NEWSLETTER

CYBERSECURITE

TOUS CONCERNES

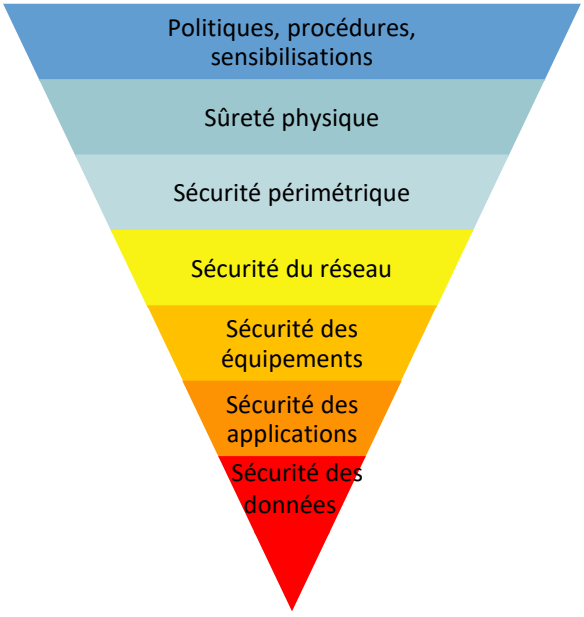
Avec 3 milliards de cyberattaques attendues dans le cadre des Jeux Olympiques *Paris 2024*, la menace cyber n'a jamais été aussi réelle et importante sur notre territoire.

Contrairement aux idées reçues, toutes les structures, quelle que soit leur taille, sont concernées. Si les grandes entreprises et collectivités sont préparées pour faire face à ces menaces, il n'en est pas de même pour les TPE / PME. Plus ou moins bien protégées, elles oublient surtout de sensibiliser les collaborateurs, maillon faible de la sécurité.

Pour vous accompagner, InfoPRO lance une plateforme pour sensibiliser les collaborateurs et gérer les risques humains liés à la cyber.

CYBERMENACE : FORMEZ VOS COLLABORATEURS !

Schéma de la défense en profondeur des systèmes d'information



TOUTES LES ENTREPRISES ONT UNE VALEUR MARCHANDE

Les dirigeants de TPE/PME pensent souvent, à tort, être peu concernés par le risque cyber.

Certes les médias se concentrent principalement sur les attaques touchant les grandes entreprises car cela marque les esprits. Malheureusement, cela fausse la réalité de la menace en passant sous silence les milliers d'attaques dont sont victimes les TPE/PME.

Selon un article des Echos du 11 octobre 2023, sur les 347 000 cyberattaques réussies touchant des entreprises en 2022, 330 000 visaient des TPE/PME, soit 95 % des attaques.

En effet, comme le rappelle le site de cybermalveillance.gouv.fr *« toute entreprise, quelle que soit sa taille, constitue une valeur marchande, que ce soit à travers une trésorerie potentielle ou des informations qu'elle détient. Et les petites entreprises sont d'autant plus faciles à pirater qu'elles sont souvent moins protégées. »*

DES TPE / PME MOINS PROTEGEES

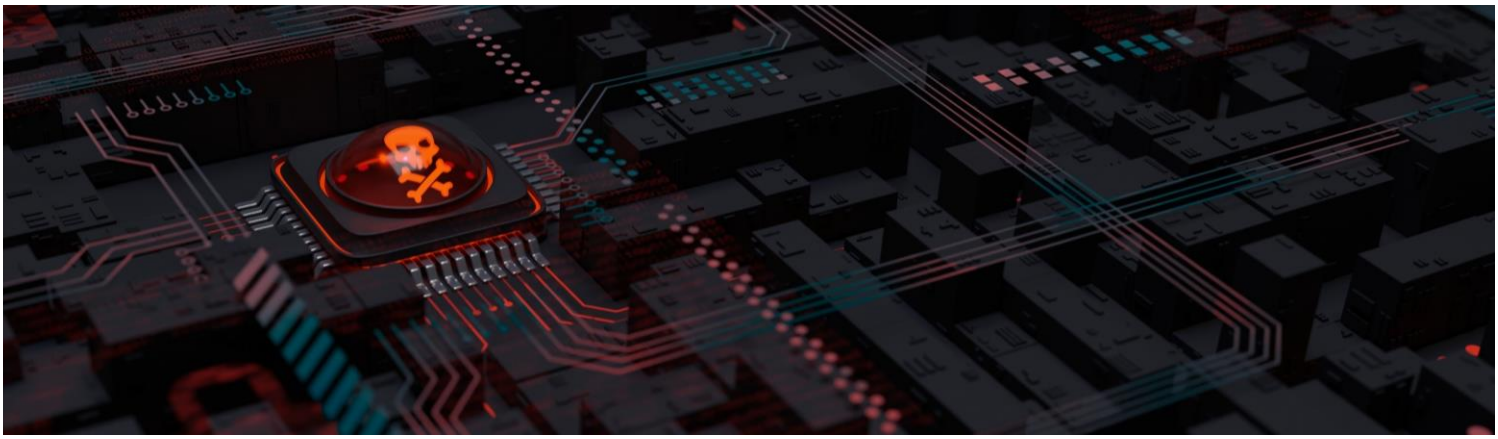
Si les 1ers niveaux de sécurité sont souvent plus ou moins appliqués, le dernier niveau de sécurité relatif à la sensibilisation des utilisateurs est souvent absent.

Or, le plus grand risque reste le facteur humain. L'erreur humaine est la cause principale de 95% des brèches de cybersécurité. Il est donc indispensable se sensibiliser les collaborateurs sur leur rôle dans la sécurité du système d'information et des accompagner à adopter les bons réflexes.

UNE SENSIBILISATION REGULIERE POUR REDUIRE LES RISQUES

Il est donc indispensable se sensibiliser les collaborateurs sur leur rôle dans la sécurité du système d'information et des accompagner à adopter les bons réflexes.

Une sensibilisation régulière et personnalisée permet de réduire les risques, notamment de phishing. Avec une sensibilisation, le collaborateur prend conscience s'il se trouve dans une situation où la sécurité est potentiellement en jeu.



UNE PLATEFORME INFOPRO DE SENSIBILISATION ET GESTION DES RISQUES HUMAINS

Afin d'accompagner les organisations dans l'amélioration de leur dispositif de sécurité, InfoPRO lance une plateforme de sensibilisation à destination des utilisateurs (collaborateurs, élus, stagiaires…) afin de les aider à acquérir les bons réflexes et renforcer leur résilience à la cybermenace. Cette plateforme s'organise autour de 4 volets :

Sessions de sensibilisation à la sécurité

La formation est totalement personnalisée. En effet, lors de la 1ère connexion, chaque utilisateur est invité à répondre à un questionnaire d'une durée de 15 minutes en moyenne afin de définir son niveau de connaissance sur une douzaine de thématiques et mettre en place des modules de formation adaptés.

La formation est accessible à tous avec des cours simples, sans jargon, et un format ludique (une vidéo de 3 à 5 minutes suivie d'un quizz pour vérifier la bonne appropriation des notions fondamentales).

Simulations de phishing

La plateforme permet de réaliser des tests de phishing réalistes pour évaluer le comportement des utilisateurs face à une série de techniques d'attaque.

Surveillance du Dark Web

La plateforme permet de contrôler si des données (identifiant, mot de passe, adresse mail…) sont exposées sur le dark web. Cette information permet de prendre les mesures adaptées pour réduire le risque de piratage.

Gestion de la charte informatique

Afin de s'assurer que les utilisateurs connaissent bien leur rôle et responsabilités dans la sécurité du système d'information, il est indispensable de mettre en place une charte informatique. La plateforme vous facile la diffusion de cette charte informatique et le suivi de sa prise en compte avec les signatures électroniques traçables.

MAIS QUI SONT CES PIRATES ?

Derrière la notion de pirate se cache une variété de cybercriminels totalement différents. Afin de mieux comprendre leur fonctionnement, ils sont répartis 5 grandes catégories :

Black hat : individus détenant de grandes compétences informatiques employées à des fins malveillantes ou destructives. Souvent appuyés par différentes entités, ils détiennent des moyens techniques et financiers importants. Leur motivation principale est le gain financier.

Cyber-terroristes : individus détenant de grandes compétences en hacking, ayant des motivations politiques ou religieuses et cherchant à inspirer la peur. En fonction des groupes, ils disposent de moyens financiers plus ou moins importants. Leur motivation principale est le prosélytisme.

Script Kiddies : individus, souvent très jeunes, ne détenant pas de réelles connaissances en piratage mais parvenant à nuire à des systèmes via des programmes prêts à l'emploi. Particulièrement nombreux, ils agissent en dehors de toute organisation. Parfois motivés par l'appât du gain facile, les script kiddies voient surtout le piratage comme un jeu.

Etatique : individus financés par des gouvernements dans le but de voler des informations secrètes ou nuire à d'autres gouvernements. En fonction des états par lesquels ils sont soutenus, ils disposent plus ou moins de moyens financiers et techniques. Leurs motivations principales sont le cyber-espionnage, la déstabilisation politique et le sabotage.

Hacktivistes : individus prônant des idéaux politiques et utilisant des techniques de piratage pour nuire ou diffuser un message. Ne disposant pas de moyens financiers et techniques importants, ils ciblent leurs victimes.