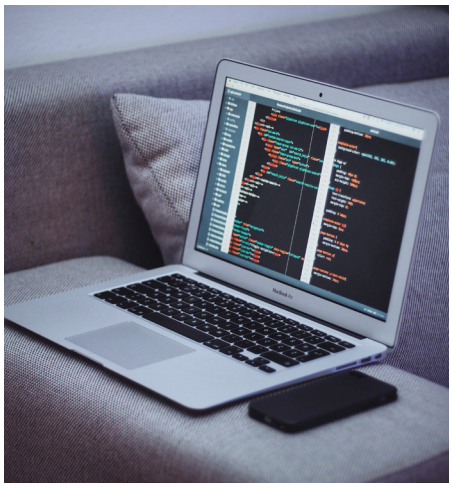
SATEC
COURTIER EN ASSURANCES

L'ACTUALITÉ CYBER EN 2022

Par Amandine Worum,
Référente technique
Cyber Risk

QUELLES SONT LES PRINCIPALES MENACES DE CYBER ATTAQUES ET LES MODES OPÉRATOIRES DES HACKERS ?

Rappelons en préambule qu'une attaque cyber est « une atteinte aux systèmes d'information (SI) de l'entreprise, y compris aux données, réalisée dans un but malveillant ». Par système d'information on entend non seulement les serveurs et ordinateurs mais également les équipements périphériques tels que les imprimantes, ordinateurs portables, téléphones mobiles ou tablettes qu'ils soient isolés ou en réseau.



Les conséquences d'une attaque Cyber sont :
- L'indisponibilité totale ou partielle du SI,
- L'arrêt des usines de production ou des chaînes logistiques
- La perte d'intégrité des données
- L'atteinte à la confidentialité des données personnelles.

Entrainant des impacts directs sur l'activité de l'entreprise/d'une organisation avec une perte de chiffre d'affaires, des frais de traitement de l'incident et des potentielles réclamations de tiers.

Le mode opératoire des attaques est différent selon les motivations des hackers. L'Agence Nationale de la Sécurité des Système d'Information (ANSSI) identifie 4 menaces distinctes d'attaques Cyber : Cybercriminalité, Atteinte à la réputation, Espionnage et Sabotage.

Cybercriminalité

La principale menace est la Cybercriminalité. Elle consiste à récupérer des informations afin de les exploiter dans un but lucratif. Un des modes opératoires le plus largement répandu est le rancongiciel (envoi d'un logiciel malveillant qui chiffre l'ensemble des données et demande le paiement d'une rançon en échange de la clé de déchiffrement). Une autre technique est le hameçonnage (utilisation de faux mails ou faux sites incitant les utilisateurs à communiquer leurs données personnelles/ bancaires et leurs identifiants).

Atteinte à la Réputation

La seconde menace vise l'atteinte à la réputation d'une entreprise ou d'une organisation. Les méthodes utilisées par les hackers consistent à les déstabiliser au moyen d'attaques rendant leur SI indisponible (attaque par Déni de Service « Ddos »), en récupérant des données confidentielles et/ou personnelles (vol de données) ou encore en modifiant le contenu de sites par des revendications politiques, environnementales ou religieuses. Ces attaques sont souvent largement relayées par les médias sociaux.

Espionnage et sabotage

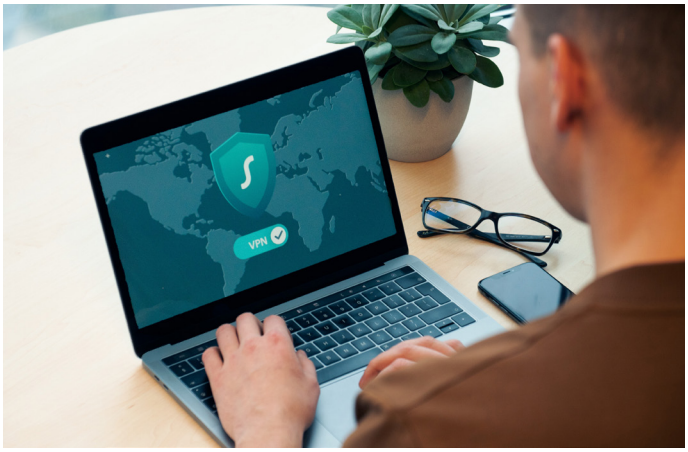
Le Cyber espionnage et sabotage sont des attaques très ciblées et sophistiquées utilisées à des fins géopolitiques, économiques ou scientifiques. TV5 Monde avait été victime de Cyber-Sabotage avec une panne sur l'ensemble de ses réseaux (chaine TV, comptes twitter et facebook, site internet et réseau interne) portant ainsi atteinte à la liberté de la presse.

QUELLES SOLUTIONS POUR AMÉLIORER SA CYBERSÉCURITE ?

La meilleure solution est la prévention !
La Cyber sécurité doit être aujourd'hui un sujet de gouvernance au sein des entreprises et non plus l'affaire de quelques ingénieurs informatiques ou encore d'un prestataire IT externalisé. La crise sanitaire, avec le recours massif au télétravail et le développement du commerce en ligne, a révélé des failles de vulnérabilité des entreprises déjà très fortement dépendantes des technologies de l'information. Dans ce contexte l'ANSSI recommande aux entreprises l'application d'un minimum de mesures d'hygiène de sécurité informatique. Parmi les principales mesures on retrouve :

- La formation et la sensibilisation des salariés aux bonnes pratiques
- Le contrôle d'accès au SI par l'intermédiaire de mots de passe personnels et complexes et mis à jour
- La sauvegarde régulière des données sur des supports externalisés ou déconnectés du réseau
- La mise à jour régulière des systèmes d'exploitation et correctifs de sécurité des logiciels
- La double authentification pour les connexions à distance (VPN)

QUE COUVRE L'ASSURANCE CYBER ?



À l'instar de l'assurance auto, l'assurance Cyber couvre les dommages subis par l'entreprise et les dommages causés aux tiers (réclamations).
L'assurance Cyber comporte également un volet assistance qu'il convient d'activer en premier lieu.
Il s'agit d'une hotline dédiée composée d'experts en gestion de crise disponibles 24h/7J. Le recours à l'assisteur permet de mettre en place les mesures d'urgence immédiates pour limiter et contenir l'incident.

DOMMAGES SUBIS

FRAIS DE GESTION DE L'INCIDENT

Volet Assistance : mesure d'urgence 24h/7j (sans franchise/sous-limite H/€)

Volet Assurance : frais et dépenses
- Experts informatique
- Restauration des données
- Frais de notification
- Frais de communication
- Avocats spécialisés

DOMMAGES DIRECTS

Perte d'exploitation et frais supplémentaires

Cyber extorsion

Enquête et sanctions prononcées par une autorité administrative

DOMMAGES CAUSÉS À UN TIERS (RC)

RÉCLAMATIONS

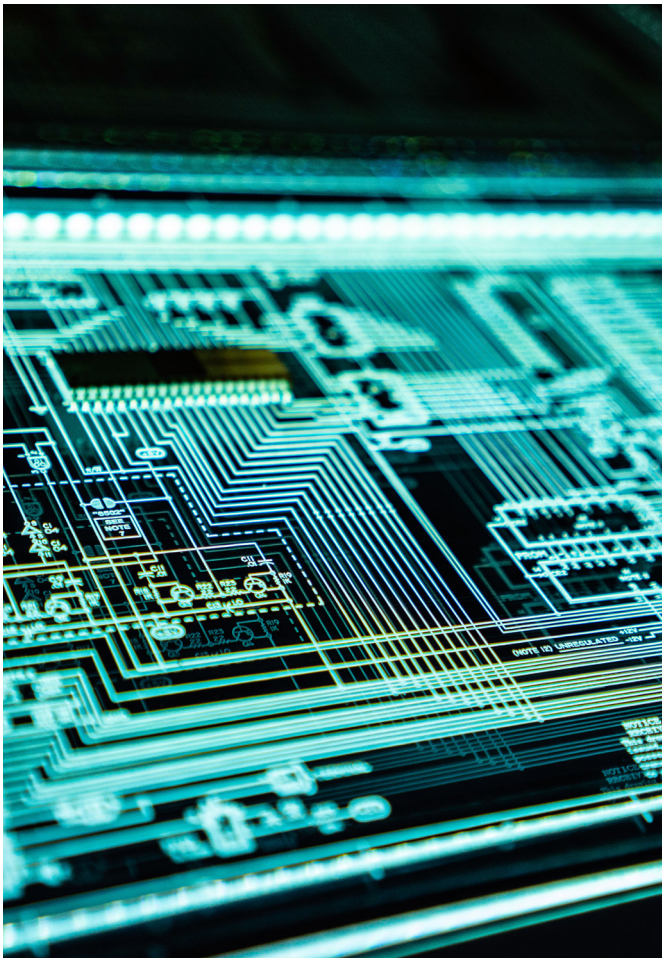
Suite à une atteinte à la confidentialité des données personnelles, à la transmission d'un virus

Manquement à l'obligation de notification

Média, diffamation

UN MOT SUR LE MARCHÉ DE L'ASSURANCE ?

Après une année 2020 marquée par une forte dégradation de la sinistralité, le ratio sinistre sur prime est redevenu rentable en 2021 (Etudes LUCY réalisées par l'AMRAE en 2021 et 2022). Cela au prix de mesures très sévères adoptées par tout le marché pour redresser cette branche d'assurance sinistrée avec d'une part :



- Hausse des primes,
- Relèvement significatif des franchises
- Réduction des capacités délivrées (voire retrait du marché pour certains assureurs ou gèle de toutes nouvelles souscriptions)

Mais également en réduisant la portée des garanties avec l'introduction d'une sous-limite - voire l'exclusion - des incidents d'origine ransomware et/ou du risque systémique.

Parallèlement au durcissement des conditions (prime/franchise/garanties), les assureurs Cyber sont devenus très exigeants sur les critères d'éligibilité et seules les entreprises qui ont investis dans la Cyber sécurité peuvent accéder à une garantie.

Cela se traduit dans les questionnaires de souscription par des prérequis indispensables à l'assurance dont notamment les sauvegardes régulières sur un support externalisé et le déploiement d'antivirus dans les 15 jours suivant leur mise à jour. Certains assureurs exigent même le déploiement de la double authentification (MFA) pour les comptes à privilèges mais également pour les connexions à distance (VPN). Or, dans la majorité des cas, nous constatons que ces mesures de sécurité ne sont pas déployées dans les PME/ PMI les rendant ainsi inéligibles à l'assurance.

Dans ce contexte, notre rôle de courtier est est de vous aider, en amont du processus de souscription à identifier vos potentielles vulnérabilités et les prérequis à déployer.