L'interdépendance et l'hyper-connectivité rendent-elles les entreprises plus vulnérables et quelles solutions à apporter?

Le monde de 2021 est empreint de changement et la récente crise sanitaire a forcé les entreprises (quel que soit leur taille) de lâcher du lest en termes de sécurité informatique. Télétravail oblige, les accès à distance ont considérablement augmenté le risque de cybercriminalité et ainsi facilité la vie des hackers. Le partenaire du GSCGI, Zurich Assurance, informait les Membres du Groupement dans une précédente édition du WealthGram (#96) que le nombre d'attaques cyber avait été multiplié par 5 ces derniers mois.

Bon nombre de sociétés se sont retrouvées du jour au lendemain à l'arrêt, tout au mieux au ralenti, suite à une attaque informatique. Et contrairement aux idées reçues, ces évènements ne touchent pas simplement les grosses structures à forte capacité financière. Il n'y a qu'à regarder le récent piratage de la commune de Rolle qui a vu les données sensibles de quelques 5'000 contribuables mises en ligne sur le *darknet* en quelques minutes. Pas une très belle pub pour la confidentialité helvétique.

De notre expérience, nous pouvons citer plusieurs cas d'attaque ayant eu lieu chez certains de nos clients:

1. Société ayant une activité de production industrielle

Evènement: ransomware provenant de Russie ayant utilisé un canal VPN. Le virus a profité de la vétusté de certains softwares et hardware pour pouvoir pénétrer dans les systèmes d'information.

Conséquences:
- Encryption de l'ensemble des données de l'entreprise.
- Logiciel de backup / restauration anéantis.
- Mise au ralenti de l'ensemble de la partie administrative de la société.

Remédiation:
- Remise en état de l'environnement de sauvegarde (plusieurs dizaines de milliers de francs),
- Travail journalier pendant 3 mois d'un informaticien afin de s'assurer de la mise à niveau sécuritaire de la société (environ CHF 30'000),
- Total du sinistre: CHF 50'000 environ.

2. Société de courtage

Evènement: virus ayant été envoyé à travers un mail et qui a été ouvert par un employé. Le virus avait pour but de rendre l'ensemble de l'infrastructure indisponible afin d'obtenir une rançon.

Conséquences:
- L'ensemble des postes de travail sont devenus inutilisables en quelques minutes.
- Une demi-journée de travail fut perdue pour l'ensemble des collaborateurs qui n'avaient plus accès à leur environnement de travail.

Remédiation:
- L'intervention rapide de l'informaticien a permis d'isoler rapidement le virus et de remettre sur pied le système. La structure informatique robuste, utilisant des canaux sécurisés et travaillant sur des *'virtual machines'*, a permis de contenir également la propagation du virus.
- Aucune rançon n'a été versée.

Le ransomware est devenu de plus en plus important dans le mode opératoire des hackers; l'avènement des crypto monnaies, réputées intraçables, facilite encore plus ce type d'attaque. Un acteur bien connu en Suisse, COMPARIS.CH, en a fait les frais tout récemment avec un blocage massif de leurs systèmes informatiques. Les pirates ont réclamé un montant de CHF 400'000, soit l'équivalent en bitcoin, pour rendre le contrôle des serveurs.

THE IFA's WEALTH GRAM
LA TRIBUNE MENSUELLE DES MEMBRES DU GSCGI
Vol.X — N°109 — Septembre 2021

L'interdépendance et l'hyper-connectivité rendent-elles les entreprises plus vulnérables et quelles solutions à apporter?

Quel est le canal principal par lequel se profile un hacker?

Depuis près de deux décennies, l'ensemble du monde professionnel s'est armé contre les attaques informatiques. De multiples acteurs spécialisés dans la sécurité informatique ont mis sur pied de nombreux moyens techniques tels que les pare-feux, connexions sécurisées, authentification multifactorielle, etc.

Dès lors, le hacker constate que le canal "le plus perfectible" reste l'humain/l'employé. Le télétravail a encore plus accentué les attaques visant l'humain; en voici quelques exemples de ce type d'attaques:

- *Phishing & Spear Phishing*—Courrier ou toute autre communication électronique contenant des informations spécifiques sur le destinataire afin d'inciter ce dernier à cliquer sur un lien, ouvrir une pièce jointe ou toute autre action pouvant mener à des compromissions des systèmes informatiques ou de données.
- *Business Email Compromise (BEC)*—Actions par l'intermédiaire de courrier électronique visant à réaliser des virements bancaires, généralement par la personnification du PDG, du directeur financier ou tout autre cadre supérieur au sein de l'entreprise.
- *Social Engineering*—Manipulation des employés sur un plan psychologique, les incitant à réaliser des opérations inhabituelles.

Quelles actions entreprendre pour réduire les risques? *

Comme mentionné précédemment, nous décelons très clairement deux axes de prévention; le niveau humain et le niveau entreprise. Ces deux axes sont différents mais doivent être le plus complémentaires possible afin d'offrir une sécurité informatique optimale.

Au niveau de l'individu:

- *Liens et pièces jointes*—Ne pas ouvrir des liens ou pièces jointes contenus dans les courriers électroniques en provenance de sources non fiables. Si les employés souhaitent naviguer vers un site Internet, il est recommandé de taper l'adresse du site directement dans le navigateur. Une adresse URL sécurisée doit commencer par le code "https" au lieu de "http". Toutefois, ce critère indispensable est insuffisant, il faut aussi inspecter soigneusement l'adresse URL avant de l'insérer dans le moteur de recherche afin de vérifier qu'elle mène au site officiel de l'entreprise/l'institution désirée.
- *Informations*—Ne pas répondre ni donner des informations au sujet d'un compte ou d'informations bancaires à une source inconnue. Les institutions de confiance, comme les fournisseurs ou les vendeurs, doivent déjà disposer de cette information. Ne jamais envoyer d'informations d'identification et/ou de mots de passe par courrier électronique.
- *Signaler toute activité suspecte et informé le support*—Contacter le service support dès qu'un courrier et sa pièce jointe sont suspects.

Au niveau de l'entreprise:

- *Formation et sensibilisation*—Il est primordial d'investir dans la formation des employés afin qu'ils soient informés des dernières techniques de '*phishing*' et les procédures à suivre dans le cas d'une attaque.

** Document de Zurich Assurance communiqué dans le WealthGram n°96*

L'interdépendance et l'hyper-connectivité rendent-elles les entreprises plus vulnérables et quelles solutions à apporter?

- *Connexions sécurisées*—Utiliser uniquement une connexion à distance sécurisée pour accéder aux réseaux de l'entreprise.
- *Authentification Multifactorielle (AMF)*—Les connexions VPNs doivent être configurées avec une authentification multifactorielle, représentant une couche supplémentaire de sécurité pour assurer que seul le personnel autorisé ait accès au réseau de l'entreprise.
- *Gestion des appareils mobiles*—Les ordinateurs portables doivent être équipés de logiciel prévoyant des contrôles de sécurité et créant un système virtuel crypté afin de stocker les données utilisées.
- *Périmètre de sécurité internet*—S'assurer que les pare-feux sont correctement installés et à jour afin de pouvoir identifier toutes les tentatives d'intrusion à partir d'adresse IP non autorisées.

Quelles peuvent être les réelles implications pour un gérant de fortune suite à une attaque cyber?

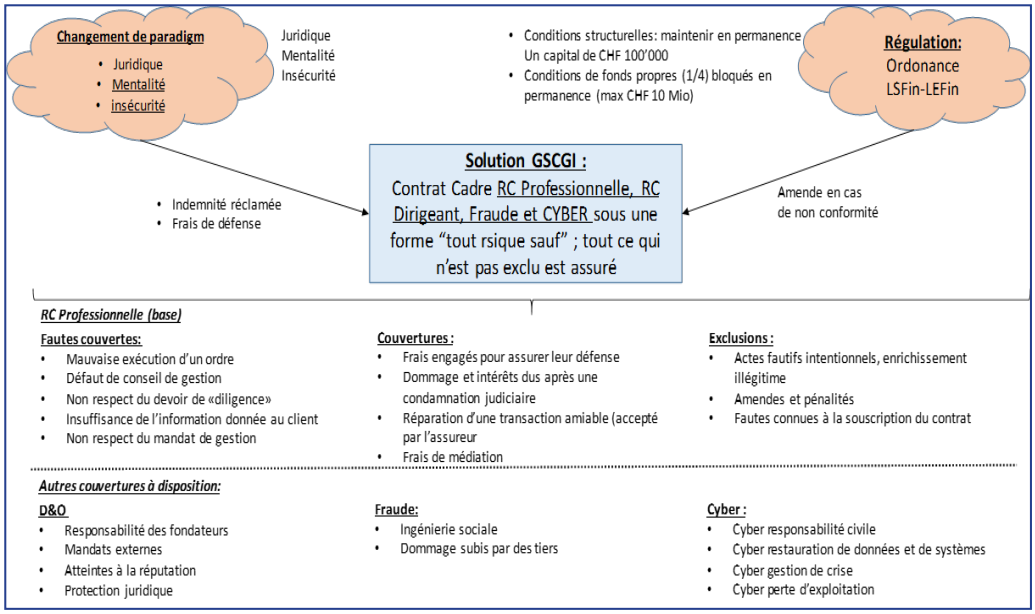
Tout d'abord, nous pouvons citer les dommages infligés sur les infrastructures propres (ordinateurs, serveurs, destructions des informations, ...) rendant impossible ou difficile de passer des ordres, d'accéder au marché ou même simplement d'envoyer des emails. Nous appelons ceci des dommages propres.

Ensuite il y a également la divulgation de données sensibles pouvant faire l'objet de poursuite par les personnes lésées. Ce type d'attaque engendre des frais de procédures, d'avocats ou de médiation. Nous pouvons lier ce type d'attaque à celle subie par la commune de Rolle, s'apparentant à un cas de responsabilité civile informatique.

Pour finir, les cas de fraude peuvent entraîner des pertes financières. Ces cas de fraude peuvent être commis par des tiers ou même par des employés, mais également à la suite d'usurpation d'identité commise de la part d'un tiers.

Au vu de ce qui précède, des solutions d'assurances ont été mises en place et sont de plus en plus sollicitées, peu importe la taille de l'entreprise.

Le contrat-cadre, proposé par le GSCGI et son courtier exclusif (Patrimgest SA), propose une solution complète pour couvrir ce type de risque. Vous les retrouverez dans la partie inférieure du graphique:



THE IFA's WEALTH GRAM
LA TRIBUNE MENSUELLE DES MEMBRES DU GSCGI
Vol.X — N°109 — Septembre 2021

LE SPONSOR DE SEPTEMBRE 2021

L'interdépendance et l'hyper-connectivité rendent-elles les entreprises plus vulnérables et quelles solutions à apporter?

Voici une explication des différentes couvertures proposées (non-exhaustive):

DOMMAGES PROPRES

1. Restauration de données et de systèmes

- Appareils assurés—Les terminaux d'utilisateurs comme les ordinateurs personnels, les ordinateurs portables, les tablettes, les *smartphones*, les téléphones, les appareils de transmission de données; les systèmes de serveurs et de stockage.
- Données assurées—Les informations sous forme de données électroniques, les logiciels, les fichiers audio et images qui sont stockés sur un appareil assuré.
- Evènements assurés—Le cryptage, la détérioration et/ou la destruction de données assurées ainsi que l'impossibilité d'utiliser ou l'utilisation détournée d'un appareil, causés par un logiciel malveillant, un accès ou une utilisation non autorisés.
- Indemnisation—Toutes les dépenses pour:
  - Analyse du sinistre.
  - Reprise de l'activité / limitation de l'attaque.
  - Remplacement des données / appareils électroniques.
  - Tests de remise en état des systèmes.

2. Gestion de crise

- Indemnisation:
  - Frais d'analyse forensiques.
  - Prise en charge des frais d'identifications.
  - Prise en charge des frais de notifications aux autorités.
  - Prise en charge des frais de relations publiques, création de service *call center*.

3. Perte d'exploitation

- Indemnisation:
  - La perte de rendement occasionnées suite à l'interruption totale ou partielle de l'activité de la société.
  - Les frais supplémentaires engagés par l'assuré pour le maintien de l'activité.

PROTECTION JURIDIQUE

Prestations en cas d'un évènement assuré:

- Conseil des mesures juridiques immédiates.
- Dépôt de plainte pénale.
- Défense pénale en cas de violation de protection des données par négligence.
- Demande d'ordonnance pénale.

RESPONSABILITÉ CIVILE (dommages au tiers)

Prestations assurées en cas de violation de la protection des données, de transfert de logiciel malveillant par le réseau informatique de l'assuré, la publication de contenus protégés par l'assuré:

- Indemnisation des prétentions justifiées par le tiers lésé (intérêts, frais de réductions du dommage, d'expertise, d'avocats, de médiation et de procédure de justice).

FRAUDE

Prestations pour tout acte de manipulation de données, diffusion de programme malveillant commis par un employé à l'interne ou à l'externe (ou avec connivence):

- Remboursement de tout dommage financier (frais et dépenses direct) subis par la société.

THE IFA's WEALTH GRAM

LA TRIBUNE MENSUELLE DES MEMBRES DU GSCGI
Vol.X — N°109 — Septembre 2021

LE SPONSOR DE SEPTEMBRE 2021

L'interdépendance et l'hyper-connectivité rendent-elles les entreprises plus vulnérables et quelles solutions à apporter?

LE GSCGI PROPOSE UNE SOLUTION ENGLOBANTE À SES MEMBRES

Outre la solution Cyber apportée, le contrat exclusif proposé par le GSCGI à ses Membres, à travers le partenariat de PATRIMGEST avec deux assureurs de renom (Zürich & Liberty), permet de souscrire à:

- Une assurance Cyber complète (la couverture fraude est conclue dans le contrat RC professionnelle).
- Une couverture en ligne avec les nouvelles exigences FINMA pour la partie RC professionnelle.
- De souscrire à une solution complète combinant la RC Dirigeant ainsi que Fraude ou même Cyber.
- De ne pas devoir immobiliser une somme de garantie pour répondre à ces mêmes exigences.
- De bénéficier de sommes d'assurance non seulement pour l'indemnité potentielle mais également pour les frais de défense ou de médiation découlant d'une plainte.

Conditions pour bénéficier des tarifs préférentiels du contrat-cadre du GSCGI

Cette solution est offerte aux Membres du Groupement Suisse des Conseils en Gestion Indépendants (GSCGI). Une adhésion au Groupement est obligatoire, avec une cotisation annuelle très modérée (amortie par les conditions tarifaires préférentielles du contrat-cadre).

L'adhésion donne en outre accès à plusieurs services et à des accords-cadres spécialement negociés pour les gestionnaires de fortune et conseillers financiers Membres du Groupement, tels que:

- Service juridique
- Contrat-type de gestion discrétionnaire
- Contrat-type de conseil financier
- Accord cadre de formation continue avec l'AZEK
- Permanence fiscale
- Accord cadre avec BRP SA pour les risques *'Cross-Border'* et *'Suitability'*
- Solutions externes pour les services de *compliance officer* et *risk control manager*.
- Conférences mensuelles éducatives.

Etant le courtier exclusif et indépendant du Groupement, PATRIMGEST sera votre partenaire dans l'analyse du risque, du dimensionnement des couvertures nécessaires à vos besoins, ainsi que de la gestion des renouvellements/négociations avec l'assureur choisi.

Intéressé? Nous répondons à toutes vos questions à l'adresse suivante:

Email: info@patrimgest.ch
Téléphone: 021 318 75 00
Site Internet: www.patrimgest.ch

PATRIMGEST

À votre service afin de vous faire bénéficier de notre connaissance approfondie des rouages liés au courtage en

THE IFA's WEALTH GRAM
LA TRIBUNE MENSUELLE DES MEMBRES DU GSCGI
Vol.X — N°109 — Septembre 2021

LE SPONSOR DE SEPTEMBRE 2021

Patrimgest SA: une société dans l'ère du temps de ses clients

Active depuis plus de 20 ans et fondée par un Membre du GSCGI, la société PATRIMGEST est spécialisée dans le courtage en assurances, la gestion de patrimoine, les placements et le conseil juridique.

Société familiale, étant restée totalement indépendante et libre de ses choix, PATRIMGEST adopte une approche «sur mesure» pour ses clients en proposant une analyse complète de leur situation en termes de risque financier, fiscal ou patrimonial.

Bien que gestionnaire de tous les risques assurantiels, l'entreprise s'est spécialisée dans les couvertures financières touchant donc les gérants de fortunes, conseillers financiers et distributeurs de fonds.

Membre du GSCGI depuis plusieurs années, PATRIMGEST a mis sur pied un contrat-cadre d'assurance spécifique aux risques des gestionnaires de fortune. Ce contrat-cadre est exclusif pour le Groupement. Les clients/GFI bénéficient également d'une expertise en termes d'assurances de personnes tels que les caisses de pension surobligatoires et la perte de gain.

Au fil du temps et de l'évolution des besoins des clients, nous nous sommes adaptés afin de pouvoir offrir des nouveaux services tels que:

- Planification financière, fiscale et successorale.
- Conseil global aux indépendants avec gestion de portefeuille titres.
- Négociation de crédit hypothécaires.
- Intégration d'un réseau de courtier international nous permettant de suivre l'ensemble de l'activité de nos clients internationaux et de pouvoir les accompagner dans les différents pays d'activité.

Se voulant être une entreprise dynamique et flexible, nous mettons également l'accent sur une «veille active» nous permettant de rester à la pointe des nouveaux risques et des solutions apportées par le marché. Cette démarche nous permet d'acquérir une analyse fine des risques de nos clients et d'optimiser les solutions apportées tout en garantissant la pérennité de leur activité.

PATRIMGEST possède désormais également une succursale sur Genève en plus de ses bureaux historiques de Lausanne, ce qui permet d'être encore plus proche du tissu économique Romand.

Intéressé? Nous répondons à toutes vos questions à l'adresse suivante:

Email: info@patrimgest.ch
Téléphone: 021 318 75 00
Site Internet: www.patrimgest.ch

PATRIMGEST

À votre service afin de vous faire bénéficier de notre connaissance approfondie des rouages liés au courtage en assurances et à la gestion de patrimoine.