07/06/2024

Cybercriminalité et moyens de protection

Présentation faite à la demande de la CAPEB Indre-et-Loire

Julien Garcia

Table des matières

Informations

Origine du document

Ce document fait suite à une prestation de présentation d'une quarantaine de minutes demandée par la CAPEB Indre-et-Loire pour ses adhérents.

Site : https://www.capeb.fr/indre-et-loire

Cette prestation a été réalisée en mon nom propre et n'est en aucun cas liée à mon emploi actuel ou à mon employeur. Toutes les actions et responsabilités liées à cette prestation sont de ma seule initiative et ne reflètent pas les positions ou les politiques de mon employeur.

Licence

Concernant l'auteur

Vous pouvez me retrouver sur :

- LinkedIn : https://www.linkedin.com/in/jgarcia-cybersec/

Remerciement

Je tiens à remercier Monsieur le Président de la CAPEB Indre-et-Loire et ses équipes pour la confiance qu'ils m'ont accordée et pour l'opportunité qui m'a été offerte.

Modifications apportées

Ajout des chapitres « liens utiles » et « 10 mesures essentielles ».

MYTHES

Mythe 1 : la sécurité est faite pour nous empêcher de travailler

La réalité : la sécurité informatique a pour but d'aider l'entreprise à créer une valeur commerciale protégée, en augmentant la résilience et en réduisant l'impact des incidents de sécurité.

Ce qui veut dire : une mesure de sécurité doit identifier un risque qu'elle corrige, avoir un impact sur les utilisateurs métier et être validée par un membre de la direction.

Il y a trois impacts importants à prendre en compte :

- Financier
    - Coûts directs et indirects associés à la mise en place et à la maintenance des mesures de sécurité.
    - Perte de revenus potentiels due à la perte de contrats ou d'opportunités commerciales.
    - Amendes et pénalités en cas de non-conformité avec les réglementations (comme le RGPD en Europe).
- Disponibilité
    - Interruption de service entraînant une perte d'accès aux systèmes et aux données critiques pendant une certaine période.
    - Impact sur la productivité des employés en cas de perte d'accès aux terminaux ou aux services en ligne.
    - Perte de données ou corruption de données pouvant nécessiter du temps et des ressources pour la récupération.
- Réputation
    - Perte de confiance des clients et des partenaires commerciaux en cas de violation de sécurité ou de fuite de données.
    - Couverture médiatique négative pouvant affecter l'image de marque et la perception publique de l'entreprise.
    - Réduction de la satisfaction client et perte potentielle de clients existants et futurs.
    - Impact sur les relations avec les investisseurs et les parties prenantes en raison de préoccupations liées à la sécurité.

« Il faut gagner des batailles assez importantes pour être significatives et assez simples pour être gagnées. »

Mythe 2 : 50% des PME mettent la clef sous la porte dans les 6 mois qui suivent une cyberattaque

La réalité : Une étude (FranceNum) menée sur 48 incidents cyber ciblant des entreprises françaises non cotées entre 2017 et 2022 indique que le risque de défaillance de l'entreprise augmente d'environ 50 % dans les 6 mois qui suivent l'annonce de l'incident.

Source (en français) : https://www.lemagit.fr/conseil/Combien-de-PME-mettent-la-cle-sous-la-porte-apres-une-cyberattaque

Source 2 (en français) : https://www.linkedin.com/posts/valerymarchive_francenum-cyberattaque-activity-7168933118362525696-Dmeu/?originalSubdomain=fr

D'où vient cette légende ? Difficile à confirmer, cependant il est possible que ce soit repris de l'Alliance Nationale pour la Cybersécurité (NCSA), une organisation à but non lucratif dont la mission est de « créer un monde plus sûr et plus interconnecté ».

Source (en anglais) : https://staysafeonline.org/news-press/press-release/national-cyber-security-alliance-statement-regarding-incorrect-small-business-statistic/

PANORAMA 2023

Paysage des menaces et des vulnérabilités

Sur l'ensemble des vulnérabilités signalées :

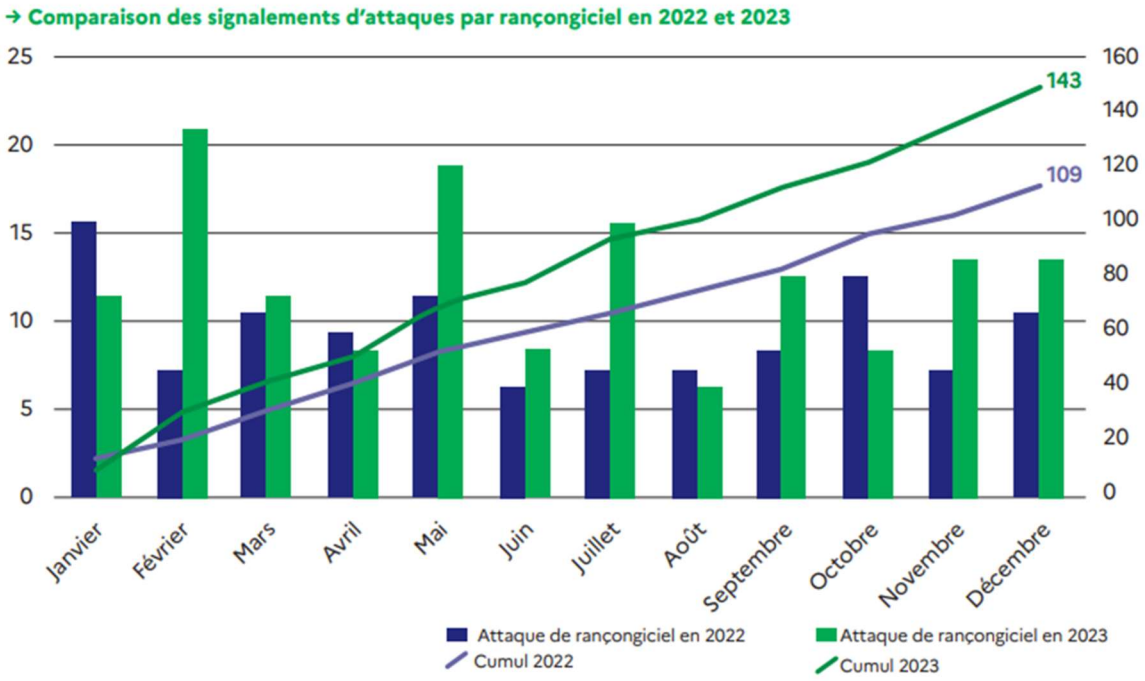
- Un quart fait l'objet d'une preuve de concept pour prouver l'existence de la vulnérabilité.
- « Seulement » 1 % des vulnérabilités font l'objet d'une industrialisation dans le cadre d'une attaque.

Il est important d'être informé du risque sans pour autant devenir paranoïaque.

Source (en anglais) : https://blog.qualys.com/vulnerabilities-threat-research/2023/12/19/2023-threat-landscape-year-in-review-part-one

Comparaison des signalements d'attaque par rançongiciel en 2022 et 2023

Rançongiciel : programme malveillant qui chiffre les données personnelles de qqn dans le but de lui extorquer de l'argent.

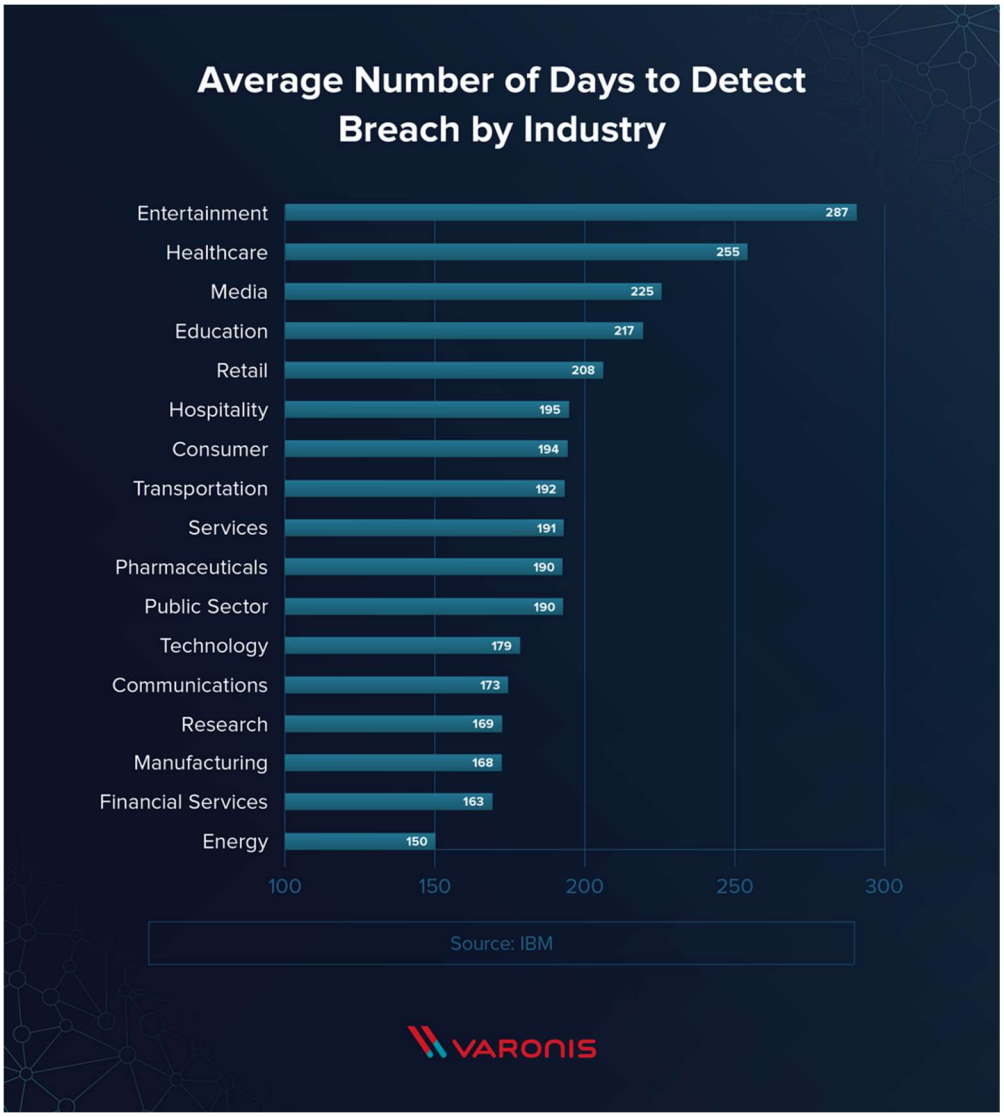


- Augmentation de 31 % du nombre de signalements de rançongiciels sur l'année 2023.
- Si l'on considère 251 jours ouvrés en 2023, cela revient à moins de deux jours entre deux signalements.

Il s'agit uniquement des signalements réalisés auprès de l'Agence Nationale de la Sécurité des Systèmes d'Information.

Source (en français) : https://www.cert.ssi.gouv.fr/cti/CERTFR-2024-CTI-001/

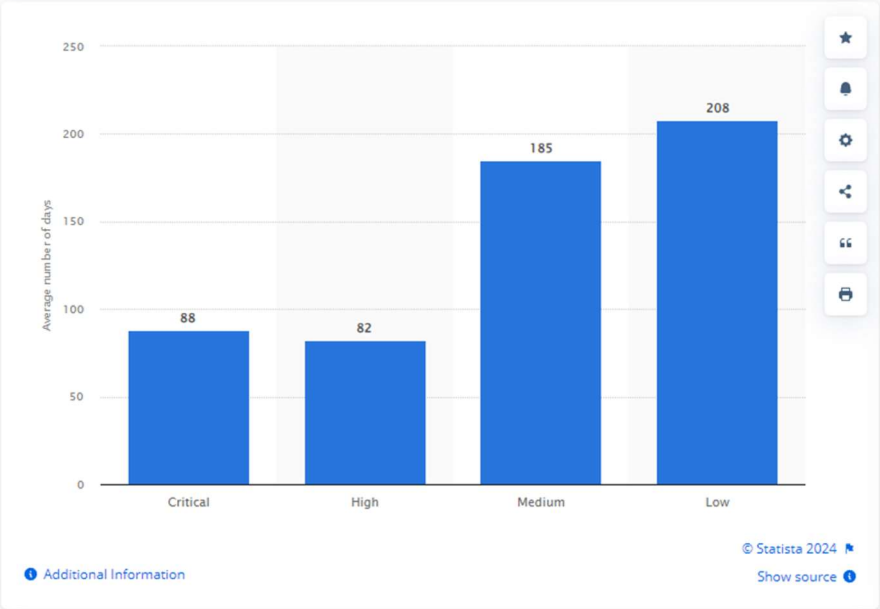
Délais de détection par secteur d’activité



- Le délai entre la compromission et la détection varie très fortement (presque de deux fois) en fonction des secteurs.
- Même s'il y a des disparités entre secteurs et pays, il reste tout de même au minimum 100 jours avant une détection.

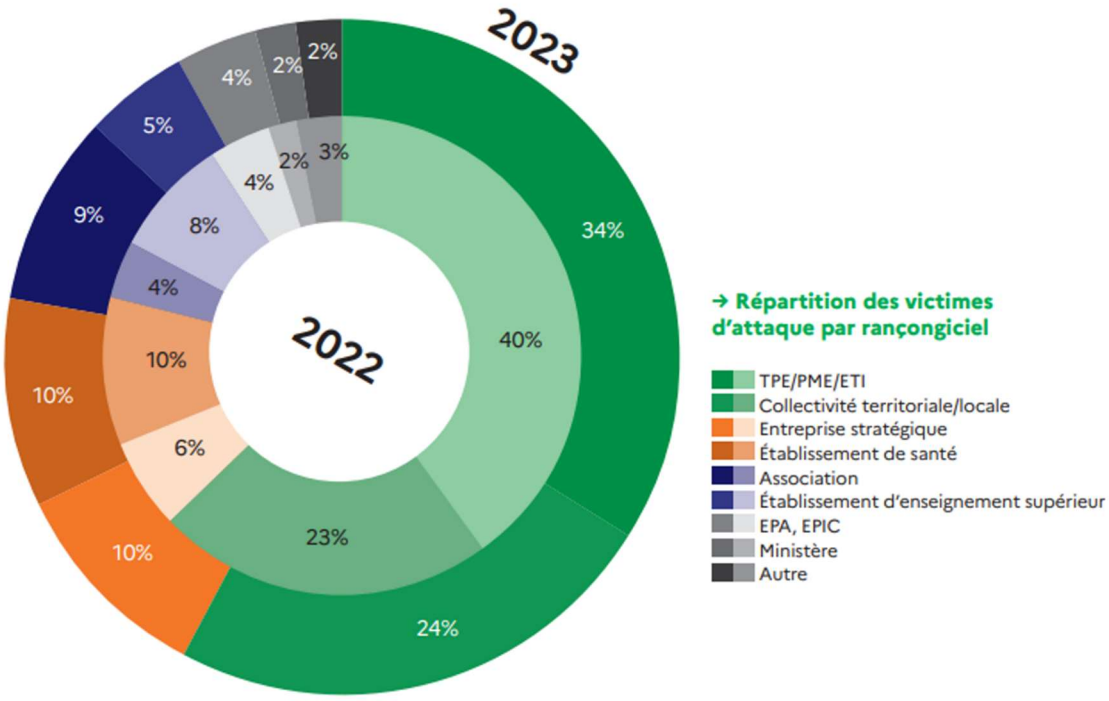
Source (en anglaise) : https://www.varonis.com/blog/data-breach-response-times

Délais de mise à jour par criticité de la vulnérabilité



- Le délai de mise à jour des vulnérabilités critiques et élevées reste très important.
- Il est impératif de comprendre que ce type de vulnérabilité peut faire l'objet d'une exploitation malveillante dans les 24 heures qui suivent sa découverte.

Victimologie



- Il est important de noter que les TPE/PME/ETI représentent une part significative des cibles, pas seulement les entreprises du CAC40.
    - Cause possible : budgets restreints, personnel moins sensibilisé.

Top 4 des menaces

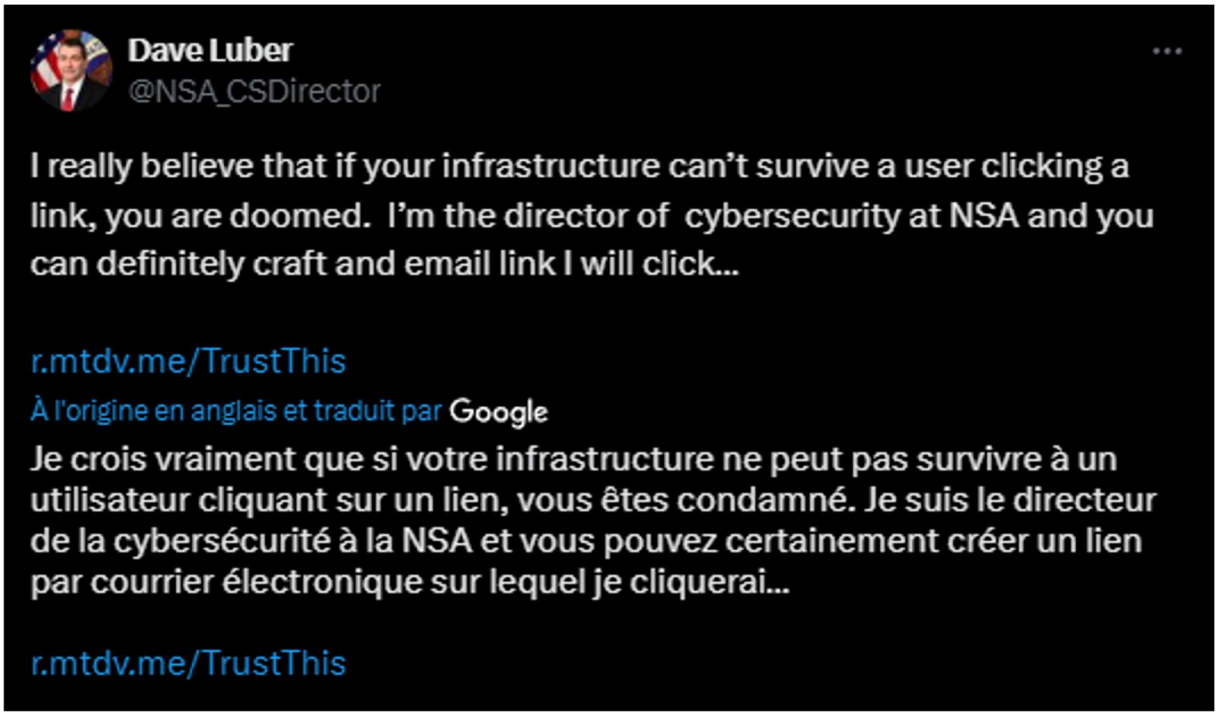
Phishing

But : Se faire passer pour un organisme (banque, service de facturation, etc.) ou un personnel important (directeur) en utilisant les logos et noms de ces entités. Utilisation du format mail ou SMS.

Méthode de compromission : Cliquer sur un lien, scanner un QR Code ou ouvrir des fichiers en pièce jointe.

À prendre en compte : L'arrivée de l'IA accessible rend l'attaque de plus en plus difficile à détecter.

Protections possibles : Formations des personnels, authentification à deux facteurs.



Faux support technique

But : Faire peur en indiquant un problème technique grave. Utilisation d'une fenêtre sur le navigateur internet.

Méthode de compromission : Appel ou téléchargement d'un fichier de prise en main à distance.

Protection possible : La vigilance.

Piratage de compte

But : Prise de contrôle d'un compte (messagerie, application, etc.) au détriment de son propriétaire légitime.

Méthode de compromission : Réutilisation de mots de passe compromis, phishing, utilisation de mots de passe faibles.

À prendre en compte : Vous pouvez devenir vecteur d'attaque sans le savoir.

Protections possibles : Authentification à deux facteurs, gestion des mots de passe sécurisée, éviter de se connecter via les boutons "connexion avec un compte Google, Facebook".

Rançongiciel

But : Bloquer l'accès aux fichiers/appareils et exiger le paiement d'une rançon pour rétablir le service.

Méthode de compromission : Ouverture de pièce jointe, clic sur un lien malveillant, visite d'un site compromis, exploitation de vulnérabilité logicielle.

Protections possibles : Antivirus, EDR (Détection et Réponse Étendue), XDR (Détection et Réponse Croisée).

Mais aussi ...

SEO poisoning : création de site malveillant bien référencé sur les moteurs de recherches

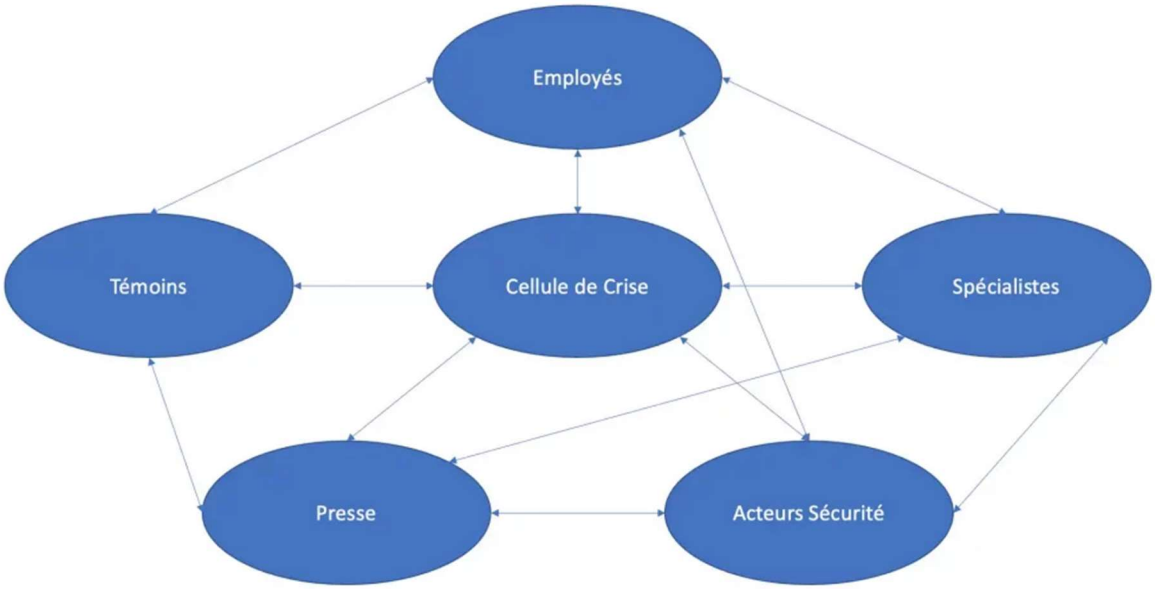
Malvertising : fausse publicité, lien sponsorisé sur les reseaux sociaux

La gestion de cyber-crise

A prendre en compte

- Il n'y a pas de definition type
- Impact potential sur l'ensemble des services / personnels

Les acteurs d'une crise



- À l'inverse d'une crise de type "problème de facturation", on constate une multitude d'acteurs internes et externes possibles.
- On pourrait ajouter : des politiques locaux, les clients, etc.

Source (en français) : https://countact.fr/la-cellule-de-crise/

Pensez à vous rapprocher de votre assurance. Êtes-vous couvert en cas de problème cyber ? Jusqu'à quel montant ? L'assurance a-t-elle des partenaires à vous conseiller ? etc.

La cellule de crise

En réalité, il y a deux cellules :

• La cellule "Direction" : elle décide des actions prioritaires, gère les aspects métiers de l'entreprise, la communication, contact avec les assurances, etc.

• La cellule "Opérationnelle" : elle identifie le vecteur d'attaque, corrige les vulnérabilités et remet sur pied l'infrastructure.

Les outils

Managériaux

• Analyses de risques :Identifier les actifs importants, les risques et les mesures de protection possibles.

• Audit : Audits internes/externes pour vérifier l'efficacité des mesures. Audit des partenaires.

• Processus / Documentation : Faciliter les processus et la documentation pour une réinstallation aisée, la communication interne/externe et s'assurer que les analyses de risques sont prises en compte, etc.

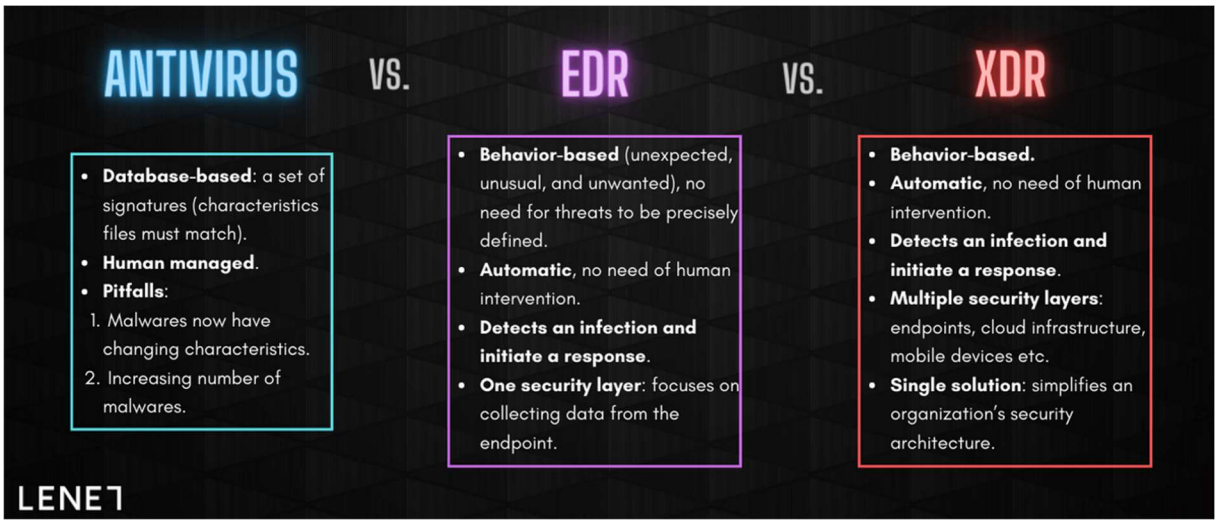
Par exemple, dans le processus de réinstallation du service de paie : "Connaissons-nous l'ordre d'installation des outils, les acteurs impliqués, etc."

• Exercice sur table : Vérifier que les processus sont connus et fonctionnels. Tester les connaissances et compétences du personnel.

• Formations : Former le personnel, constituer une équipe de sécurité, former le personnel aux premiers gestes (comme pour la sécurité physique).

Logiciels

- Antivirus
- Endpoint Detection and Response // Extended Detection and Response
- Data Loss Prevention / Canary
- Gestionnaire de configuration / mises à jour



Source (en anglaise) : https://lenet.com/blog/antivirus-vs.-edr-vs.-xdr-best-solution-for-your-cybersecurity

Liens utiles

Services	Lien
SignalConso est un service public gratuit pour permettre aux consommateurs de signaler les problèmes rencontrés avec les entreprises.	https://signal.conso.gouv.fr/fr
CNIL	https://cnil.fr/fr https://www.cnil.fr/fr/professionnel https://www.cnil.fr/fr/cnil-direct
Cybermalveillance.gouv.fr a pour missions d'assister les particuliers, les entreprises, les associations, les collectivités et les administrations victimes de cybermalveillance, de les informer sur les menaces numériques et les moyens de s'en protéger.	Bonnes pratiques (particulier et professionnels) : https://www.cybermalveillance.gouv.fr/bonnes-pratiques Vous pensez être victime d'un acte de cybermalveillance ? https://www.cybermalveillance.gouv.fr/diagnostic/accueil#signaler Se former (particulier et profesionnels) : https://www.cybermalveillance.gouv.fr/sens-cyber/apprendre Fiche pratique de réponse aux menaces courantes : https://www.cybermalveillance.gouv.fr/tous-nos-contenus/actualites/liste-des-ressources-mises-a-disposition
L'Agence Nationale de la Sécurité des Systèmes d'Information (ANSSI) est l'autorité nationale en matière de cybersécurité. Sa mission est de comprendre, prévenir et répondre au risque cyber.	https://cyber.gouv.fr/securiser-son-organisation
Signal Spam est une association à but non lucratif qui permet aux internautes de signaler tout ce qu'ils considèrent être un spam dans leur messagerie. Les signalements sont assignés aux autorités ou aux professionnels en mesure de prendre des actions contre ces spams	https://www.signal-spam.fr/parcours-signalant/
Orange Cybersecurite : Un site, un lien, un email ou un SMS vous semble suspect ? On le vérifie pour vous !	https://cybersecurite.orange.fr
Faites le point sur votre niveau de protection contre les menaces cyber avec cette check-list des actions indispensables pour être bien protégé des cyberattaques. Ce test vous aidera à déterminer votre niveau d'exposition au risque et à vous préparer contre les attaques en ligne.	https://www.francenum.gouv.fr/guides-et-conseils/protection-contre-les-risques/cybersecurite/check-list-etes-vous-bien-prepare

Un canary token est un mécanisme de sécurité utilisé pour détecter des accès non autorisés à des systèmes informatiques, des réseaux ou des données sensibles. Dans le cas present il s'agit de générer un fichier type Word ou Excel avec un nom qui servira d'appat enc as d'attaque. Une fois ouvert par une personne, vous recevez une notification mail.	https://canarytokens.org/generate
KeePass est un gestionnaire de mots de passe permettant de sauvegarder un ensemble de mots de passe dans une base de données chiffrée sous la forme d'un seul fichier.	https://keepass.info
"Have I Been Pwned" vous permet de rechercher à travers plusieurs violations de données pour voir si votre adresse e-mail ou numéro de téléphone a été compromis.	Tester son adresse mail : https://haveibeenpwned.com Activation les notifications : https://haveibeenpwned.com/NotifyMe

Les 10 mesures essentielles pour assurer votre sécurité numérique

Source (en français) :
https://www.cybermalveillance.gouv.fr/medias/2021/01/FichePratique_SecuriteNumerique.pdf

1. Protégez vos accès avec des mots de passe solides.
2. Sauvegardez vos données régulièrement (il est possible de trouver des disques durs externes pour moins de 100€. Une fois sauvegardées, le disque est débranché et rangé dans une armoire. Cela représente une augmentation significative de votre sécurité pour un coût modeste).
3. Appliquez les mises à jour de sécurité sur tous les appareils (ordinateur, téléphone) dans les 24 heures suivant leur disponibilité et redémarrez vos appareils.
4. Utilisez un antivirus, même sous Mac.
5. Téléchargez vos applications uniquement depuis les sites / magasins officiels (Google Play Store / Apple Store pour les smartphones).
6. Méfiez-vous des messages inattendus (ou trop beaux pour être vrais).
7. Vérifiez les sites sur lesquels vous effectuez des achats (le cadenas ne suffit pas ! Méfiez-vous des offres trop belles pour être vraies, des sites sur lesquels vous ou vos connaissances n'avez jamais réalisé d'achats, etc.).
8. Maîtrisez vos réseaux sociaux et professionnels.
9. Séparez vos usages personnels et professionnels (pas la même adresse e-mail, pas les mêmes comptes en ligne, pas le même ordinateur, etc.).
10. Évitez les réseaux Wi-Fi publics ou inconnus.