Jamais sans mon expert

LA CYBER SÉCURITÉ

DOSSIER · DOSSIER · DOSSIER · DOSSIER · DOSSIER

Christophe PRIEM
Centre Val de Loire
Président de l'IFEC

Marie-Christine LAMPERT
Paris Ile-de-France
Dirigeante Associée
Expert-comptable, L3 Conseils

Stéphane JULLIEN
Rhône-Alpes
Directeur du Système d'Information Groupe IN EXTENSO

Eric AGUILAR
Occitanie
CEO ACSF
Cyber sécurité financière numérique/fintech
Officier de réserve Gendarmerie nationale

Christophe FORET
Nord
Président C-Risk
Co-chair FAIR Institute Paris

CHRISTOPHE PRIEM
PRÉSIDENT DE L'IFEC

LE MOT DU PRÉSIDENT

Depuis l'invasion de Poutine en Ukraine, le nombre de cyberattaques a fortement décuplé. Aujourd'hui, nous sommes dans un monde fortement digitalisé et les cybermenaces sont par conséquent omniprésentes.

Pour y faire face, malheureusement, tout le monde n'est pas logé à la même enseigne. Alors que les ETI et les grands groupes sont relativement bien armés contre les cyber-risques, les TPE et PME peinent à se protéger, faute de moyens et de temps.

Les hackers l'ont bien compris et les ciblent en priorité afin de tenter d'accéder à leur système d'information ; aucune organisation n'est totalement à l'abri d'une attaque aujourd'hui.

On peut donc dire que, si la transformation numérique est source de développement et d'opportunités pour les entreprises, elle se double d'une menace grandissante pour celles-ci.

Tous les secteurs d'activité sont visés par les cyberattaques.

Le contexte du télétravail a accentué ces risques. Le télétravail a en effet mis au jour les failles de sécurité des entreprises. Les collaborateurs ont été amenés à travailler avec du matériel personnel et mal protégés, non sécurisés par VPN. Ils ont pu travailler, échanger, télécharger sans une sécurité optimale.

C'est pourquoi, l'entreprise doit repenser la mise en place des systèmes de défense pour se protéger, sachant que le premier risque à réduire est l'erreur humaine. Il faut donc savoir se préparer aux cyber risques ; c'est une étape fondamentale dans la gestion de crise.

I Des chiffres et des définitions

Eric AGUILAR
Occitanie
CEO ACSF
Cyber sécurité financière numérique/fintech
Officier de réserve Gendarmerie nationale

Plus de 4 000 cyberattaques par jour dans le monde !

Les cyberattaques constituent le nerf de la guerre numérique. On estime qu'une entreprise française sur deux est visée chaque année par une cyberattaque. **En 2022, 45 % des entreprises ont subi une attaque réussie** (dommages matériels et réputationnels) contre 54 % en 2021. Ces derniers mois, l'actualité nous a montré que tout le monde peut être touché : hôpitaux, institutions, collectivités locales, les pompiers, les groupes du CAC40 tout comme les PME et TPE.

Le paysage du « cyber espace » est en constante évolution. **La cybercriminalité,** qui comprend le vol, le détournement de fonds, le piratage et la destruction de données, **a augmenté de 600 % depuis la pandémie de COVID-19**. Avec la démocratisation du cloud et du télétravail, tous les secteurs doivent adopter de nouvelles solutions de cyber sécurité, obligeant les entreprises, les États et les institutions à adapter leurs techniques de travail pour mieux protéger leurs données.

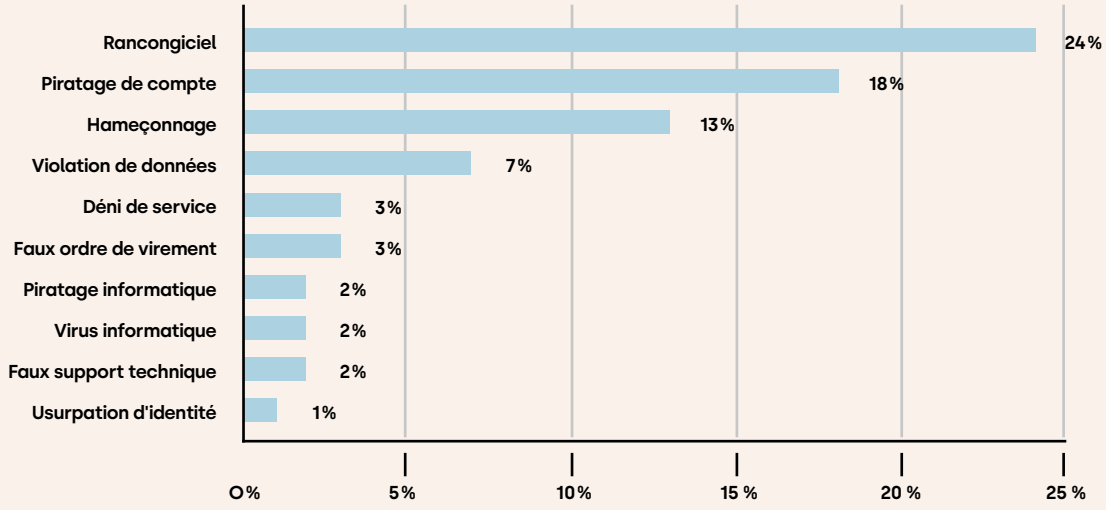
Dans son rapport annuel d'activité, le GIP ACYMA (Groupement d'Intérêt Public Action contre la Cyber malveillance) révèle une hausse importante des demandes d'assistance en ligne : **173 000 demandes en 2021** pour la plateforme cybermalveillance.gouv.fr, soit 65 % de plus que l'année 2020 (voir graphique*).

Même constat dans le rapport d'activité 2021 de la Commission nationale de l'informatique et des libertés (CNIL), **où les PME et les micro-entreprises représentaient 69 % des notifications de violations de données personnelles** liées au piratage informatique.

De son côté, l'ANSSI aura enregistré **1 082 intrusions au sein de systèmes d'informations en 2021**, soit 37 % de plus qu'en 2020.

On estime que la cybercriminalité coûtera aux entreprises du monde entier environ 10 500 milliards de dollars par an d'ici à 2025, contre 3 000 milliards de dollars en 2015, selon le rapport de Cybersecurity Ventures. La cybercriminalité représente même à ce jour le plus grand transfert de richesse économique de l'histoire, comme le précise le rapport d'AT&T.

Principales recherches d'assistance pour les entreprises et associations



Quelques définitions

- ANSSI : l'Agence Nationale de la Sécurité des Systèmes d'Information, instance officielle, accompagne les entreprises en fonction de leur profil par des actions de conseil, de politique industrielle et de réglementation afin de rendre disponibles des produits de sécurité et des services de confiance.
- Cyberattaque : Une cyberattaque désigne tout acte malveillant portant atteinte à un système IT pour des raisons d'ordre politico-économique. Vol de données, phishing, ransomware, spoofing...
- Cryptovirus : Cryptovirus ou Crytolocker est un ransomware ou rançongiciel, un logiciel pirate imaginé et conçu par des cybercriminels. Depuis 2013, ce logiciel malveillant se promène sur le Net en infiltrant les ordinateurs des utilisateurs de Microsoft ou Windows.
- DDOS : Une attaque par déni de service distribué (DDoS) est une arme de cyber sécurité visant à perturber le fonctionnement des services ou à extorquer de l'argent aux organisations ciblées.
- Hacker : Est un spécialiste informatique qui recherche les moyens de contourner les protections logicielles et matérielles.
- Malware : logiciel malveillant.
- Phishing : L'hameçonnage (phishing en anglais) est une technique frauduleuse destinée à leurrer l'internaute pour l'inciter à communiquer des données personnelles (comptes d'accès, mots de passe...) et/ou bancaires en se faisant passer pour un tiers de confiance.
- Rançongiciel ou Ransomware : Est un cheval de Troie qui chiffre les fichiers de l'utilisateur et prend en otage ses données personnelles afin qu'il puisse demander à leur propriétaires une somme d'argent.

II Cyber mois 2022 : faire face aux cyberattaques

Eric AGUILAR
Occitanie
CEO ACSF
Cyber sécurité financière numérique/fintech
Officier de réserve Gendarmerie nationale

« Si vous pensez que les produits de sécurité offrent à eux seuls une véritable sécurité, vous vous contentez de l'illusion de sécurité. »
Kevin MITNICK

Cybermalveillance.gouv.fr, autorité gouvernementale, a piloté avec l'ANSSI en octobre 2022 une campagne de sensibilisation aux cyberattaques.

Place au Cyber Mois 2022 !
Octobre, c'est le mois pour prendre conscience ou approfondir ses connaissances des enjeux de sécurité numérique et, ainsi, adopter les bons réflexes pour sécuriser ses usages. Nous sommes tous de plus en plus actifs dans nos vies numériques, et par conséquent, de plus en plus exposés aux cyber-risques qui ne cessent d'augmenter.

C'est l'occasion de faire un point sur les cyberattaques : **Sous quelle forme peut se manifester une cyberattaque ? Comment les éviter ?**

Qu'est-ce qu'une cyberattaque ?

> **" Une cyberattaque est une atteinte à des systèmes informatiques réalisée dans un but malveillant.**

Elle cible différents dispositifs informatiques : des ordinateurs ou des serveurs, isolés ou en réseaux, reliés ou non à Internet, des équipements périphériques tels que les imprimantes, ou encore des appareils communicants comme les téléphones mobiles, les « smartphones » ou les tablettes[1].

Les cyberattaques peuvent prendre différentes formes, parmi les plus fréquentes :

- **Le phishing**

Le phishing ou l'hameçonnage est une forme d'escroquerie. Le fraudeur se fait passer pour un organisme connu (banque, service des impôts, CAF, etc.), en utilisant le logo et le nom de cet organisme. Il envoie un mail demandant généralement de "mettre à jour" ou de "confirmer vos informations suite à un incident technique", notamment les coordonnées bancaires (numéro de compte, codes personnels, etc.)[2].

Plus récemment apparaissent les escroqueries au faux RIB, où le pirate intercepte (middle attaque) le formulaire bancaire d'un fournisseur afin de le substituer par un RIB mentionnant ses coordonnées bancaires et de tromper son client[3]. Les boites email des « deux côtés », client ou fournisseur peuvent avoir été piratées !

Si des identifiants peuvent être récupérés grâce au phishing, certains hackers utilisent des méthodes nettement plus simples : ils testent les mots de passe les plus logiques par rapport au compte. Prénoms, dates de naissance, de mariage, adresse... Ils essayent des dizaines de combinaisons jusqu'à tomber sur la bonne. Pour éviter cela, il faut choisir des mots de passe compliqués, et ne pas hésiter à jeter un œil sur le site qui indique si le mot de passe a été piraté.

- **Le Faux Ordre de Virement (FOVI)**

L'escroquerie aux faux ordres de virement (FOVI) est un type d'arnaque qui, par persuasion, menaces ou pressions diverses, vise à amener la victime à réaliser un virement de fonds non planifié. Parfois présenté comme émanant d'un dirigeant et ayant un caractère « urgent et confidentiel », on parle alors « d'arnaque au Président », communément.

1. https://www.gouvernement.fr/risques/risques-cyber
2. https://www.cnil.fr/fr/cnil-direct/question/le-phishing-cest-quoi
3.https://www.cybermalveillance.gouv.fr/medias/2021/01/Faux-Ordres-De-Virement.pdf

Une variante consiste à usurper l'identité d'un fournisseur pour communiquer de nouvelles coordonnées bancaires (changement de RIB) sur lesquelles il faut effectuer un règlement.

Une autre variante consiste à usurper l'identité d'un chargé de clientèle bancaire pour valider une opération en attente de paiement, (divulgation mot de passe et login), ou bien d'un salarié pour demander le changement des coordonnées bancaires où virer son salaire. Le compte bancaire appartenant à l'escroc est souvent situé à l'étranger, en Europe où par la suite les sommes détournées rebondiront aussitôt sur des comptes Asiatiques.

Cette catégorie d'escroquerie est généralement réalisée par téléphone et systématiquement confirmées par email. Elle concerne tous les types d'organisation[4].

- **Le piratage informatique**

Le piratage informatique ou atteinte au STAD, (système de traitement automatisé des données), consiste à s'introduire, sans autorisation, dans une ressource comme un ordinateur, un serveur, un réseau, un service en ligne ou un téléphone mobile, ou tout autre objet connecté. L'objectif du pirate informatique est de prendre le contrôle de la ressource et/ou de dérober des informations dans le but d'en faire un usage malveillant.

En pratique, le piratage informatique peut prendre deux formes principales : le piratage d'un compte ou le piratage d'un équipement[5].

Pour les hackers, il est facile de créer un réseau wifi public, gratuit et sans mot de passe, en usurpant le nom d'un réseau connu (café, galerie commerçante...). Les utilisateurs qui vont vouloir s'y connecter sont cependant en danger, car les pirates pourront se servir de ce lien informatique pour voler leurs données numériques. Afin de se protéger contre les faux réseaux wifi, il faut s'assurer de la fiabilité du réseau... Il ne faut jamais installer de mise à jour en utilisant un réseau wifi inconnu, et encore moins d'acheter des produits.

- **Les attaques par logiciel malveillant**

Un logiciel malveillant, malware en anglais, est un programme ou un code créé dans le but de causer des dommages à un serveur, à un réseau ou à un ordinateur. Il s'introduit en douce dans un système informatique, de sorte que lorsque l'utilisateur s'aperçoit que son système est infecté, des données ont généralement déjà été compromises[6].

Par exemple, un cheval de Troie informatique ou Trojan est un programme d'apparence inoffensive, mais qui contient un logiciel malveillant installé par l'utilisateur lui-même, ignorant qu'il fait pénétrer un intrus malveillant sur son ordinateur.

- **Les rançongiciels**

L'attaque par rançongiciel, ransomware en anglais, désigne une cyberattaque qui bloque l'accès à l'appareil ou à des fichiers en les chiffrant et réclame à la victime le paiement d'une rançon pour en obtenir de nouveau l'accès.

Les chiffres démontrent en effet un intérêt décroissant des cybercriminels pour les particuliers, jugés sans doute moins solvables, tandis que les rançongiciels constituent la première cybermenace chez les professionnels, avec une hausse de plus de 95 % en 2021[7].

Deux types de ransomwares co-existent : ceux qui relèvent de l'espionnage et de la vente de données sur le dark, (origine criminalité organisée, étatique) à forte rançon et ceux qui relèvent d'opportunisme, de robots, ou d'organisations criminelles, uniquement destinés à récupérer une rançon « résiduelle » pour déchiffrer les fichiers compromis.

> **L'usage de la cryptomonnaie est exclusivement dédié à ces fins.**

4.https://www.cybermalveillance.gouv.fr/tous-nos-contenus/fiches-reflexes/escroquerie-faux-ordres-virement-fovi

5.https://www.cybermalveillance.gouv.fr/tous-nos-contenus/actualites/quels-sont-les-differents-types-de-piratage-informatique

6.https://www.crowdstrike.fr/cybersecurity-101/malware/

7.https://www.cybermalveillance.gouv.fr/tous-nos-contenus/actualites/cybersecurite-les-cybermalveillances-les-plus-frequentes

Comment éviter les cyberattaques ?

Dans un contexte d'industrialisation et de professionnalisation de la cybercriminalité, le droit est une arme essentielle pour renforcer la stratégie de sécurisation de ses actifs. Il est nécessaire d'être précautionneux et de rester vigilant en ligne. Il existe de nombreuses choses à faire, en amont, ou ne pas faire, pour se protéger de ces attaques.

A FAIRE POUR LES ENTREPRISES

- **Protéger et valoriser votre actif informationnel**
  - Audit et diagnostic (identifier les données stratégiques et sensibles ; identifier les partenaires clés et les sources de risques commerciaux et juridiques…),
  - Compliance RGPD (sécuriser la licéité et la disponibilité de vos bases de données…),
  - Secret des affaires (cartographie et protection défensive de votre patrimoine immatériel…).

- **Sécuriser vos contrats du numérique**
  - Sous-traitance (rédiger, négocier, et mettre en place vos accords de sous-traitance…),
  - Conditions générales (maintenance dynamique de vos conditions générales…),
  - Accords d'échanges de données (encadrer et valoriser vos échanges de données…),
  - Responsabilité des partenaires (négocier, rédiger des clauses de responsabilité des prestataire…).

- **Définir une PSSI (Politique de Sécurité du Système d'Information)**

- **Souscrire une assurance cyber-risques**

A FAIRE POUR LES PARTICULIERS

- **Activer votre filtre anti-spam**
- **Télécharger un logiciel anti-virus**
- **Installer l'authentification à deux facteurs**
- **Survoler l'URL avant de cliquer**
- **Chercher les fautes d'orthographe et de grammaire**

A NE PAS FAIRE

- **Cliquer sur des téléchargements inconnus**
- **Répondre à des appels ou des emails d'expéditeurs inconnus**
- **Dévoiler vos informations personnelles à des sources inconnues**
- **Utiliser le même mot de passe pour se connecter à plusieurs comptes différents**
- **Se servir d'un ordinateur professionnel à des fins personnelles, confusion des boites emails, aller sur les réseaux sociaux, télécharger des fichiers ou applications diverses…**

Que faire en cas de cyberattaque ?

Si vous pensez être victime d'une cyberattaque, quel qu'en soit le type, voici quelques conseils à adopter :

Premiers réflexes :

- **Déconnectez immédiatement les équipements suspects du réseau et les éteindre**, en retirant le câble réseau ou en déconnectant le Wi-Fi, afin d'éviter la propagation de l'attaque.
- **Laissez les équipements suspects allumés, uniquement en cas de ransomware et sur le poste récepteur du message de compromission demandant la rançon, n'essayez pas de les modifier** afin de préserver les éléments techniques nécessaires à la compréhension de l'incident puis éventuellement à l'enquête.
- **Ne connectez aucun autre appareil** sur le réseau.
- **Gardez les preuves de l'attaque** (messages reçus, machines touchées, journaux de connexions…).
- **Contactez immédiatement le service informatique ou le prestaire informatique,** pour qu'il puisse déclencher la mise en place d'un dispositif adéquat de gestion de l'incident.

Piloter la crise (si vous êtes responsable) :

- **Déposez plainte** avant toute action de remédiation en fournissant toutes les preuves en votre possession.
- **Mettez en place une cellule de crise** pour gérer les conséquences de la cyberattaque et coordonner les actions.
- **Tenez un registre** des évènements et des actions réalisées pour pouvoir en conserver la trace à disposition des enquêteurs et tirer les enseignements de l'incident a posteriori.
- **Avertissez la CNIL dans les 72h**, si des données à caractère personnel ont été consultées, modifiées ou détruites. En cas de risque élevé pour les données, vous devez également notifier les personnes concernées.
- Si vous êtes un opérateur d'importance vitale, **prévenez l'ANSSI dans les meilleurs délais.**
- **Mettez en place des solutions de secours** pour pouvoir continuer d'assurer les services indispensables : activez vos plans de continuité et de reprise d'activité (PRA/PCA) si vous en disposez.
- **Préparez une stratégie de communication** adaptée au sujet afin d'informer avec le juste niveau de transparence vos administrés, agents, partenaires, fournisseurs…

Sortir de la crise :

- **Faites une remise en service progressive et contrôlée** après vous être assuré que le système attaqué a été corrigé de ses vulnérabilités et en surveillant son fonctionnement pour pouvoir détecter toute nouvelle attaque.
- **Tirez les conclusions, les enseignements pour améliorer la sécurité** après une intrusion et définissez les plans d'action et d'investissements techniques, organisationnels, contractuels, financiers, humains à réaliser pour pouvoir éviter, ou a minima, pouvoir mieux gérer l'éventuelle prochaine crise.

III Des exemples d'attaques

Eric AGUILAR
Occitanie
CEO ACSF
Cyber sécurité financière numérique/fintech
Officier de réserve Gendarmerie nationale

Des exemples d'attaques relayés par la presse...

Une attaque de grande ampleur

SEPTEO, un groupe de 2 400 personnes, spécialisé dans le logiciel pour les notaires, les avocats, les SIRH et l'immobilier (12 millions d'utilisateurs) a été victime d'une cyberattaque en janvier 2023. Des experts techniques et d'investigation indépendants ont été mobilisés. « Nos investigations continuent et Notamail reste perturbé mais les indicateurs de ce matin sont positifs » déclarait le dirigeant début février.

Des hackers pro-russes

Les attaques par déni de service distribué (DDoS) reprennent du poil de l'ours, en ce début d'année 2023. Les groupes de hackers pro-russes inquiètent de nombreux pays à la suite de cyberattaques à l'encontre de ministères, hôpitaux et banques.

> **Depuis le 1er janvier 2023, plus d'une centaine de cyberattaques de type DDoS ont été détectées, lancées par des groupes de pirates pro-russes plus ou moins organisés. Parmi les « team » les plus virulentes, hors le groupe nationaliste Killnet, présenté par ZATAZ* au lancement du conflit entre la Russie, l'ours NoName057.**

Depuis le 1er janvier, ZATAZ a repéré des dizaines d'attaques contre la Lituanie, l'Italie, la Pologne, l'Estonie, le Danemark, la République Tchèque, l'Ukraine, l'Allemagne.

Des élections ciblées

Des cyberattaques qui se veulent politiques. Par exemple, plusieurs sites internet tchèques ont été visés le premier jour du scrutin du second tour des élections présidentielles. Les sites Internet du candidat à la présidence Petr Pavel et du ministère tchèque des Affaires étrangères se sont retrouvés bloqués sous les coups de NoName057.

Hôpitaux compris

Pour rappel, un DDoS a pour mission de rendre inutilisable un service informatique en le noyant de fausses connexions. Imaginez un camion de poubelle venir déverser ses détritus devant vos portes et fenêtres. Plus personne ne peut sortir, ni entrer, dans le logement. Killnet a utilisé cette méthode à l'encontre de sites web appartenant à des hôpitaux américains, forçant le ministère américain de la Santé et des Services sociaux à publier une alerte avertissant les établissements de santé des tactiques du groupe pirate.

> **" Il est probable que des groupes ou des opérateurs de rançongiciels pro-russes, tels que ceux du défunt groupe Conti, répondront à l'appel de Killnet et apporteront leur soutien. Cela entraînera probablement que les entités ciblées par Killnet seront également touchées par des ransomwares ou des attaques DDoS comme moyen d'extorsion, une tactique que plusieurs groupes de ransomwares ont utilisée ».**

Acheter des DDoS

Les autorités agissent, mais les malveillants trouvent toujours, pour le moment, les ressources pour leurs actions. En décembre 2022, le ministère de la Justice saisissait, avec l'aide d'autorités judiciaires de par le monde, 48 sites (6 noms de domaine principaux) utilisés par des vendeurs de services DDoS. Des sites web qui permettent aux utilisateurs d'acheter des minutes de DDoS afin d'inonder de fausses connections leurs cibles.

> **Les américains avouaient que « cette mesure d'application de la loi » pouvait n'avoir que très peu d'impact sur des groupes tels que Killnet « qui a transformé son service DDoS à louer en une opération hacktiviste ».**

Le Danemark victime des DDoS

Il y a quelques semaines, le Danemark a annoncé relever son niveau d'alerte cyber à la suite de cyberattaques contre des banques et le ministère de la Défense du pays.

> **" Nous élevons à nouveau le niveau de menace contre le Danemark, entre autres sur la base du niveau élevé d'activité des groupes de pirates informatiques pro-russes contre les pays de l'OTAN, y compris le Danemark » annonce le Centre danois pour la recherche cyber sécurité sur Twitter.**

Un pays précurseur dans le 100 % numérique. La digitalisation par défaut : santé, impôts, Etc. Ce qui n'empêche pas les DDoS ou encore les infiltrations de type ransomware comme après l'attaque à l'encontre de DSB, équivalent de la SNCF, le 29 octobre 2022. Une cyberattaque ayant paralysé le trafic ferroviaire.

Les DDoS utilisées comme couverture

Bien que les attaques DDoS ne causent généralement pas de dommages majeurs ou durables, elles peuvent provoquer des interruptions de service qui s'étendent sur plusieurs heures, voire plusieurs jours. Akamai a publié un rapport révélant que les incidents DDoS en Europe avaient augmenté de 73 % en 2022, avec davantage de campagnes impliquant désormais des tactiques d'extorsion. Ils ont averti que les attaques DDoS sont désormais de plus en plus utilisées comme couverture pour de véritables intrusions impliquant des ransomwares et des vols de données.

La santé touchée

Le groupe Ramsay invite le personnel administratif de ses cliniques à ne plus toucher l'informatique jusqu'à nouvel ordre à la suite de la découverte d'une anomalie ! Plusieurs établissements de santé du groupe Ramsay (Toulouse, Bourg-en-Bresse) tournent au ralenti, le temps de contrôler des anomalies informatiques découvertes. « Des anomalies ont été détectées sur certains serveurs informatiques et nous soupçonnons une tentative d'intrusion extérieure confirme le service presse à ZATAZ. Par mesure de sécurité pour protéger les patients, employés et partenaires, la procédure de sécurité a été immédiatement déclenchée, à savoir la fermeture des accès extérieurs. Nous avons immédiatement informé nos partenaires et les autorités sanitaires et mobilisé des experts techniques et d'investigation indépendants, et l'enquête que nous avons menée avec eux n'a révélé aucun vol de données ni aucun cas de propagation de l'incident à nos patients. » Voilà qui est rassurant. Action, réaction.

Arnaque à la Sécu

En juin 2022, ce fut un envoi massif de SMS demandant « la mise à jour de la carte vitale », par un pirate informatique inconnu, à destination de centaines de milliers de français. Derrière ce phishing qui pourrait sembler classique, il s'agissait d'une cyberattaque massive à l'encontre des hexagonaux.

> **Ce pirate informatique a lancé sa malveillance informatique de Russie. Son SMS est propre, efficace, rapide : « Assurance Maladie : Renouvellement obligatoire de votre Carte Vitale à effectuer avant le 10/06/2022. Rendez-vous immédiatement sur : assurance-maladie[.]com ».**

Jusqu'ici, rien de particulier. Quand vous sélectionnez, sans cliquer, sur l'url proposé, une page d'erreur. Seulement, le format et le support exploité, les smartphones, permettent bien des manipulations. Quand vous cliquez sur l'adresse web présente dans le message, redirection vers la page usurpatrice. Sur téléphone portable cela passe en douceur, sans faire apparaitre la moindre trace de malversation. Autant dire que 99 % des gens pourront tomber dans le piège. D'autant plus que l'internaute arrivera sur une page sans faute, aux couleurs, logo et url ressemblant comme deux gouttes d'eau à l'assurance maladie : [ameli]carte-vitale.com.

De la suite dans les idées

Le black hat a des moyens, du temps et de la suite dans les idées. Il ne s'est pas contenté d'AMELI. Il s'est organisé pour viser une dizaine d'entreprises officiant sur le territoire hexagonal. Le pirate a lancé des cyberattaques aux couleurs de la Banque Populaire, Caisse d'Epargne, Netflix, FNAC, ...

> **Une motivation qui peut s'expliquer par la recherche massive de données et d'un besoin important de liquidité pour des pirates qui souffrent, aussi, du conflit entre la Russie et l'Ukraine.**

Les collectivités locales pas épargnées

Une cyberattaque contre la région Normandie s'ajoute à une longue liste de collectivités territoriales touchées par les pirates en 2022. **L'impact de cette opération est conséquent puisque 600 serveurs et 1 500 ordinateurs ont été arrêtés.** Compte tenu de leur impact, les attaques contre les régions et les départements sont plus médiatisés, les données de millions d'habitants peuvent être prises en otage et divulguées sur les forums de hackers. De plus en plus d'organismes publics sont touchés par des cyberattaques.

Un ransomware déjoué aux USA

Après une opération secrète de plusieurs mois, le ministère américain de la Justice (DOJ) et ses partenaires internationaux (en Allemagne, aux Pays-Bas et en France) ont mis hors d'état de nuire un réseau international de ransomware connu sous le nom de Hive. Depuis 2021, le groupe de ransomware Hive a ciblé plus de 1 500 victimes à travers le monde, obtenant plus de 100 millions de dollars en paiements de rançon de la part d'hôpitaux, d'écoles, ou encore de sociétés financières. Les autorités ont désorganisé le groupe de ransomware Hive en infiltrant ses réseaux informatiques et en saisissant ses clés de déchiffrement.

*ZATAZ : est un site web français d'information traitant principalement de la délinquance informatique.

Témoignage d'une cyberattaque au cabinet L3 Conseils

Marie-Christine LAMPERT
Paris Ile-de-France
Dirigeante Associée
Expert-comptable, L3 Conseils

Le cabinet L3 Conseils est une petite structure de 8 personnes qui intervient dans le conseil et l'accompagnement de petites et moyennes entreprises de tous secteurs avec une bonne connaissance du milieu audiovisuel. L3 Conseils compte environ 300 clients ; elle a subi une cyberattaque par cryptovirus dans la nuit du 23 au 24 mai 2019.

« L'attaque est survenue heureusement juste après nos bilans et le traitement de la TVA du mois d'avril. C'était miraculeux si on peut dire...

Pour rappeler le contexte, on avait classiquement un serveur de production qui hébergeait également la messagerie, un seul site, une sauvegarde sur un NAS avec une réplication au domicile via une liaison internet. Le prestataire informatique est un ami et le contour de la mission n'était pas vraiment formalisé.

Le 24 mai au matin, nous avons constaté en arrivant au bureau que nous n'avions plus accès à rien (la connexion à distance était également inactive depuis 7h du matin). Les fichiers étaient cryptés ; un visuel de tête de mort apparaissait à l'ouverture des fichiers sur tous les postes. Nous avons vite compris ce qui arrivait et avons rapidement constaté l'ampleur du désastre ; presque toutes les sauvegardes avaient été chiffrées. Le premier réflexe a été de tout débrancher d'internet.

Un message nous invitait à contacter le pirate dans le « darkweb » mais cela ne nous tentait pas... !

Nous n'avons jamais su si les données avaient été aspirées. Nous étions en tous cas paralysés. La seule partie non cryptée était la base bureautique contenant les dossiers annuels et les dossiers permanents. La messagerie était bloquée mais heureusement, nous avions les contacts dans les téléphones.

Nous avons très rapidement mis en place un mail de secours et envoyé un message d'attente à nos clients.

L'assurance groupe, contactée, nous a mis en contact très vite avec une cellule spécialisée d'experts en cyberattaque. Nous avons déposé plainte (sans grand espoir) et averti la CNIL. Les experts ont alors fait un état des lieux précis afin de savoir notamment combien de clés de chiffrement avaient été utilisées et si le ransomware était connu.

Au bout de deux jours, nous savions qu'il n'y avait rien à faire si ce n'est de payer la rançon. Il fallait donc discuter avec le pirate, il n'a pas répondu pendant une semaine. Une semaine difficile car nous étions dans l'incertitude et à l'arrêt complet. Les paies de mai n'ont pas pu être faites, nous avons demandé aux clients de verser des acomptes à leurs salariés.

Le pirate a enfin répondu en demandant 15 000 € en bitcoins pour nous débloquer. Il faut 2 semaines pour ouvrir un wallet permettant de payer en bitcoins mais le cabinet spécialisé en possédait un et a donc payé le pirate à notre place (rançon payée par virement par nous en attendant de connaitre la position de l'assurance).

Une fois la somme visible sur son portefeuille virtuel, le pirate a envoyé des clés de déchiffrement. Elles ont d'abord été testées par les experts puis déployées sur notre serveur et tout a été décrypté en quelques heures au bout de 15 jours !

Sur le plan humain, cette expérience a été un bon test de cohésion d'équipe et nos clients ont tous été compréhensifs.

Sur le plan technique, ce fut une leçon : nous ne pouvons pas espérer éviter les attaques mais nous savons que le meilleur moyen est de réfléchir en amont à comment réagir quand cela se produit.

L'expérience nous a tous rendus méfiants et conscients de la vulnérabilité des systèmes. Nous sensibilisons maintenant nos clients régulièrement. Aujourd'hui, nous n'avons plus de serveur, nous utilisons le cloud et systématiquement la double authentification, tout en veillant bien à la qualité de nos sauvegardes ».

Fallait-il vraiment payer ?

Le cabinet n'avait pas vraiment le choix. Mais il peut arriver qu'il y ait une sur-attaque. Un virus peut rester sourd plusieurs mois. Il est important de faire une sauvegarde de la sauvegarde. La mise en place de la double authentification est un bon réflexe.

www.l3conseils.fr

Témoignage d'une cyberattaque au cabinet In Extenso

Stéphane JULLIEN
Rhône-Alpes
Directeur du Système d'Information
Groupe IN EXTENSO

Ignorer le risque n'est pas une option

Sur le plan IT, In Extenso est sur une architecture complexe gérée de manière centralisée et orientée volumétrie et flux de données avec environ 1 500 serveurs à l'échelle du groupe, 700 lignes réseaux et 6 000 unités de bureautique. En tant que profession réglementée, la protection de la donnée est un sujet fondamental au niveau de notre activité.
Avant la cyberattaque, il est bon de préciser que In Extenso est certifié ISO27001, que nous sommes équipés d'un outil contre la fuite de données et que nous avons un management de la sécurité avec un ensemble d'outils de protection et de supervision.

Tout commence par un coup de fil...

En avril 2021, je reçois un appel, un dimanche à 1 h du matin, c'est la supervision de notre infrastructure qui m'informe que toute notre activité est à l'arrêt du fait d'une attaque ; nous sommes entièrement cryptolockés. Une fois la stupeur passée, il est temps de dérouler le process de gestion de crise que nous avons anticipé. Une réunion est organisée le dimanche matin avec la direction générale et les parties prenantes pour constater et prendre les premières décisions fondamentales lors d'un incident de ce type.

Un premier constat

Nous avons été attaqués par un groupe russe de cybercriminalité qui demande une rançon. Il est important de savoir que dans ce cadre nous avons affaire à une organisation internationale qui fonctionne comme une entreprise avec un ROI sur les attaques et par conséquent des moyens considérables et une sophistication des techniques d'attaques.

> **"La première question qui ressort est « devons-nous payer ? ».**

Cette question se traduit en fait par un constat simple : avons-nous des sauvegardes, sont-elles cryptées et avons-nous une stratégie de restauration qui permette de rétablir les services essentiels ? Les pirates, lorsqu'ils lancent une attaque comme celle-ci sont dans votre système depuis plusieurs mois ; la stratégie qui consiste à restaurer votre système au jour précédent l'attaque est inefficace car votre sauvegarde embarque les outils des pirates. Nous avions délocalisé nos sauvegardes en dehors de notre SI. Par conséquent, il est décidé lors de cette première réunion de ne pas payer et de nous relever de cette attaque par nous-mêmes.

> **"La deuxième question qui ressort est « Combien de temps cela va durer ? ».**

Cette question est très délicate et varie d'une entreprise à l'autre. Il faut savoir qu'en moyenne la remédiation d'un tel évènement prend plusieurs mois ; il est nécessaire de se concentrer sur les services essentiels de l'entreprise afin de ne pas pénaliser le business, la feuille de route est rapidement tracée.

La remédiation

La stratégie est simple : nous couper du monde, considérer que tout élément du SI est corrompu, même ce qui ne le semble pas à première analyse, remettre à blanc l'intégralité du système d'information, en reconstruire un plus sécurisé et réinjecter uniquement les données métier des sauvegardes et enfin rétablir progressivement le service.
Derrière cette simple phrase se cache une complexité importante, **les points fondamentaux à retenir sont :**
La communication doit être gérée finement ; une organisation est mise en place ; la communication est gérée par la direction générale avec des points journaliers avec le DSI ; personne d'autre ne communique à l'extérieur ni ne communique avec les équipes.
C'est un projet, par conséquent et au vu des enjeux, l'approximation n'a pas sa place, celui-ci doit être géré dans les règles de l'art. Tout doit être tracé. Tout doit être vérifié. Tout doit être maîtrisé.
Une trentaine de partenaires, des équipes opérationnelles 24/24, une gestion de projet avec plus de 3 000 lignes d'opérations tracées, un process cadré, mécanique et organisé nous ont permis de revenir à une situation business opérationnelle en moins d'un mois. Aucune fuite de données n'a été constatée et nous avons drastiquement élevé nos exigences en termes de sécurité, que ce soit en interne comme pour nos partenaires externes.

De la menace à l'opportunité

Cet événement nous a permis de prendre conscience qu'il existe différents niveaux dans les cybermenaces. Bien évidement nous avons révisé notre système de management de la sécurité, nos process internes ainsi que nos outils. La sensibilisation de l'ensemble des collaborateurs aux problématiques de sécurité a été renforcée et nous pouvons dire à la suite de cet événement que la protection cyber des actifs de l'entreprise ainsi que ceux de nos clients fait vraiment partie de l'ADN du groupe. Toutes les mesures de sécurité peuvent être vues comme un dogme de la DSI à l'échelle du groupe par certains mais elles sont nécessaires et intransigeantes, on a toujours le niveau de sécurité du maillon le plus faible.

Nous avons subi une nouvelle attaque du même groupe en août 2021, cette fois-ci sans succès, malgré la violence de l'attaque (20 000 tentatives de connexions étrangères à l'heure pendant 3 jours), les pirates ont été détectés instantanément et notre système a tenu le choc.

En conclusion, il faut se poser les bonnes questions

Ayez les bonnes questions. La question n'est pas de savoir si ça va arriver, mais quand. **Il faut se demander « que vais-je faire une fois que mon système sera corrompu ? ». C'est la seule question qui compte vraiment.**

Prévoyez la crise, rejouez le scénario avant. Ayez une démarche proactive. Qui communique ? Ai-je les bons partenaires ? Qui appeler en cas de besoin et surtout comment ? Quelles sont les stratégies de retour à la normale ? Lors d'une attaque, le stress, les enjeux, vous n'aurez pas les idées claires et ça ne sera plus le moment de vous demander ce qu'il faut faire. Surtout choisissez avant le bon partenaire opérationnel qui saura vous conseiller et vous accompagner. Si vous n'avez pas les ressources internes pour gérer les problématiques de sécurité, externalisez l'activité et prenez un SOC (Security Operation Center).

Investir dans une stratégie Cyber peut être très couteux ; mettez vos investissements dans un système de sauvegarde fiable et sécurisé en premier lieu ; faites un audit de vos sauvegardes et de la protection de celles-ci.

Prenez une assurance Cyber spécialisée. De la même manière, une remédiation peut être couteuse, choisissez un contrat d'assurance pour vous faire accompagner sur ce type de sinistre.

En ce qui concerne notre stratégie actuelle, elle est sur deux volets : d'une part la protection et d'autre part la capacité au travers de l'automatisation de réduire le temps de reconstitution et remédiation d'une attaque à une semaine. La sensibilisation et formation est aussi un élément central et notre système d'information est testé plusieurs fois par an au travers de tests techniques (pentest) mais aussi de tests de phishing pour l'ensemble des collaborateurs.

L'uniformisation de votre système d'information, de vos actifs IT, la gestion perpétuelle de vos mises à jour sont un élément clé. La gestion des droits d'accès et de « qui a accès à quoi » doivent être maîtrisés, l'idéal étant de limiter au maximum les privilèges.

Ne soyez pas naïfs, les cyberattaques sont un risque et comme tout risque il se gère, sa probabilité, son impact sont très élevés. Par conséquent, ignorer ce risque n'est pas une option et fonder la protection des actifs et des services essentiels d'une entreprise sur la chance n'en n'est pas une non plus.

In Extenso réalise des services à destination des TPE-PME, tant dans les domaines de l'expertise comptable que dans les domaines liés à la gestion et à l'accompagnement du chef d'entreprise.

Notre groupe propose un service professionnel complet, à tous les stades de la vie de l'entreprise et sur l'ensemble des domaines liés à la gestion de l'activité de nos clients : comptabilité, fiscalité, gestion, juridique, conseil social et paies, gestion du patrimoine du dirigeant, conseil en innovation-croissance, transmission d'entreprise.

In Extenso est l'interlocuteur privilégié de plus de 120 000 clients appartenant à tous les secteurs d'activité et a réalisé en 2022 un chiffre d'affaires de 500 millions d'euros.

In Extenso est un groupe avec plus de 5 500 collaborateurs répartis sur 250 agences.

I Cyber risques, cyber sécurité et gouvernance

Christophe FORET
Nord
Président C-Risk
Co-chair FAIR Institute Paris

La cyber sécurité et les cyber risques sont devenus des thèmes récurrents et centraux de nos conversations, et nous pensons tous parler des mêmes choses. Mais est-ce vraiment toujours le cas ?

La Cyber Sécurité

La cyber sécurité fait référence à l'ensemble des activités, des méthodes et des solutions permettant d'assurer la sécurité des systèmes informatiques – et des informations qu'ils contiennent. Elle est ainsi un ensemble de réponses aux risques cyber.

> **Le plus grand problème avec la communication c'est l'illusion qu'elle ait eu lieu.**
> George Bernard Shaw

Au fur et à mesure de la digitalisation de nos économies et nos sociétés au cours de la dernière décennie (>60 % du PIB mondial digitalisé fin 2025[1]), la cyber sécurité est devenue un des tous premiers postes budgétaires de la direction informatique puisqu'elle représente jusque plus de 10 % du budget informatique.

Apparemment à juste titre lorsqu'on rapproche ces investissements de la place qu'occupent les risques cyber dans les classements des risques opérationnels. Ainsi, le baromètre des risques de Allianz[2], celui du World Economic Forum[3] et beaucoup d'autres, classent, depuis plusieurs années, le risque cyber parmi les trois ou quatre risques opérationnels les plus importants.

Les Risques Cyber

Puisque ce sont les risques cyber qui légitiment les investissements en sécurité informatique, définissons de quoi on parle. Le Larousse définit le risque comme étant « la possibilité, la probabilité d'un fait, d'un évènement considéré comme un mal ou un dommage ». Singulièrement, le monde de l'entreprise a élargi cette définition et ISO 31000 définit le risque comme étant : "l'effet de l'incertitude sur les objectifs" et laisse ainsi la possibilité de conséquences préjudiciables… ou bénéfiques.

Dans le secteur informatique, la norme ISO/IEC Guide 73 précise que c'est « la possibilité qu'une menace donnée exploite les vulnérabilités d'un actif ou d'un groupe d'actifs et cause ainsi un préjudice à l'organisation. Il est mesuré en termes de combinaison de la probabilité d'occurrence d'un événement et de ses conséquences. »

Ces imprécisions sémantiques sont loin d'être anodines car on parle de risque en pensant alternativement aux vulnérabilités, aux menaces, aux vecteurs d'attaques ou encore aux impacts redoutés sur la disponibilité, la confidentialité ou l'intégrité des systèmes d'informations et les données.

Cyber risque : Toute **atteinte**, volontaire ou non à la **confidentialité, l'intégrité ou la disponibilité** des **données** numériques ou du **système** d'information.

MENACE	impacte →	**ACTIF**	résultant en →	**SINISTRE**
Cybercriminels, Acteurs des Etats-nations, Script Kiddies, Nature, Personnel, Clientèle, Tierces parties, etc…		Données, Site web, Applications, Réseau, Serveur etc…		Atteinte à la **C**onfidentialité Perte d'**I**ntégrité des données Pannes/in**D**isponibilité

1. WEF 2019 & International Monetary Fund 2020, 2. Allianz Risk Barometer 2022, 3. WEF Global Risks report 2023

La Gouvernance des risques cyber et de la sécurité de l'information

On voit bien que le risque cyber mérite une définition plus précise. Initialement technologique, il ne peut plus être considéré seulement comme une problématique technique mais bien comme un véritable risque métier. Après avoir été géré principalement par les experts sécurité du département informatique, c'est un sujet dont les fonctions métiers et régaliennes de l'entreprises doivent s'emparer avec l'aide des experts informatiques et de la cyber sécurité pour comprendre quels sont ces risques en les liants aux actifs métiers (données, applications, processus industriels, propriété intellectuelle, ...) les plus essentiels au bon fonctionnement de l'entreprise.

Il existe de nombreux frameworks et méthodes pour conduire un programme de sécurité des SI et/ou gérer les risques – NIST, ISO31000 et 27005, EBIOS RM, ... Mais la plupart sont destinées à des populations d'experts et ne s'adressent donc pas aux responsables métiers. Ils restent génériques et pas prescriptifs quant à la mise en œuvre de ce qu'ils préconisent. Or la gestion des risques pour répondre correctement à l'exigence de la gouvernance de la sécurité informatique doit justement éclairer, assister la prise de décision.

Les entreprises ont donc jusqu'à présent utilisé des approches essentiellement qualitatives qui reposent sur l'expérience et le savoir-faire des experts et des cartographies haut/moyen/bas ou rouge/orange/vert pour classifier les risques. Les démarches pour prioriser les investissements en cyber sécurité sont guidées par la conformité et les bonnes pratiques qui sont certes nécessaires mais pas suffisantes – des études du Gartner montrent ainsi que de lourds investissements n'apportent pas forcément un gain important en termes d'amélioration de la sécurité, faute d'avoir investi là où cela était réellement nécessaire[4].

Pour efficacement décider des priorités sur lesquelles l'entreprise doit porter ses efforts, toutes les fonctions métiers, IT et infosec doivent parler le même langage afin de se comprendre et comparer puis choisir ensemble les solutions de sécurité les plus adaptées. L'approche qualitative et les avis divergents des experts ne suffisent pas. Il faut un modèle détaillé et robuste qui permette de mesurer et classifier les scenarios de risques entre eux, dans le contexte de l'entreprise (activités, géographie, business model, nature des données collectées et traitées, ...). Sur cette base objective et quantifiable, l'entreprise pourra sélectionner les contrôles et solutions de sécurité qui réduiront le plus l'exposition aux cyber risques.

Le rôle des professions du chiffre dans la gestion des risques cyber

Dans toutes les entreprises mais en particulier celles de taille intermédiaire et les PME, les experts-comptables ont un rôle à jouer dans cette identification des actifs critiques et des risques associés. En effet, ils ont une bonne connaissance des chaines de valeur, c'est-à-dire de la manière dont l'entreprise produit sa proposition de valeur. Ils ont la connaissance, d'un point de vue financier, des actifs, y compris ceux intangibles dont une partie croissante est sous une forme digitale et donc exposée en premier chef aux risques cyber.

> Enfin, c'est précisément un des rôles des experts-comptables et des commissaires aux comptes que de rendre compte des résultats économiques et financiers de l'entreprise et d'identifier, puis évidement de quantifier, les risques et incertitudes qui pèsent sur l'atteinte de ces résultats.

4. https://www.gartner.com/en/newsroom/press-releases/2016-12-09-gartner-says-many-organizations-falsely-equate-it-security-spending-with-maturity

La quantification des risques cyber

Christophe FORET
Nord
Président C-Risk
Co-chair FAIR Institute Paris

Le standard FAIR™ (Factor Analysis for Information Risk) explique comment analyser et exprimer les risques en termes métiers et, lorsque c'est nécessaire, quantifier financièrement les scénarios de risques cyber et opérationnels.

Analyser et exprimer les scénarios de risques

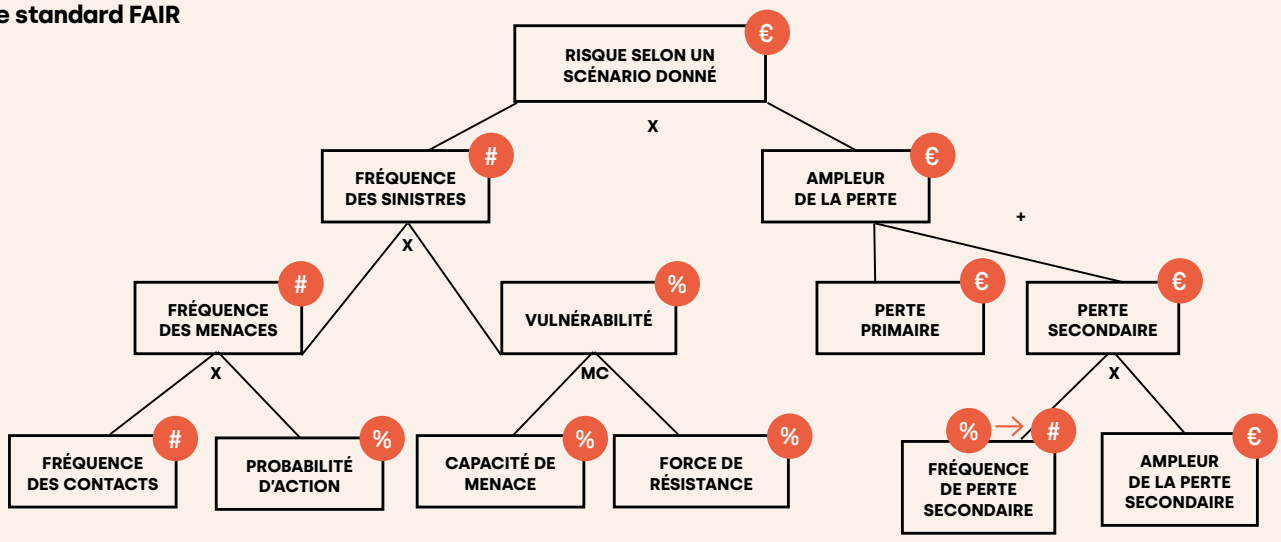
Pour analyser et exprimer les scénarios de risques, le standard FAIR propose une ontologie qui est une série de définitions de termes décrivant également les liens entre ces termes et les concepts sous-jacents. Elle est plus complète et détaillée que celles qu'on trouve dans les standards déjà mentionnés.

L'ontologie permet d'articuler les scénarios de risques de manière précise, en les liant aux enjeux métiers. La précision du modèle FAIR permet d'éviter de confondre, comme dans beaucoup de registres de risques, des menaces, des actifs, des conclusions d'audit, des inquiétudes, des contrôles, ... qui sont souvent des composantes du risque mais pas un risque en eux-mêmes. Par ailleurs, en les reliant aux enjeux et processus métiers, on évite de poser des questions qui n'ont pas de réponse ou qui sont trop génériques pour être pertinentes pour l'organisation.

Quantification financière des scénarios de risques

Le standard FAIR se base sur l'utilisation des statistiques et des probabilités pour quantifier certains scenarios. C'est la robustesse de la modélisation de l'ontologie qui permet ainsi d'utiliser ces deux branches des mathématiques que sont les statistiques et les probabilités, qui constituent les sciences de l'aléatoire.

Le standard FAIR



Lorsque cela est nécessaire pour une prise de décision entre plusieurs solutions de sécurité, la quantification se fait grâce à la décomposition en variables de la probabilité d'occurrence d'une part et de l'importance de l'impact, d'autre part.

A chacune de ces variables sont associées des plages de valeurs. Ces plages de valeurs sont obtenues auprès des fonctions IT, infosec et métiers de l'entreprise, ou, lorsqu'elles ne sont pas disponibles (par exemple lors de l'analyse de scenarios de risque pas encore rencontrés), elles peuvent être estimées grâce à des techniques de décomposition et de calibration .

Ces plages de valeurs servent ensuite d'échantillonnage aux simulations Monte-Carlo qui produisent des montants de pertes potentielles et les probabilités associées

FAIR aide ainsi le management à prendre des décisions éclairées en matière de réponse aux cyber risques en leur apportant une meilleure visibilité et compréhension que les autres méthodes. Il permet de répondre aux deux questions que se posent tous les dirigeants, lorsqu'ils doivent prendre une décision :

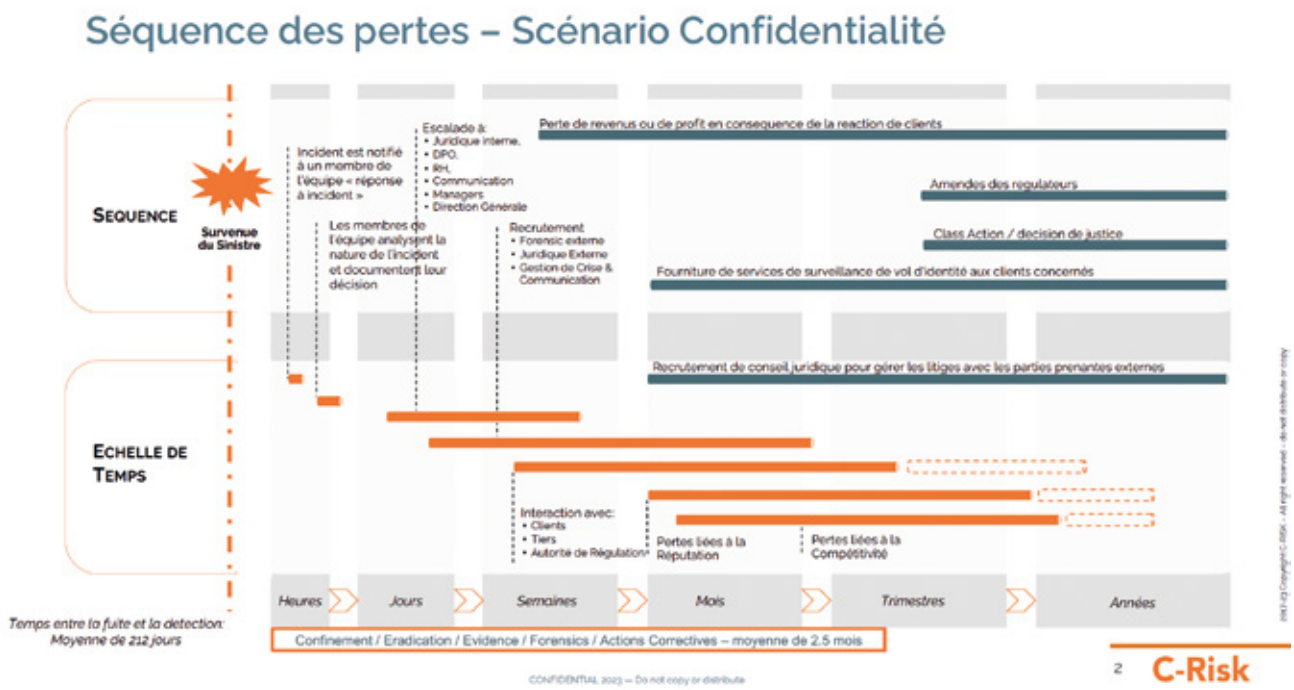
- Combien de fois un sinistre pourrait se produire dans les X prochains mois ?
- S'il se produit, combien coûtera ce sinistre ?

FAIR permet d'obtenir une vision plus globale de la sécurité de l'organisation et de répondre, pratiquement, à des questions de la direction sur des scenarios de risques précis tel que celui de la conformité au RGPD :

- Quel est mon risque global ?
- Quels sont mes risques les plus importants ? sur lesquels de mes actifs ?
- Quels investissements ont permis de réduire mes risques et de combien ?
- Entre deux solutions de mise en œuvre d'un contrôle, laquelle est la plus efficace pour réduire mon risque ?
- Quels sont les risques que l'organisation ne peut assumer et qu'il faut transférer pour être couvert par une assurance cyber ?
- Dans le contrat de cyber assurance qui nous est proposé, quelles sont les clauses d'exclusion qui sont ou non acceptables ?

La sécurisation des systèmes d'information et des actifs digitaux requièrent toujours les gestes d'hygiène cyber de base comme ceux de l'ANSSI ou les 20 contrôles du CIS. Mais prioriser les investissements ne peut plus être du seul ressort des experts de la sécurité. Toutes les fonctions de l'entreprises doivent communiquer entre elles pour articuler les risques cyber en termes métiers quantifiables et ainsi prendre les décisions stratégiques pour se protéger le plus efficacement possible.

Exemple de livrable



Projection vers le futur

Eric AGUILAR
Occitanie
CEO ACSF
Cyber sécurité financière numérique/fintech
Officier de réserve Gendarmerie nationale

L'anticipation des cybermenaces pour les prochaines années constitue l'un des plus gros chantiers menés par nos autorités gouvernementales sous l'égide de l'ANSSI.

Les cyberattaques ont été classées au cinquième rang des risques les plus importants, selon un rapport du World Economic Forum. Cette nouvelle industrie criminelle protéiforme affecte les particuliers, les institutions, les États et surtout notre tissu économique. Elle continue inlassablement de croître en 2023.

Pour les années à venir, selon un ouvrage collectif élaboré et mis en ligne par le Campus Cyber, les défis à relever dans ce domaine à horizon 2030, seront principalement axés :

- sous l'angle de l'ultra-connectivité,
- de l'ultra-cloisonnement,
- de l'ultra-green,
- ou encore de l'ultra-réglementation.

Opportunités et types d'attaques informatiques et défis à relever varient selon les tendances futures auxquelles le monde se confrontera dans les années à venir.

Dans le cas **d'un monde ultra-connecté**, par exemple, les cyberattaquants seront en mesure de cibler un éventail de cibles et d'accès sans précédent et pourront s'appuyer sur la généralisation de plateformes numériques et de réseaux sociaux pour réaliser leurs opérations malveillantes. Il faudra dans ce cas s'attendre à un recours plus large à des réseaux de bots pour lancer des attaques, une instantanéité de propagation de malwares ou encore à la multiplication de services numériques piégés et la diffusion en masse de fausses informations tous secteurs confondus.

Si la tendance **d'un monde hyper-cloisonné** prédomine, l'avenir de la cybercriminalité devrait alors passer par la recrudescence de cyber gangs spécialisés sur des cibles bien déterminées, simplifiant d'autant leur détection. « La proximité entre Etats et cybercriminels permet aux groupes d'être dotés de meilleures capacités offensives tout en bénéficiant d'impunité et de protection dans leur propre espace souverain », prévient le rapport. Dans ce contexte, on devrait alors voir monter en puissance les actions de déstabilisation sur des services critiques nationaux avec la multiplication « d'attentats numériques », le renforcement d'attaques par rançongiciels et complexes de niveau étatique, du cyber-espionnage, voire aussi de la destruction physique de certains câbles sous-marins ou de satellite et sur des chaines d'approvisionnement critiques.

Dans le cas **d'un monde dominé par les enjeux écologiques**, les cyberattaquants s'adaptent aussi bien en monétisant par exemple leurs services à des fins d'hacktivisme visant des systèmes trop énergivores mais aussi en privilégiant les actions de manipulations, d'arnaques nécessitant peu d'exploitation de ressources informatiques élevées rendues à ce stade beaucoup plus compliquées. Dans ce scénario, il faudra alors s'attendre à la prolifération d'attaques contre la réputation des personnes (morales ou physiques), la destruction de systèmes numériques trop énergivores, des attaques contre des chaines d'approvisionnement non locales ou encore l'instrumentalisation des idéologies environnementales à des fins de cyberattaques par rançongiciel, extorsion...

Enfin, dans le cadre d'un f**utur de société hyper-réglementée** « les cyberattaquants profitent de la multiplicité des régulations pour entreprendre du cyber chantage. Ils menacent de dénoncer leurs victimes aux régulateurs pour non-conformité, ou proposent de faux services de régularisation », indique le guide.

« Les investissements humains et financiers portant sur la sécurité sont délaissés au profit de ceux œuvrant uniquement à la mise en conformité réglementaire aux nouvelles exigences, dans une logique parfois idéologique et sans prise en compte des risques réels ». Avec à la clé une explosion de cyber-extorsions, la recrudescence d'attaques usurpant des autorités régulatrices, la montée en puissance de fausses amendes…

Sur cette base de scénarios évolutifs dans notre monde, les défis cyber sécurité à relever peuvent ainsi être adaptés en se focalisant sur **5 priorités communes :**

- sécuriser par défaut tous les systèmes numériques,
- redonner aux individus le contrôle de leur vie numérique et de leurs données,
- s'orienter vers une résilience à grande échelle à base d'automatisation et d'IA,
- combattre l'impunité des cybercriminels,
- développer l'attractivité de la filière cyber sécurité.

Enjeu de souveraineté nationale, la sécurité numérique commence à s'imposer parmi les administrations, entreprises et particuliers. Cependant, l'évolution des cyberattaques et le renforcement induit du contrôle de l'Etat risquent d'atteindre systématiquement nos libertés individuelles à l'horizon 2030.

Audit conseil sécurité financière et patrimoine

Avec la participation d'Eric AGUILAR, CEO ACSFP, expert en sécurité financière, proche collaborateur ayant dirigé comme Officier au sein de plusieurs Sections des recherches en Gendarmerie nationale, des enquêteurs financiers « Fintech », cyber et analystes criminels. Expert en gestion et communication de crise, sa connaissance fine de la cyber et son expérience de terrain seront des atouts précieux pour épauler vos différents services.

- Intervention dans des entreprises victimes de cyber attaque/conseil/gestion de crise,
- Formation et entraînement de dirigeants, DAF, juridiques, équipes opérationnelles, experts-comptables et CAC, avocats, officiers publics, lutte contre les cyber-risques, gestion de crise,
- Expertise croisée, fruit d'une riche expérience de terrain permettant de prévenir les risques, la fraude, le blanchiment et de pérenniser la poursuite d'activité,
- Expert en cryptoactifs, NFT, blanchiment, droit pénal des affaires.
- Expert dans le montage PCA/PRA entreprise pour crise CYBER.

E-mail : aguilar.eric@neuf.fr
Tél : + 33 (0) 6 40 37 51 67