DÉCEMBRE 2023

CYBERATTAQUES
QUELLES SONT LES PRINCIPALES MENACES ?

FACE AUX CYBERATTAQUES, UNE VIGILANCE DE TOUS LES INSTANTS S'IMPOSE. ELLES SONT DE PLUS EN PLUS NOMBREUSES ET SOPHISTIQUÉES, ET PEUVENT PROVOQUER DE GRAVES CONSÉQUENCES POUR VOTRE ENTREPRISE.

LOGICIEL MALVEILLANT OU MALWARE

Logiciel spécialement conçu dans le but d'endommager ou de désactiver les ordinateurs et les systèmes informatiques (exemple : récupérer des informations personnelles, supprimer des fichiers, prendre le contrôle de votre ordinateur).

Un logiciel malveillant peut se trouver dans des logiciels de téléchargement gratuit (site web non fiable), dans une clé USB dont vous ne connaissez pas la provenance, dans une pièce jointe d'un mail.

HAMEÇONNAGE OU PHISHING

Se faire passer pour une personne de confiance (institution ou personne légitime) afin de soutirer des informations personnelles (données bancaires, mot de passe).

Par mail, appel téléphonique, sms, ou par le biais des réseaux sociaux. Le message contient généralement un lien qui dirige la victime vers un faux site web qui semble identique au site légitime.

VOL DE MOT DE PASSE

Utilisation d'un logiciel qui tentera un maximum de combinaisons possibles dans l'objectif de trouver votre mot de passe.

FRAUDE AU VIREMENT / FAUX RIB

Piratage de la messagerie : le hacker usurpe l'identité du créancier. Il envoie à ses contacts un mail avec la facture et un « faux RIB » contenant les informations bancaires d'un autre compte pour dérober l'argent.

RANÇONGICIEL OU RANSOMWARE

Logiciel malveillant qui bloque l'accès à vos fichiers ou à votre ordinateur en les chiffrant et qui réclame le paiement d'une rançon pour en obtenir de nouveau l'accès.

Si vous cliquez sur une pièce jointe ou un lien frauduleux, parfois en navigant sur des sites compromis ou dû à une intrusion dans le système.

WIFI OUVERTS ET PUBLICS

Des hackers peuvent pirater les connexions afin d'accéder à l'ensemble des informations que vous consultez en vous connectant au wifi ouvert et public.

QUELLES CONSEQUENCES POUR VOTRE ENTREPRISE ?

Perte immédiate d'argent (fraude au RIB).

Perte d'exploitation (arrêt de l'entreprise).

Des coûts directs et indirects : (remise en état du système / coût de reconstruction des informations perdues (ex: fichier client, la facturation, devis / perte de confiance des clients).

RÉALISER UN ÉTAT DES LIEUX DE VOS SYSTÈMES NUMÉRIQUES

De quels équipements / logiciels disposez-vous ?

Quelles conséquences si vos informations sont volées ou détruites ?

Quelles mesures avez-vous pris pour empêcher un hacker d'accéder à vos données (mot de passe, anti-virus, mise à jour des logiciels...) ?

AVOIR UNE VISION GLOBALE DE VOS INFORMATIONS / SOLUTIONS MISES EN PLACE ET SUR LES POTENTIELLES AMÉLIORATIONS.

LA RESPONSABILITÉ JURIDIQUE CIVILE ET PÉNALE DU CHEF D'ENTREPRISE PEUT ÊTRE ENGAGÉE EN CAS DE MANQUEMENT À SES OBLIGATIONS DE PROTECTION DES INFORMATIONS À CARACTÈRE PERSONNEL ET DES SYSTÈMES INFORMATIQUES.

POUR EN SAVOIR + » »

VOUS AVEZ UNE QUESTION ? CONTACTEZ VOTRE CAPEB !

CAPEB L'Artisanat du Bâtiment PLUS FORTS. ENSEMBLE.