**
  Chiffrement complet du disque pour protéger les données.
- **Clés de récupération stockées**
  Conservation sécurisée des clés dans un espace protégé.
- **Protection en cas de vol**
  Empêche l'accès aux données même si l'appareil est volé.
- **Obligatoire pour les portables**
  Tous les ordinateurs mobiles doivent être chiffrés.

Journalisation et suivi



- **Journaux de sécurité**
  Enregistrement des événements importants : connexions, erreurs, alertes.
- **Alertes automatiques**
  Notifications en cas d'activité suspecte ou tentative d'intrusion.
- **Archivage**
  Conservation des logs dans un espace sécurisé, non modifiable.
- **Analyse mensuelle**
  Vérification régulière pour détecter les anomalies et améliorer la sécurité.

Sauvegardes & continuité

6

Pourquoi sauvegarder ?

- **Pannes**
  Défaillance matérielle ou logicielle pouvant entraîner une perte totale des données.
- **Vol**
  Disparition d'un appareil contenant des informations sensibles.
- **Ransomware**
  Chiffrement malveillant des fichiers rendant les données inaccessibles.
- **Erreurs humaines**
  Suppression accidentelle, mauvaise manipulation, écrasement de fichiers.
- **Incendie / dégâts des eaux**
  Destruction physique des équipements et des données locales.

Types de sauvegardes

- **Locale**
  Sauvegarde sur un disque externe ou un NAS situé dans l'EPN.
- **Cloud sécurisé**
  Stockage hors site dans un service conforme (ISO 27001).
- **Chiffrée**
  Protection des sauvegardes pour éviter tout accès non autorisé.
- **Automatique**
  Planification régulière pour éviter les oublis et garantir la continuité.

Plan de continuité

- **Fonctions critiques**
  Identifier les services indispensables : accès Internet, logiciels clés, comptes administrateurs.
- **Solutions alternatives**
  Connexion 4G, générateur, matériel de secours, logiciels libres.
- **Procédures d'urgence**
  Actions immédiates en cas d'incident : qui fait quoi, dans quel ordre.
- **Communication interne**
  Informer l'équipe, les usagers et les partenaires en cas de perturbation.

proximus NXT cybersecurity

Continuité & reprise d'activité

Le plan de continuité des activités décrit exhaustivement les étapes à effectuer, les personnes à contacter et les moyens de mitigation rapide pour revenir à une situation stable (même si elle n'est pas encore au niveau normale).

Continuité – fonctions principales		
Fonctions critiques	***Prérequis***	***Ressources alternatives***
Accueil du public	Conformité aux normes (température, exiguïté, luminosité etc.. Assurances (incendie, responsabilité civile, vol) Présence de personnel (coordinateur et/ou animateur ICT) Electricité Chauffage Climatisation	 Générateur 220v Chauffage électrique Climatisation de secours
Mise à disposition d'un ordinateur & outils bureautique	Ordinateur / laptop/ tablette Suite bureautique installée Licence d'utilisation valide	 Open Office
Mise à disposition d'un ordinateur connecté à Internet	Ordinateur / laptop/ tablette Connectivité internet	 connectivité SIM / Smartphone / Dial-up
Scanner	Scanner	Smartphone E-Scan
Imprimer	Imprimante Cartouche d'encre	
S'authentifier avec une carte d'identité électronique	Lecteur de carte intégré Lecteur de carte externe	Its me / Token MyGov.be Smart-ID User & password + sms

Tester les sauvegardes

- **Restauration régulière**
  Vérifier que les données peuvent être récupérées sans erreur.
- **Vérification de l'intégrité**
  S'assurer que les fichiers sauvegardés ne sont pas corrompus.
- **Simulation d'incident**
  Tester un scénario de panne ou d'attaque pour valider les procédures.
- **Documentation** Consigner les résultats, les problèmes rencontrés et les améliorations nécessaires.

Bonnes pratiques

- **Sauvegarde hebdomadaire**
  Réaliser une sauvegarde complète au minimum une fois par semaine.

- **Hors site**
  Stocker une copie dans un lieu externe ou un cloud sécurisé.

- **Chiffrée**
  Protéger les sauvegardes contre l’accès non autorisé.

- **Responsable désigné**
  Une personne identifiée pour gérer, vérifier et maintenir les sauvegardes.

digital wallonia .be

7

Sécurité physique

proximus

Contrôle d’accès

- **Locaux fermés**
  Les salles doivent rester verrouillées en dehors des heures d’ouverture.

- **Clés ou badges**
  Accès réservé aux personnes autorisées, traçable si possible.

- **Registre des visiteurs**
  Enregistrement systématique des personnes externes présentes dans l’EPN.

- **Zones sensibles protégées**
  Local technique, serveurs, armoires réseau accessibles uniquement au personnel.

Protection du matériel

- **Câbles antivols**
  Sécurisation des mini-PC, laptops et écrans.
- **Armoires sécurisées**
  Stockage protégé pour le matériel sensible ou coûteux.
- **Local technique protégé**
  Accès restreint, ventilation correcte, absence de risques physiques.
- **Inventaire mis à jour**
  Liste complète du matériel avec emplacement et état.

Surveillance

- **Caméras**
  Surveillance des zones d'accès et du local technique.
  ⓘ Bien s'assurer des obligations règlementaires et législatives applicables

- **Alarmes**
  Détection d'intrusion ou d'ouverture non autorisée.

- **Détecteurs**
  Détecteurs de fumée, chaleur, inondation selon les risques.

- **Politique d'accès**
  Règles claires : qui peut entrer, quand, et dans quelles conditions.

Environnement

- **Température**
  Maintenir une température stable pour éviter la surchauffe du matériel.

- **Ventilation**
  Assurer une bonne circulation d'air dans les locaux techniques.

- **Propreté**
  Limiter la poussière, nettoyer régulièrement les postes et armoires.

- **Absence de liquides**
  Idéalement aucun liquide à proximité des équipements électriques ou informatiques.

Destruction des données

- **Déchiqueteuse**
  Destruction physique des documents papier contenant des données sensibles.

- **Effacement sécurisé**
  Suppression définitive des fichiers avant recyclage ou réaffectation.

- **Procédure de déclassement**
  Processus clair pour retirer un appareil du service en toute sécurité.
- **Journalisation**
  Enregistrement des destructions pour assurer la traçabilité.

Protection des données & RGPD

8

Les données collectées

- **Identité**
  Nom, prénom, informations minimales nécessaires à l'inscription.
- **Contact**
  Adresse e-mail, numéro de téléphone si indispensable.
- **Historique d'usage**
  Heures de connexion, postes utilisés, activités liées au service.
- **Données techniques**
  Adresses IP, journaux de connexion, configuration des postes.

Informer les usagers

- **Finalité**
  Expliquer pourquoi les données sont collectées (gestion des accès, sécurité, statistiques).

- **Durée**
  Indiquer combien de temps les données sont conservées.

- **Destinataires**
  Préciser qui peut accéder aux données (gestionnaires, partenaires techniques).

- **Droits**
  Informer sur les droits RGPD : accès, rectification, effacement, opposition.

Droits des usagers

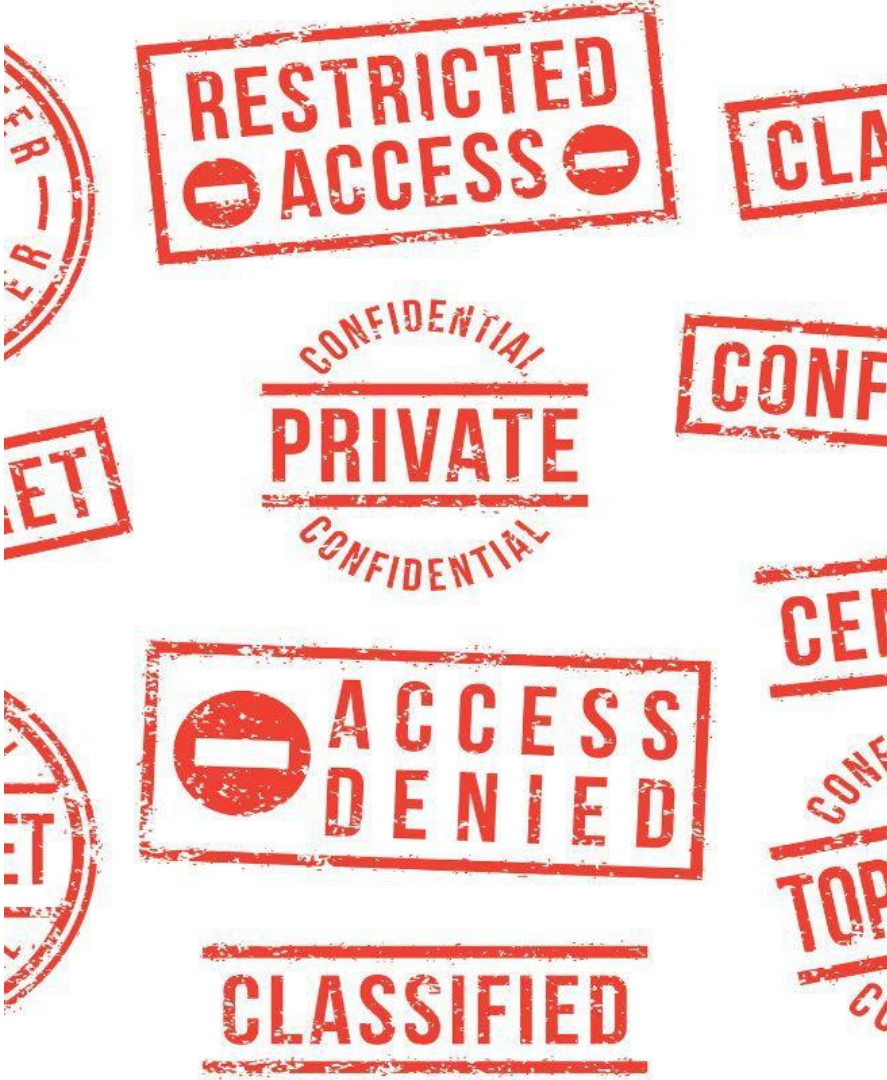
- **Accès**
  L'usager peut demander une copie de ses données.
- **Rectification**
  Correction des données inexactes ou incomplètes.
- **Effacement**
  Suppression des données lorsque leur conservation n'est plus justifiée.
- **Opposition**
  Possibilité de refuser certains traitements non essentiels.

Minimisation des données

- **Collecter le minimum**
  Uniquement les données nécessaires au fonctionnement de l'EPN.
- **Pas de données inutiles**
  Éviter les informations sensibles ou non pertinentes.
- **Pas de stockage excessif**
  Limiter la durée de conservation au strict nécessaire.
- **Effacement automatique**
  Mettre en place un délai d'effacement des données laissées sur les machines.

Confidentialité

- **Accès limité**
  Seules les personnes autorisées peuvent consulter les données.
- **Chiffrement**
  Protection des données stockées ou transférées.
- **Stockage sécurisé**
  Serveurs, cloud ou supports conformes aux bonnes pratiques de sécurité.
- **Politique interne**
  Règles claires sur la gestion, l'accès et la protection des données.



digital wallonia .be

9

Procédures internes & gestion des incidents

proximus

Pourquoi des procédures ?

- **Cohérence**
  Assurer une réaction uniforme, quel que soit le gestionnaire présent.
- **Réactivité**
  Gagner du temps en sachant immédiatement quoi faire.
- **Professionnalisation**
  Gérer les incidents de manière structurée et crédible.
- **Conformité**
  Respecter les obligations légales et les bonnes pratiques de sécurité.

Reconnaître un incident

- **Virus**
  Comportement anormal, alertes antivirus, fichiers chiffrés.
- **Vol**
  Disparition d'un appareil, accès non autorisé aux locaux.
- **Intrusion**
  Connexion suspecte, activité inhabituelle sur le réseau.
- **Fuite de données**
  Données copiées, envoyées ou accessibles sans autorisation.

Réagir efficacement

- **Isoler la machine**
  Déconnecter immédiatement l'appareil du réseau pour limiter la propagation.

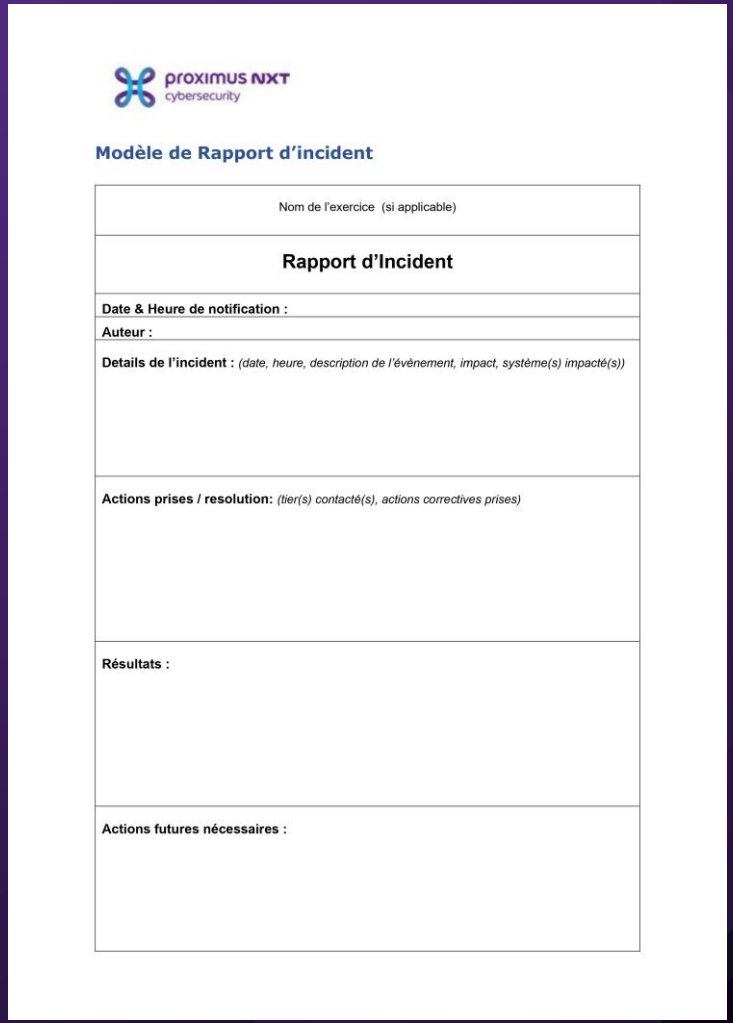
- **Prévenir le responsable**
  Informer le gestionnaire principal ou la personne référente.

- **Documenter**
  Noter la date, l'heure, les symptômes, les systèmes touchés.

- **Appliquer les mesures**
  Nettoyage, restauration, changement de mots de passe, blocage d'accès

Rapport d’incident

- **Date**
  Moment exact de la détection et de la prise en charge.
- **Impact**
  Conséquences sur les usagers, les données et les services.
- **Systèmes touchés**
  Machines, comptes, réseaux ou données concernés.
- **Actions menées**
  Mesures prises, résultats obtenus, actions encore nécessaires



proximus NXT cybersecurity

Modèle de Rapport d’incident

Nom de l’exercice (si applicable)
Rapport d’Incident
Date & Heure de notification :
Auteur :
Details de l’incident : *(date, heure, description de l’évènement, impact, système(s) impacté(s))*
Actions prises / resolution: *(tier(s) contacté(s), actions correctives prises)*
Résultats :
Actions futures nécessaires :

Que faire en cas d'incident?

- **Identifier l'incident**
  Décrire clairement ce qui s'est passé : panne, vol, comportement suspect, fuite de données, malware.

- **Informer la bonne personne**
  Prévenir immédiatement le gestionnaire principal ou le référent sécurité.

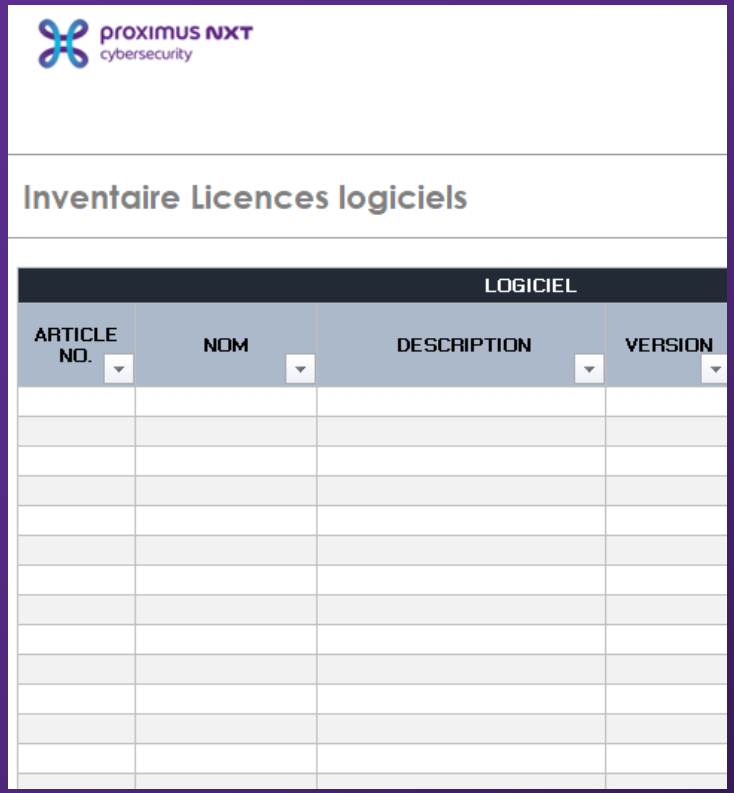
- **Documenter**
  Noter la date, l'heure, les machines concernées, les symptômes et les actions déjà tentées.

- **Escalade interne**
  Contacter le technicien, la direction ou le service informatique selon la gravité.

Signalement aux autorités compétentes:

- **Police** : en cas de vol, intrusion physique, dégradation.
- **Safeonweb** : en cas de phishing, malware, comportement suspect.
- **Centre pour la Cybersécurité Belgique (CCB)** : en cas d'incident majeur ou de fuite de données.
- **Autorité de protection des données (APD)** : si des données personnelles ont été compromises.

Gérer les licences



proximus NXT cybersecurity

Inventaire Licences logiciels

	LOGICIEL		
ARTICLE NO.	NOM	DESCRIPTION	VERSION

- **Inventaire des licences**
  Lister toutes les licences logicielles utilisées dans l'EPN (OS, antivirus, bureautique, logiciels métiers).
- **Dates d'expiration**
  Suivre les renouvellements pour éviter les interruptions de service.
- **Stockage sécurisé des clés**
  Conserver les clés de licence dans un espace protégé et accessible uniquement aux gestionnaires.
- **Conformité légale**
  S'assurer que chaque logiciel installé est couvert par une licence valide.

Procédure de déclassement du matériel

- **Effacement sécurisé**
  Supprimer définitivement les données avant réaffectation ou recyclage.
- **Retrait des comptes et licences**
  Dissocier l'appareil des comptes administrateurs, logiciels et services cloud.
- **État du matériel**
  Documenter l'état, les réparations éventuelles et la raison du déclassement.
- **Traçabilité**
  Enregistrer la date, la destination (recyclage, don, destruction) et la personne responsable.

Amélioration continue

- **Analyse post-incident**
  Comprendre ce qui s’est passé et pourquoi.
- **Mise à jour des procédures**
  Adapter les règles pour éviter que l’incident ne se reproduise.
- **Sensibilisation**
  Informer l’équipe et les usagers des bonnes pratiques.
- **Prévention**
  Renforcer les protections techniques et organisationnelles

digital wallonia .be

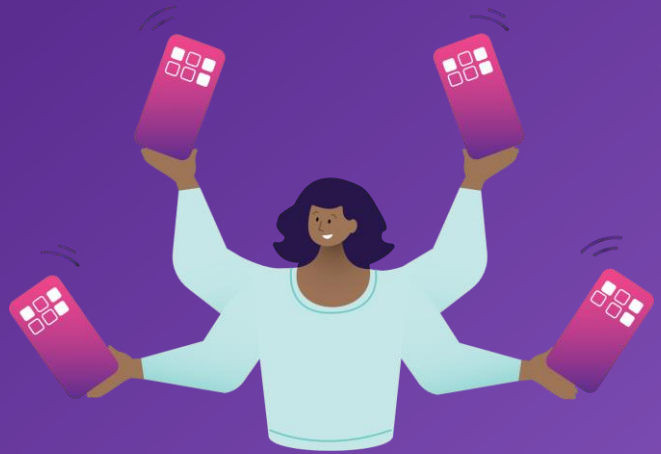
10

Menaces & techniques des cybercriminels

proximus

Usage sécurisé des appareils mobiles

- **Prudence** avec les smartphones, tablettes et objets connectés
- **Attention** aux paiements mobiles et en ligne
- Réseaux **Wi-Fi publics** : une porte d'entrée pour les hackeurs



- **Prudence** avec les **QR codes.**

Empreinte numérique et vie privée

Toutes vos activités **laissent des traces sur internet.** La quantité de traces et de données qu'on laisse derrière soi, c'est ce qu'on appelle **l'empreinte numérique.**

Plus on peut retrouver de données, plus l'empreinte numérique est importante.

Comment sont collectées les traces?

Cookies

Fichiers log de sites

Historique et navigateur

Adresse postale

Adresse IP & info sur l'hôte

Identification faciale
& empreinte digitale

Localisations

Carnet d'adresse

Données d'applications & usage


How's your torn muscle?

Exemple d’utilisation frauduleuse de votre empreinte numérique:

Security question 1

What was your first pet's name?

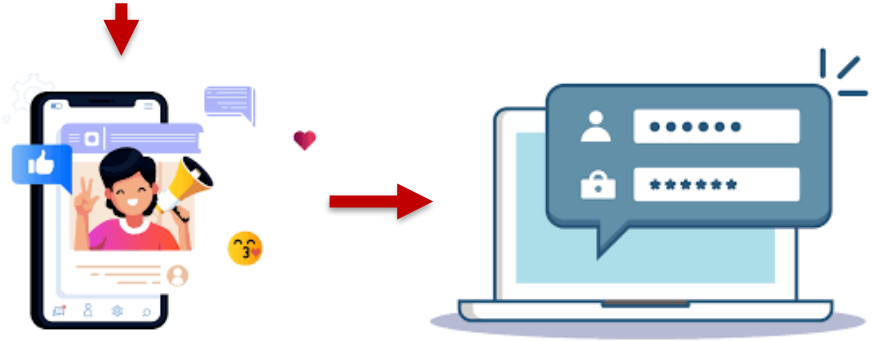
What is the name of the city where you were born?

What was your childhood nickname?

What is the name of the city where your parents met?

What is the first name of your oldest cousin?

What is the name of the first school you attended?



Tester son empreinte numérique:

1. **Tester son empreinte numérique sur Google.**

2. **Effectuer une vérification sur le site web « Have I Been Pwned? »**

- ☑ Si l'écran devient vert en bas, votre adresse e-mail ou numéro de téléphone ne sont pas impliqués dans une fuite de données.
- ✖ Si l'écran devient rouge, vos données ont été piratées. Il est urgent de changer vos mots de passe !

Techniques et méthodes :

Phishing / smishing

Malware (Rootkit, Ransomware, virus, bot, Trojan, Spyware, Malvertising, Keyloggers)

Social engineering, Brutforce attack, DDos attack, man-in-the-middle attack (MitM), Spoofing, Sniffing

CYBER SECURITY COALITION

Déjouez les attaques de phishing

Techniques et méthodes :

Phishing /smishing

Phishing

-Vol de données

- Souvent des mails frauduleux

Smishing

-Phishing mais sur smartphone

-Toujours un lien

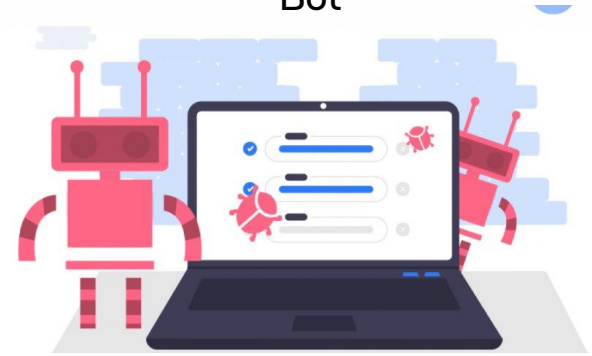
Techniques et méthodes :

Malware
Virus/ Bot

Virus

- Perturber l'acitivité
- S'auto répliquer
- Similaire à un vrai virus

Bot



- Contamine un maximum de machines
- Créer un Botnet
- Utilisé pour des attaques de plus grandes envergures

Techniques et méthodes :

Malware
Rootkit

- Créer une porte dérobée

- Contrôle total de la machine

- Vol de données

Techniques et méthodes :

Malware
Ransomwares

- Chiffre les données de l'ordinateur
- Une des plus grosse menace des entreprises

Ransomware : les risques

- Paralysie des activités
- Perte financière
- Risques légaux
- Perte de confiance

Quelques exemples de ransomwares récents…

Août 2024

IHECS

Août 2023

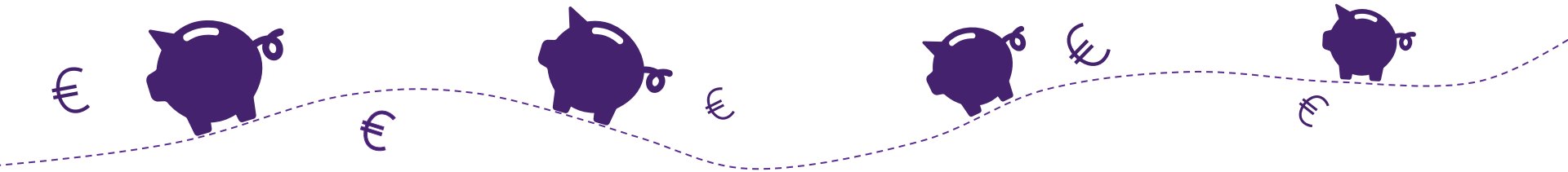
CPAS de Charleroi

Mai 2023

Hôpital Sambre et Meuse

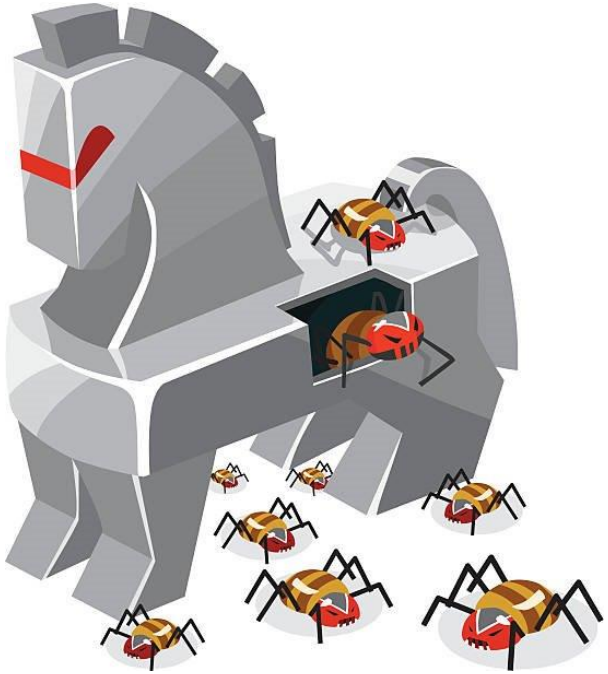
Déc. 2022

Ville d'Anvers



Techniques et méthodes :

Malware
Trojan



- Tire son nom du cheval de Troie
- Se fait passer pour un programme légitime et dissimule son code malveillant
- Peut être indétectable au près des antivirus tant qu'il est inactif

Techniques et méthodes :

Malware
Spyware/ Keyloggers

Spyware :

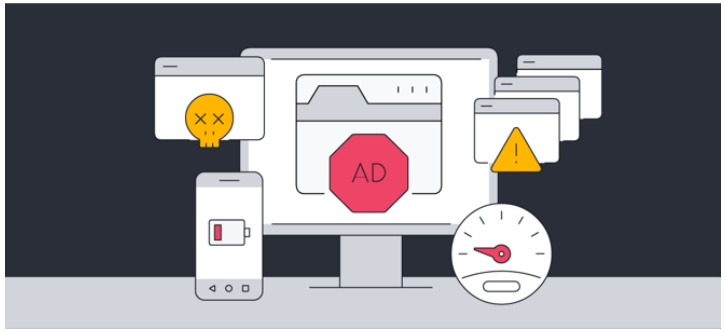
- Similaire à un espion
- Vole les données

Keyloggers :

- Enregistre les entrées
- Comparable au Spyware

Techniques et méthodes :

Malware
Adwares/ Malvertising



Adwares :

- Collecte des infos comme un Spyware
- Personnalise les pubs
- Va jusqu'à modifier les paramètres du navigateur

Malvertising :

- Virus qui vient d'une pub
- Paye pour que la pub apparaisse sur des vrais sites
- Redirige sur un site ou teléchargement frauduleux

Techniques et méthodes :

DDoS

Attaque par déni de service

- Utilise un réseau de machines pour innonder un serveur de requête
- A pour but par exemple de faire planter un site web
- Utilisé aussi pour extroquer de l'argent à des entreprises

Techniques et méthodes :

Social Engineering

Consiste à se faire passer pour quelqu'un / une entitée pour voler des informations ou arnaquer

Utilise la première faille de sécurité au monde, l'homme. Il faut toujours verifier l'identitée des personnes en face de nous

Le social engineering n'est pas que numérique,
il arrive aussi que ça se produise dans la vraie vie

Techniques et méthodes :

Brutforce Attack

Brutforce Attack :

- Une attaque par brutforce consiste en l'essai de plein de combinaisons pour trouver un code
- C'est considéré comme l'attaque le plus basique/simple
- Utiliser un mot passe fort (avec des majuscules, chiffres, symbols) et ne pas réutiliser le même mot de passe

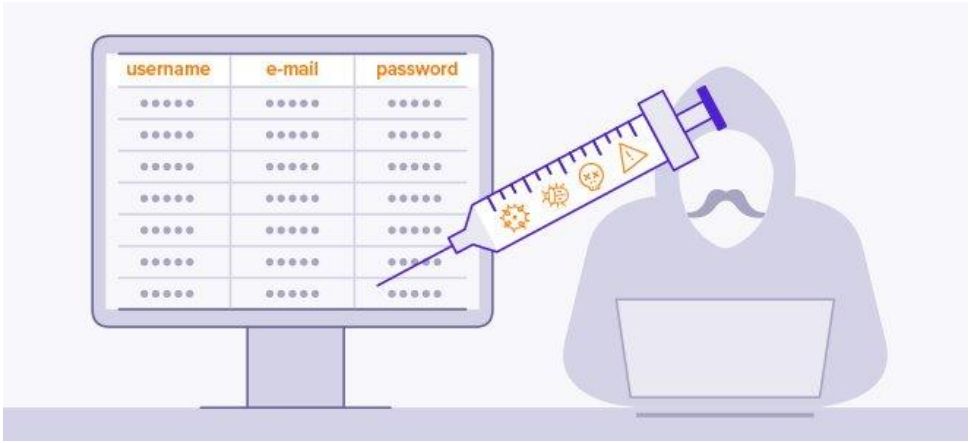
Techniques et méthodes :

Injection SQL

- Injecte du code “SQL” pour envoyer des requêtes au serveur

- Utilisé pour voler des informations dans des bases de données

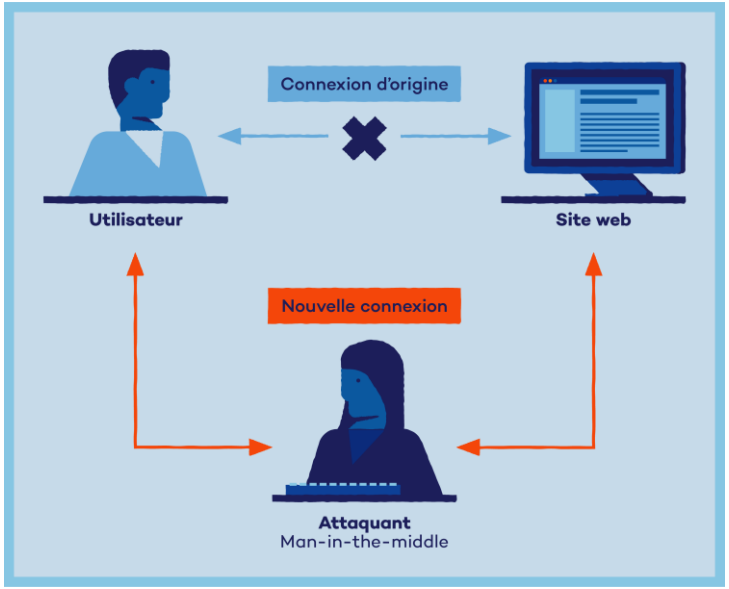
- Les données telles que les mots de passes sont hachés dans la base de données



Techniques et méthodes :

Man in the middle/ Sniffing

- Man in the middle et sniffing sont assez similaire
- Man in the Middle : Vol de données en s'interposant dans le réseau
- Sniffing : Analyse les données qui passent sur le réseau et les lis



Ursurpation d’identité

Qu’est ce que le **Spoofing** ?

Usurpation d’identité en ligne pour tromper les utilisateurs.

- E-mails frauduleux imitant des expéditeurs légitimes.
- Sites web contrefaits ressemblant à des sites officiels.
- Appels téléphoniques ou messages texte se faisant passer pour des institutions de confiance.

Soyez toujours méfiant(e) !

Si quelque chose semble trop beau pour être vrai, c'est très probablement le cas !

Désinformation, Fake News et Deepfakes

Les objectifs :

Influencer

Nuire à la société

Gagner de l'argent

Arme stratégique en temps de crise

Impact sur la santé publique

...

Pourquoi cela fonctionne t-il?

« Think before you post »

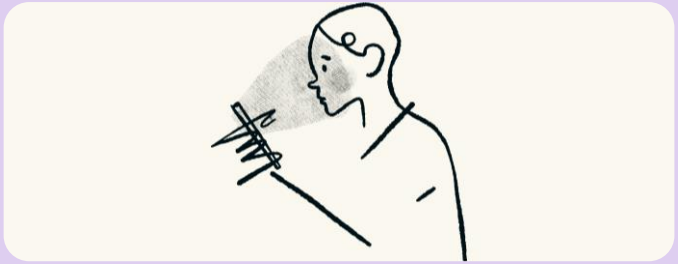
Une information non vérifiée peut causer plus de dégâts qu'une information absente.

Une Arme dans le Cyberespace

- Risques de sécurité
- Manipuler et compromettre les systèmes sensibles

Comment s’en protéger?

- Fact checking
- Renforcer son esprit critique
- Chercher le contexte initial
- Analyser et varier les sources
- Anticiper la manipulations



Que sont les deepfakes?

Les manipulations visuelles et audio

- Création de contenus réalistes imitant une personne réelle.
- Faux discours ou déclarations
- Modification d’événements clés
- Outils accessibles au grand public
- Une évolution rapide grâce à l’intelligence artificielle.

Les deep-nudes : un danger majeur pour les jeunes

- Génération de fausses images intimes via l'IA.

- **50% des contenus pédocriminels proviennent de photos ou vidéos postées par des parents.**

- Atteintes graves à la vie privée et à la dignité.

- Harcèlement, chantage et traumatisme psychologique.

Nos responsabilités :
- **Respecter** le **droit** des enfants à une vie **privée** numérique.
- Sensibiliser à la protection des données en ligne.

La création et diffusion de deepnudes sont des actes illégaux.


Here's what she had to say.

Protéger les enfants et soi-même face aux deep-fakes?

1. Limiter l'exposition en ligne

2. Éviter le "sharenting"

3. Renforcer l'éducation médiatique

4. Établir un mot de sécurité familial

5. Dialoguer avec les jeunes

6. Développer l'esprit critique

Que faire en cas de cyberattaque?

Vous êtes victime d'une tromperie, d'une arnaque, d'une fraude ou d'une escroquerie ?

Escroquerie impliquant vos moyens de paiement?	Escroquerie, tromperie, arnaque fraude, droits en tant que consommateur non respectés?	Victime de cyberharcèlement?	Email frauduleux reçu? (Spam, phishing, scam, etc.)	Mes données ont été volées	Mon téléphone est sur écoute (logiciel de surveillance installé souvent par un proche)
Contacter votre banque et/ou Card Stop au 078 170 170	Plainte à la Police + Signalement au point de contact du SPF Economie	Rassemblez un dossier de preuve et porter plainte à la police	Transmission du mail frauduleux à SafeOnWeb	Changer vos mots de passes, vérifier si vos données ne sont pas en ventes sur des sites du « dark web » avec haveibeenpawned par exemple	Supprimez l'application ou le programme de surveillance. Vérifiez par le biais de votre logiciel anti-virus que ce logiciel de surveillance est complètement supprimé. Réinitialisez votre appareil aux paramètres d'usine. Changez vos mots de passe.
078 170 170	https://www.police.be/fr/ https://pointdecontact.belgique.be	https://www.police.be/fr/ https://aide.igvm-iefh.belgium.be/fr	suspect@safeonweb.be	https://haveibeenpwned.com/	https://www.ecouteviolencesconjugales.be/ / ou 080030030 https://tele-accueil.be/ ou 107 https://www.police.be/fr/
+ Dans certains cas vous pouvez faire une demande de remboursement		Vous pouvez contacter child focus (pour les enfants) ou l'égalité des femmes et des hommes (pour les adultes)		- Utilisez l'authentification à deux facteurs partout où vous le pouvez. - Utilisez des mots de passe différents et conservez-les dans un gestionnaire de mots de passe	contacter un professionnel de l'écoute au niveau des violences conjugales Déposer plainte à la police

La lute contre la cybercriminalité

	Opérationnel	Judiciaire	Contre-mesures	Prévention	Planification & Coordination	Coopération
Europe	EUROPOL EC3 European Cybercrime Centre	EUROPOL EC3 European Cybercrime Centre	Cert-EU	CSIRTs NETWORK	enisa THE EU CYBERSECURITY AGENCY	CyCLONe European Cyber Crises Liaison Organisation Network Powered by ENISA
Fédéral	CERT.be The Federal Cyber Emergency Team	Federale Politie Police Fédérale	ADIV - SGRS DEFENSIE LA DÉFENSE Quaero et tego	CENTRE FOR CYBER SECURITY BELGIUM	CENTRE FOR CYBER SECURITY BELGIUM ibpt	CENTRE FOR CYBER SECURITY BELGIUM
Sectoriel	telenet orange proximus	CSIRT's TEAMS	CSIRT's TEAMS	CYBER SECURITY COALITION.be ISPA febelfin	CYBER SECURITY COALITION.be ISPA febelfin	CYBER SECURITY COALITION.be ISPA febelfin

Conclusion

Récap’ des bonnes pratiques

1. Se maintenir informé.e

2. Etre vigileant en ligne

3 . Faire preuve d’esprit critique

4. Reporter les incidents

5. Sensibiliser autour de soi.

La cybersécurité, une responsabilité partagée!