DIGITAL

L'ESSENTIEL SUR ...

Cybersécurité et environnements de travail

Décembre 2022

CONTEXTE

- Bureaux, domiciles, cafés, transports…de plus en plus, les salariés français travaillent depuis une multitude d'environnements.
- Si les environnements deviennent plus fluides, ce contexte d'hybridation produit des nouveaux risques. D'après l'Agence nationale de la sécurité des systèmes d'information (ANSSI), le nombre de cyberattaques dans les entreprises avaient augmenté de 37 % entre 2020 et 2021 (près de 3 par jour en moyenne). Cette hausse a été alimentée par l'amélioration des capacités des acteurs malveillants, couplée avec la protection insuffisante de nombreuses entreprises françaises.

Définition

Cybersécurité : d'après IBM, la cybersécurité « est la pratique qui consiste à protéger les systèmes critiques et les informations sensibles contre les attaques numériques. Également appelées sécurité des technologies de l'information (IT), les mesures de cybersécurité visent à lutter contre les menaces qui pèsent sur les systèmes et les applications en réseau, qu'elles proviennent de l'intérieur ou de l'extérieur d'une entreprise».

QUELS SONT LES CYBERRISQUES ?

- Dans le monde des entreprises, les organisations font face à plusieurs types de cyberrisques :
  - **Ransomware (ou rançongiciel)** : des codes malveillants qui bloquent les fichiers ou appareils d'une entreprises. Pour les débloquer, les acteurs malveillants demandent le paiement d'une rançon.
  - **Espionnage informatique entre concurrents**.
  - **Attaques sur la supply chain** : attaquer les entreprises en ciblant les outils moins sécurisés de leur chaîne d'approvisionnement.
  - **Phishing (ou hameçonnage)** : une forme d'escroquerie où les acteurs malveillants se font passer par des organismes connus (banque, service des impôts, etc.). Dans ce cadre, ils envoient des messages en demandant à la victime de « mettre à jour » ou « confirmer » certaines informations sensibles (ex. leurs coordonnées bancaires).
  - **Attaques par ingénierie sociale** : une forme d'attaque qui exploite le comportement humain et ses biais cognitifs. Ainsi, la victime partage des informations sensibles et/ou personnelles.
  - **Espionnage du stock de données sur le Cloud.**

A savoir

- Après une cyberattaque, de nombreuses TPE-PME ne s'en relèvent pas en raison des coûts de réparation.
- D'après le baromètre de NordLocker, les entreprises en France sont parmi les plus cyberattaquées au monde.
- D'après une étude 2022 du cabinet de conseil Mc2i, 40 % des entreprises interrogées n'avaient toujours pas de politique de détection de cyberattaques au printemps 2022.

RÉGLEMENTATION

Loi Godfrain du 5 janvier 1988

- Retrouvée dans le Code Pénal (Livre III, titre II, chap. III), elle englobe toute infraction liée à la fraude numérique et les « atteintes aux systèmes de traitement automatisé de données ».

Cybersecurity Act

- Adoptée à niveau européen, elle encourage la certification de cybersécurité d'un produit et valide le rôle de l'ENISA (l'Agence européenne pour la cybersécurité) dans les échanges entre les Etats.

Règlement Général sur la Protection des Données (RGPD)

- Adopté à niveau européen, il renforce la protection des données personnelles dans l'Union européenne. Depuis l'entrée en vigueur du RGPD, les entreprises sont responsables de l'ensemble des actions de leur écosystème en termes d'utilisation de leurs données, de celles de leurs collaborateurs et de celles de leurs clients.

Directive Nis 2

- Adoptée à niveau européen, elle apporte des normes plus strictes dans la gestion de risques numériques. Concernant une longue liste de secteurs économiques, les mesures de sécurité varient selon le niveau de gravité, de probabilité niveau de gravité, de probabilité et de l'impact du dysfonctionnement sur la société victime d'une cyberattaque.

METTRE EN PLACE UNE STRATÉGIE DE CYBERSÉCURITÉ

Pour mettre en place cette stratégie, il est nécessaire de renforcer trois capacités dans les entreprises.

- **Prévention** :
  - Déterminer l'ensemble de menaces et vulnérabilités ;
  - Mettre en œuvre les mesures ou contrôles nécessaires (campagnes de sensibilisation, restrictions d'accès, copies de sécurité, etc.).
- **Détection de menaces :**
  - Suivre le système de cybersécurité en temps réel ;
  - Gérer les vulnérabilités des différents actifs utilisés.
- **Réaction** : mettre en place des protocoles en cas de cyberattaque ou cybermenace.

BONNES PRATIQUES

- **Utiliser plusieurs mots de passe efficaces.** Ici, il est recommandé de suivre les indications de l'Agence nationale de la sécurité des systèmes d'information (ANSSI) - mot de passe long (au moins 16 caractères) et utilisant des caractères spéciaux -.
- **Activer la double ou triple authentification.**
- **Fournir aux salariés des ordinateurs réservés à un usage professionnel.**
- **Protéger les ordinateurs des risques des connexion hors-site (Wifi public, domicile, etc.)** : l'entreprise doit maîtriser les réseaux Wifi autorisés et pouvoir les désactiver dès que possible au profit d'une connexion LAN. Les PC portables doivent également être en mesure de réserver les connexions au seul VPN lorsqu'elle est active, afin d'éviter les attaques par rebond.
- **Favoriser la communication entre DSI et Directions des environnements de travail.**

BONNES PRATIQUES (SUITE)

S'appuyer sur une architecture « confiance zéro »

- **Principe** : chaque connexion est une menace potentielle pour l'entreprise.
- **Fonctionnement** :
  - Par défaut, les données et ressources des entreprises sont inaccessibles ;
  - Pour accéder aux données et ressources, chaque utilisateur doit respecter un ensemble de règles de sécurité établies en amont ;
  - Chaque utilisateur n'aura accès qu'aux informations nécessaires pour réaliser ses missions.
  - Pour mettre en place une architecture « confiance zéro », il est nécessaire de suivre les prochaines étapes :
    - Cataloguer les actifs du réseau d'une entreprise ;
    - Mettre en place des systèmes pour identifier en permanence les utilisateurs.

Établir les mesures de la norme ISO/CEI 27001

- Adressée à toutes les organisations, la norme ISO/CEI 27001 définit les objectifs à remplir lors de la mise en place d'un système de management de la sécurité de l'information. Pour plus d'informations, n'hésitez pas à visiter le site de l'ISO.

L'AIDE DE L'ÉTAT

- Les entreprises manquent parfois de moyens pour assurer leur cybersécurité. Conscient de cela, l'État s'emploie à faciliter leur transition *via* la mise en place de certains outils.
- Le ministre délégué à la Transition numérique et aux télécommunications a annoncé une série de mesures pour les TPE-PME. Ce dispositif comprend :
  - Une enveloppe de 30 millions d'euros ;
  - La mise en place d'un outil de diagnostic de leur vulnérabilité. Si la vulnérabilité est élevée, et que les entreprises manquent de moyens pour assurer leur cybersécurité, des actions de sécurisation leur seront proposées ;
  - Un « bouclier cyber » pour protéger 750 entreprises issues de secteurs sensibles et susceptibles de constituer un maillon faible pouvant contaminer leurs clients et fournisseurs en cas d'attaque ;
  - Une campagne de communication pour faire connaître le site cybermalveillance.gouv.fr, conçu pour accompagner les entreprises dans leurs démarches.

SOURCES

- **Cyberuniversity** : https://www.cyberuniversity.com/post/la-cybersecurite-et-son-importance
- **Cybermalveillance** : https://www.cybermalveillance.gouv.fr/tous-nos-contenus/actualites/ransomware-rancongiciel-definition#definition-ransomware-rancongiciel
- **Face au Risque** : https://www.faceaurisque.com/2022/10/04/attaques-par-ransomware-les-entreprises-francaises-parmi-les-plus-ciblees-au-monde/
- **Forbes** : https://www.forbes.fr/brandvoice/la-cybersecurite-figure-de-proue-de-lentreprise/
- **HelloWorkplace** : https://www.helloworkplace.fr/travail-hybride-cybersecurite/
- **Serenicity** : https://www.serenicity.fr/loi-cybersecurite/
- **Terranova Security & IPSOS** : https://terranovasecurity.com/wp-content/uploads/2022/10/FROM-DATA-PROTECTION-TO-CYBER-CULTURE-EN.pdf

A propos de l'Arseg

L'Association des Directeurs de l'Environnement de Travail est l'unique instance représentative des professionnels de l'environnement de travail. Grâce à ses 2 000 membres, elle forme un réseau d'organismes privés ou publics, appartenant à tous les secteurs et ayant toutes les tailles.

Pour le prochain *l'EssenTiel sur*, n'hésitez pas à nous transmettre vos suggestions ou documents à : **etudes@arseg.asso.fr**

Avertissement