LA CYBERSÉCURITÉ

« Ensemble des moyens utilisés pour assurer la sécurité des systèmes des données informatiques d'un Etat, d'une entreprise, etc. » Le Robert

Un concept plus complexe et profond qu'il n'y parait

La cybersécurité, si l'on s'arrête à la définition du « Robert dico en ligne » énoncée plus haut, peut sembler simple. Il existe bien évidemment des définitions plus complètes mais aucune n'est jamais réellement exhaustive. À l'instar du billet qui suit, elles sont le fruit d'une réflexion résultat d'une expérience personnelle.

Pour certain, la cybersécurité s'arrête à une simple installation d'un anti-virus et un mot de passe. Même si c'est un début, dans le monde réel, la cybersécurité est un sujet bien plus complexe à mettre en œuvre pour être efficiente.

Tout d'abord, on ne doit pas se cantonner à la vision étatique ou entreprise de la chose.

La cybersécurité nous concerne tous car nous avons été/sommes/ou seront tous victime d'une cyberattaque, de l'individu à la multinationale en passant par la TPE/PME et l'État.

Il faut appréhender le problème d'une manière globale, sans quoi la démarche sera inefficace. Pas question de lister ici tous les points à vérifier pour avoir une bonne protection contre les risques informatiques. Il s'agit plutôt de vous donner une ébauche rapide de l'état d'esprit et de la philosophie, à adopter.

Des deux postulats de départ en matière de cybersécurité, *la sécurité à 100% n'existe pas et la question n'est pas de savoir si, mais quand on va se faire attaquer*.

On en conclue qu'il est nécessaire de se préparer à l'attaque, à la gestion de crise et enfin à la reprise d'activité.

La préparation s'effectue, si possible, dès le départ d'un projet. Plusieurs textes comme le RGPD1[1], le NIS2[2], certaines normes, vous obligent à vous protéger ou vous donnent des clefs pour mettre en œuvre une politique en matière de cybersécurité. Comme pour tout problème, un état des lieux doit être effectué, suivi d'un diagnostic et enfin d'une solution pour remédier à l'essentiel des failles. Cette politique, quelle que soit la taille de la structure, dépend uniquement de la volonté du décideur qui, pour la mettre en œuvre, peut s'appuyer sur des personnes compétentes en interne ou en sous-traitant.

La gestion de crise. Quand vous avez votre système informatique qui ne fonctionne plus du tout comme par exemple : plus de réservation accessible pour les hôtels, les caisses et les commandes indisponibles dans un restaurant, inaccessibilité aux listes des fournisseurs et de la facturation, aux fiches de payes, un transporteur aérien ou maritime en Corse qui n'a plus de centrale de réservation juste avant le début de la période estivale, un personnel médical qui se fait voler tous ses dossier patients…

Qui fait quoi ? Comment fonctionner ? Qu'est ce qui est essentiel à la survie de la société ? Obligations et risques légaux ? Quelle communication en période de crise ? Comment récupérer les données perdues ?

Tout cela se réfléchit en amont par l'élaboration d'un plan de continuité de l'activité (PCA) qui peut se résumer à une simple feuille A4 en fonction de la structure.

La reprise d'activité se fait par étape, elle fait également l'objet d'un plan, le Plan de Reprise de l'Activité (PRA), elle ne s'improvise pas. Il faut s'interroger sur ce qu'il est nécessaire de redémarrer en priorité et comment revenir à un fonctionnement à 100 % sans oublier l'évolution de la protection des outils informatiques pour ne pas subir immédiatement une nouvelle attaque.

1 Règlement Général Européen de la Protection des Données, règlement (UE) 2016/679 du Parlement Européen et du conseil du 27 avril 2016

2 Network and Information System Security (EU 2016/1148) : assurer un niveau de sécurité élevé et commun pour les réseaux et les systèmes d'information de l'UE

La Corse : un territoire protégé ?

Depuis quelques années des exemples concrets de cyberattaques rendus publics ont permis de mettre en lumière que la Corse, bien qu'étant une île baignée de soleil, n'est pas à l'abri.

Plusieurs secteurs ont été récemment touchés : la recherche avec l'Université de Corse, les transports avec Corsica Linea, la santé avec l'hôpital de Castellucio et des structures ayant des missions de service public. On peut y ajouter, le secteur du tourisme avec des hôtels et des restaurant. Aucun secteur n'a été épargné : Notaires, médecins…

Les particuliers en Corse sont également victimes d'escroqueries ou de vols de données. Il ne s'agit pas forcément d'actes ciblés pour la plupart une bonne hygiène informatique avec les bons réflexes suffiraient à réduire considérablement les attaques ou au moins leur impact.

Être victime d'une attaque informatique n'est qu'une question de temps, il faut juste s'y préparer pour en limiter l'impact.

G.R.,
Membre de l'Association CORSICA SFERA

QUELQUES CHIFFRES

Dans le *Panorama de la menace informatique* du 9 mars 2022 l'Agence Nationale de la Sécurité des Systèmes d'Information (ANSSI) nous informe d'une **augmentation de 37 % des intrusions avérées** dans les systèmes d'information passant de 787 en 2020 à 1082 en 2021. En 2020, les attaques avaient déjà été multipliées par quatre par rapport à 2019. Et il ne s'agit là que des données connues, reste le chiffre noir des atteintes cyber.

Il est intéressant de prendre connaissance de la répartition des victimes d'attaques par **rançongiciel** entre 2020 et 2021.

En effet, **en 2021 les PME/TPE/ETI représentent 52 % des victimes** contre 34 % en 2020. Les collectivités territoriales/locales 19 %, les entreprises stratégiques 10 % et les établissements de santé 7 %.

Une étude IFOP, de fin 2021, montre que 14 % des entreprises victimes déclarent qu'elles ont dû dépenser plus de 50 000 euros pour se remettre en ordre de marche, et même plus de 100 000 euros pour 6 % d'entre elles. Conséquence : **70 % des PME victimes d'une attaque informatique déposent le bilan dans les trois ans**.

MOTS DE PASSE

6, 8, 10, 12, jusqu'où s'arrêtera le nombre de caractères demandés pour un mot de passe et leur complexité (Majuscule, minuscule, caractère spécial, chiffre) rendant ces derniers quasiment impossible à retenir. Si l'on ajoute qu'il faut un mot de passe unique pour chaque application. La crise de nerf n'est pas loin.

De nos jours, le **gestionnaire de mots de passe** permet de répondre à toutes ces exigences de manière simple.

Vulnérabilité incontestée, demain, le mot de passe sera peut-être amené à disparaitre avec le standard FIDO2 soutenu par Google, Apple et Microsoft.

Sans remettre en cause l'efficience du concept, qu'il m'est impossible de juger techniquement, il est toutefois indispensable de s'interroger sur tous les tenants et les aboutissants, comme pour toute innovation qui impacte les données personnelles.

VOCABULAIRE

Rançongiciel ou Ransomware :

Attaque informatique consistant à chiffrer les données de la victimes en les rendant inaccessibles, indisponibles et dont l'objet principal est une demande de rançon. Parfois, les données sont extraites et revendues permettant d'autres attaques sur d'autres cibles.

Gestionnaire de Mot de passe :

Outil permettant de générer et/ou stocker ses mots de passe dans une base de données protégée. L'accès se fait avec un mot de passe unique allégeant la difficulté de mémorisation de l'utilisateur et permettant de choisir un mot de passe très robuste.

LIENS UTILES :

https://www.cybermalveillance.gouv.fr

https://www.ssi.gouv.fr