RAPPORT DE SYNTHÈSE

MISSION RÉGIONALE D'EXPLORATION FIC - FORUM INTERNATIONAL DE LA CYBERSECURITÉ

LILLE 5 ET 6 AVRIL 2023

solutions&co
L'agence de développement économique RÉGION PAYS DE LA LOIRE

RÉGION PAYS DE LA LOIRE

LA CYBERSÉCURITÉ
UN ENJEU CRUCIAL

La cybersécurité est devenue un enjeu crucial pour toutes les entreprises, quel que soit leur secteur d'activité. Près d'une entreprise victime d'une attaque sur deux dépose le bilan dans les 18 mois. En effet, les attaques ont pour conséquences de ralentir voire stopper l'activité de l'entreprise (commercial, production, facturation, opérations, trésorerie, etc.) sur des durées allant de quelques jours à plusieurs semaines, voire des mois. En outre, les attaques peuvent nuire à la réputation de l'entreprise et entraîner des conséquences juridiques.

40%

des entreprises (-50 salariés) ont subi une cyberattaque (ou tentative) en France en 2020.

(Source : Enquête Confédération des Petites et Moyennes Entreprises)

4

fois plus d'attaques par rançongiciels entre 2019 et 2020 en France.

(source ANSSI)

+13%

de cyberattaques contre les entreprises publiques et privées entre 2020 et 2021.

(Source : Orange Cyberdéfense)

75 %

des entreprises déclarent que le phishing à été un vecteur d'entrée pour les attaques subies.

(Source ADVENS)

+1 entreprise sur **2** considère toujours que le niveau de menaces en matière de cyber espionnage est élevé.

(source 8e édition du baromètre annuel du CESIN sur la cybersécurité des entreprises françaises, par OpinionWay)

LE FIC EN QUELQUES MOTS
ET CHIFFRES

Le Forum International de la Cybersécurité est un évènement annuel de référence créé en 2007 et consacré à la sécurité et la confiance numérique.

En 2023, le salon organisé par Avisa Partners, Euratechnologies et la Région Hauts-de-France, s'est déroulé à Lille Grand Palais les 5, 6 et 7 avril 2023 :

20 000m²

110
pays représentés

460
partenaires

12 000
participants

Le FIC rassemble de jeunes entreprises innovantes, des grands groupes, des décideurs, des experts de premier plan de l'écosystème et d'autres acteurs liés à la cybersécurité autour de sujets comme la sécurité en entreprise, la lutte anti-cybercriminalité, les nouvelles technologies, les questions de société et les technologies de sécurité. Il s'inscrit dans une démarche de réflexions et d'échanges visant à promouvoir une vision européenne de la cybersécurité et à renforcer la lutte contre la cybercriminalité.
Il est à noter lors de cette édition la non-participation du ministère des Armées et de la DGSE.

« Le Fic n'est pas un salon pour débutants, mais avec un peu de préparation, les conférences techniques se sont avérées très enrichissantes. »

En 2024, le Fic devient le Forum INCYBER.

UNE ACTION PORTÉE
PAR LA RÉGION DES PAYS DE LA LOIRE

La Région des Pays de la Loire a pour objectif d'encourager et de soutenir le développement économique du territoire. Un des enjeux actuels est l'accompagnement du tissu économique vers une montée en compétences en matière de cybersécurité. En 2023, elle organise une mission régionale d'exploration du FIC avec le soutien organisationnel de :

L'agence de développement économique de la Région des Pays de la Loire, au service des entreprises et des territoires.

Premier réseau de professionnels du numérique du Grand Ouest qui œuvre au quotidien pour représenter et développer la filière numérique en Pays de La Loire et en Bretagne.

2 entreprises ligériennes expertes en matière de cybersécurité.

La délégation d'entreprises participantes se compose de 15 personnes de profils type DSI/RSSI et de dirigeants d'entreprises ligériennes de secteurs différents et ayant des niveaux de maturité divers en matière de cybersécurité : certains participants commencent à s'y intéresser, ont déjà subi des cyberattaques, d'autres ont déjà effectué des exercices de gestion de crise et ont déjà participé au FIC.

« Le fait d'être en groupe permet de se comparer à d'autres afin de se situer en matière de cybersécurité, mais également d'en savoir davantage sur l'état de l'art et de partager des bonnes pratiques en toute convivialité. »

Organisation de la délégation en 3 temps

1 - Lancement officiel de la mission : Rencontre et networking, présentation de la délégation et préparation au salon via un exercice de simulation de cyberattaque

« L'exercice de simulation de crise a permis de retenir les éléments importants, à refaire avec les équipes ! »

Cette séquence a été marquée par une expérience immersive proposée par ADVENS destinée à faire vivre une cyberattaque fictive aux participants. Proche des conditions réelles, chacun ayant été affecté à un poste de l'entreprise, cette simulation a permis de mesurer les réflexes et de mettre en avant les bonnes pratiques à adopter en cas d'attaque et de mettre les participants en conditions éclairées avant la visite du salon.

2 - Visite du salon à Lille

La visite du salon alternait visite collective, avec un parcours guidé des rencontres avec des acteurs clés (CESIN, ANSSI et Cybermalveillance), des temps de visite libre, et des propositions de conférences & ateliers à la carte Les entreprises ligériennes présentes sur le salon ont fait l'objet d'échanges particuliers : Advens, Almond, Make it Safe, Orange Cyberdefense, All 4 Tech, Tranquil IT, Nameshield et ESIEA.

« Cette découverte du FIC constitue une bonne opportunité de se familiariser avec les acteurs notamment régionaux de la cyber. »

Deux partenaires avaient également proposé des temps forts à l'occasion du salon, Almond avec un cocktail de networking entre acteurs de l'écosystème régional des Pays de la Loire et Advens avec une visite de son SOC au sein des bureaux lillois.

3 - Réunion de debriefing

Retour d'expérience du salon et atelier collaboratif dans le but de formuler collectivement les propositions présentées plus bas dans ce rapport de synthèse.

Réalisation d'un rapport de synthèse

L'objectif initial de cette mission d'exploration soutenue par la Région des Pays de la Loire est de mieux aborder les grandes tendances, les enjeux, l'écosystème, l'offre de cybersécurité et surtout de partager collectivement cette expérience à l'ensemble des entreprises ligériennes.
Ce cahier de tendances est le fruit de la réflexion des participants à l'issue de cette délégation. Vous y trouverez plutôt des propositions de solutions actionnables à mettre en œuvre à court terme. Elles sont adaptées selon la taille et les moyens des entreprises, pour ainsi lever les freins à la mise en place d'une politique de cybersécurité.

Sommaire

Enjeu 1

SENSIBILISER LES COLLABORATEURS

Enjeu 2

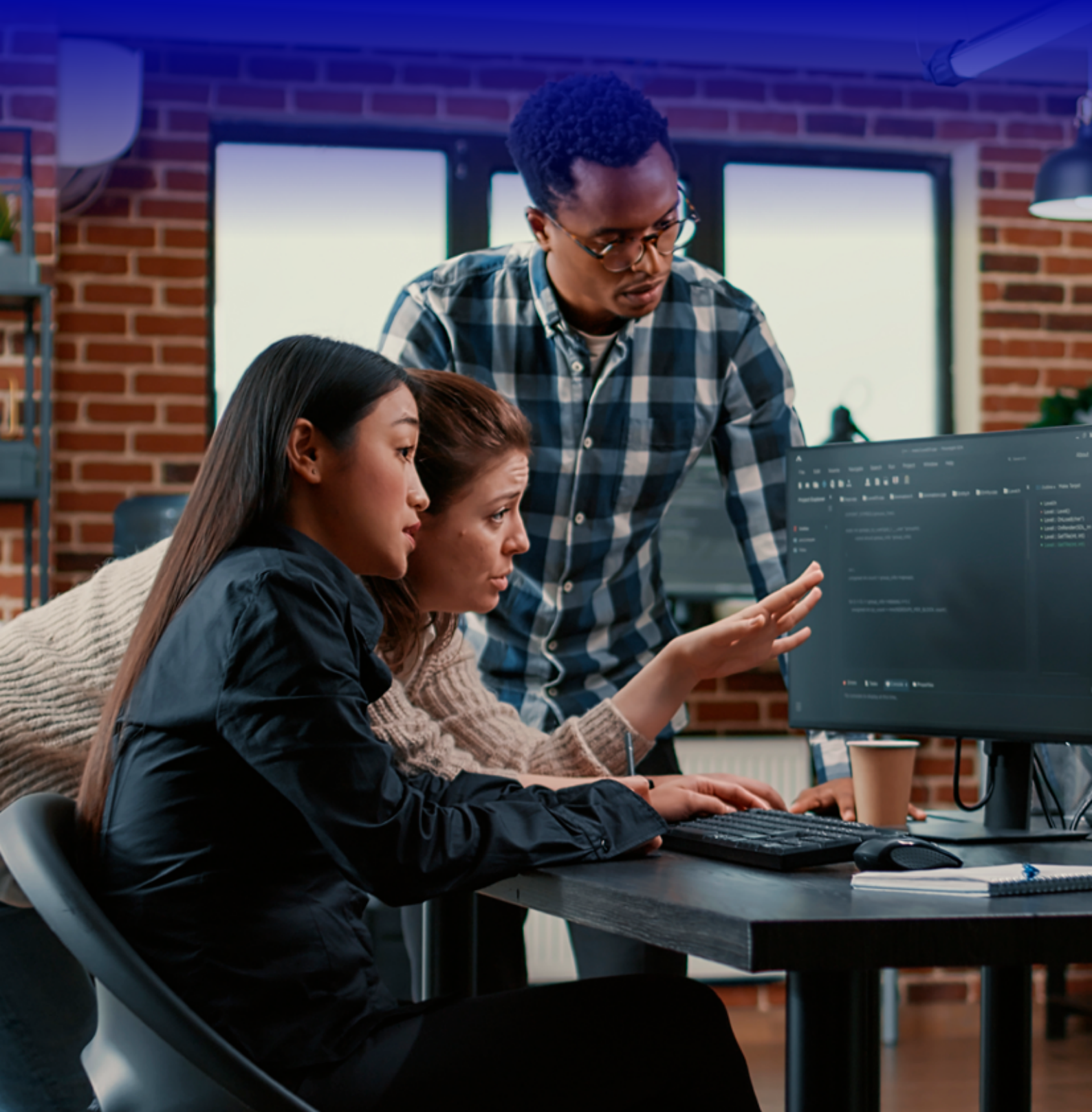
PROTÉGER SON ENTREPRISE DES CYBERATTAQUES

Enjeu 3

SE PRÉPARER ET S'ADAPTER

Enjeu 1

SENSIBILISER LES COLLABORATEURS



1. Engager le dirigeant / la direction

Pour mettre en place une politique efficace de protection contre les cyberattaques, il est essentiel d'avoir le soutien de la Direction afin de disposer des moyens nécessaires et des capacités d'actions.

Cependant les problèmes ci-dessous sont régulièrement observés :

- La conviction que la menace ne concerne pas directement la structure car trop petite, même s'il a été démontré que les petites structures sont des cibles de choix pour les pirates du fait de la faible sécurité de leurs infrastructures, ou simplement parce que l'entreprise n'a jamais été touchée, que ça « n'arrive qu'aux autres »,
- Il peut y avoir un frein à l'investissement dans la cybersécurité par manque de visibilité sur le retour sur investissement,
- Les mesures à prendre pour limiter le risque cyber peuvent être perçues comme trop contraignantes au quotidien pour les salariés, les dirigeants ne préférant pas les inquiéter ni freiner leur productivité.

Cela peut aboutir à la formation d'une barrière entre le Service Informatique (SI) et sa Direction Générale, avec une circulation de l'information qui n'est plus fluide, ou un manque de vision commune.

S'appuyer sur des cas d'attaques avérées dans des organisations comparables peut permettre aux Direction des Systèmes d'Information d'engager et d'impliquer leur Direction. Il est important pour la DSI de présenter à sa Direction le niveau de risque causé par de potentielles cyberattaques, en y ajoutant la probabilité que l'entreprise soit victime d'une cyberattaque dans un avenir proche (entre 1 et 36 mois), en se basant sur des chiffres régulièrement communiqués par des acteurs de référence (ANSSI, etc.).

60 %

des victimes de cyberattaques sont des TPE/PME en 2021.

52 %

des entreprises ont déclaré au moins une cyberattaque

2. Sensibiliser régulièrement et former les collaborateurs aux enjeux de sécurité informatique

L'erreur humaine est la principale source de cyber incidents. Il est donc important de proposer des séances de sensibilisation et/ou formation régulières à tous les collaborateurs afin de maintenir une culture de la sécurité, un niveau de vigilance approprié à l'évolution de la menace, une capacité à détecter les signes d'une attaque et à la signaler immédiatement. En effet, le respect de simples mesures « d'hygiène informatique » de la part des collaborateurs peut réduire drastiquement les risques de cyberattaques.

Cela peut passer par des simulations d'attaques (campagnes de phishing via des outils OpenSource comme Gophish), ateliers pratiques, des formations en ligne ou présentiel, la formation PIX, des conférences, des séances de questions-réponses, voire des formats plus ludiques comme l'escape game ou le serious game.

Les éléments suivants s'opposent souvent aux actions de sensibilisation et mesures à prendre de la part des collaborateurs pour limiter le risque d'attaques :

- Le manque de temps à consacrer à la question, les collaborateurs ayant déjà beaucoup de tâches à effectuer au quotidien. Dans ce cas, il peut donc être souhaitable d'alléger la charge qui pèse sur les employés en supprimant les contrôles inutilement compliqués sans pour autant réduire le risque et adopter des contrôles plus centrés sur l'humain comme l'authentification multi-facteurs ou les contrôles d'accès basés sur les rôles (administrateur réseau, stagiaire...). Cela permet en outre de limiter l'accès aux informations sensibles selon le rôle de l'utilisateur.
- La sensibilisation peut déboussoler les utilisateurs si le vocabulaire est trop technique ou trop complexe. Il est essentiel

de vulgariser au maximum les messages de sensibilisation, d'adapter le discours au niveau des collaborateurs et que les ressources soient clairement accessibles pour toutes les personnes concernées.

- Le sentiment que le risque lié aux Systèmes d'Information ne les concerne pas et que c'est le rôle de la DSI de protéger l'entreprise. A l'inverse certains collaborateurs ont trop confiance en leur propre capacité à détecter les menaces et peuvent ne pas voir l'intérêt de suivre des formations en cybersécurité. Il est dans ce cas utile de leur faire comprendre que même les utilisateurs expérimentés peuvent être piégés,
- La réticence liée à l'obsolescence des logiciels ou au fait d'effectuer une mise à jour qui changerait la manière d'utiliser l'outil et donc les habitudes des collaborateurs, voire de perturber le fonctionnement du système (par exemple la mise à jour d'une machine qui la rendrait indisponible pour plusieurs heures).

Encourager les retours d'expérience en interne

Il est intéressant pour les DSI plus matures de mettre en place des sessions de retour d'expériences pour la Direction Générale afin de partager les problèmes rencontrés dans l'entreprise et d'échanger avec les Directions concernées. Ces sessions permettent d'informer sur les cyberattaques passées et les mesures mises en place pour les contrer. Elles permettent également de sensibiliser la Direction Générale aux risques liés à la sécurité de l'information. Pour détecter tous les problèmes, les collaborateurs doivent se sentir libre de parler des incidents à la Direction sans appréhension.

3. Un contexte qui influe sur le niveau de risques

Le développement du télétravail

Le télétravail est un élément de contexte du monde professionnel qu'il faut prendre en compte pour évaluer les risques dans la mesure où les collaborateurs utilisent désormais plus largement des dispositifs personnels, augmentant ainsi le nombre de points d'accès et de vulnérabilités potentielles que les pirates peuvent exploiter.

Pour gérer au mieux le risque tout en conservant les bénéfices du télétravail pour les collaborateurs, on peut passer par une réorganisation des équipes, une amélioration des processus de validation, une simplification des outils utilisés ou encore une formation des employés à la sécurité informatique. La systématisation du recours au VPN fait partie des bonnes pratiques.

L'émergence du Shadow IT

Le Shadow IT ou l'IT parallèle est un phénomène de plus en plus courant dans les entreprises. Il s'agit de l'utilisation de technologies, de logiciels ou de services sans l'approbation ou la supervision de la Direction des Systèmes d'Information. Le Shadow IT peut se produire lorsque les utilisateurs ont besoin de fonctionnalités spécifiques pour leurs tâches quotidiennes, mais qu'ils ne peuvent pas les obtenir par le biais des canaux officiels de l'entreprise. Ils peuvent alors chercher et utiliser des solutions alternatives de leur propre chef.

Une application Shadow IT peut être parfaitement sécurisée, si l'utilisateur prend les précautions nécessaires, mais c'est rare. Le Shadow IT constitue donc un contexte encore plus favorable pour les cyberattaques, car mis en œuvre le plus souvent en interne par des non-professionnels de l'informatique, sans respect des mesures de sécurité élémentaires.

Ces solutions alternatives, potentiellement non conformes aux politiques de sécurité de l'entreprise, peuvent l'exposer à des risques de sécurité importants. Par exemple, elles peuvent avoir des vulnérabilités de sécurité qui ne sont pas corrigées, ou ne pas être gérées de manière centralisée, ce qui tend à rendre difficile la détection d'incidents ou la mise en place de mesures de sécurité.

Par conséquent, il est important pour les entreprises de mettre en place des politiques claires en matière d'utilisation des technologies et de fournir des solutions alternatives officielles pour répondre aux besoins des utilisateurs. Cela peut également passer par une gestion stricte des droits des utilisateurs sur leur poste de travail en fonction de leur périmètre (téléchargement de logiciels réservé aux admin par exemple). Il est également important de sensibiliser les utilisateurs aux risques de sécurité liés au Shadow IT et de les encourager à signaler toute utilisation de technologies non approuvées à la Direction des Systèmes d'Information.

4. Les menaces principales

Le phishing

Le phishing (ou « hameçonnage ») est une technique destinée à tromper l'internaute en lui envoyant un mail pour l'inciter à communiquer des données personnelles en se faisant passer pour un tiers de confiance (banque, administration...). Les signaux d'alerte sont :

- **une adresse d'expédition suspecte,**
- **un objet de mail trop alléchant ou alarmiste** (« remboursement » ou « alerte de sécurité » par exemple),
- **une demande inhabituelle** ou d'informations confidentielles...

Le rançonnage

On parle de « ransomware » et de « rançongiciels ». Le cybercriminel met un logiciel dans l'ordinateur ou le système d'information de sa victime pour crypter ses données via une pièce-jointe ou un lien de téléchargement. Il menace de les rendre inutilisables ou publiques si une rançon n'est pas payée.

Autres formes d'ingénierie sociale

Le plus souvent les cyberattaques proviennent d'une faille dont l'origine est un salarié, en ligne ou même en physique : des personnes mal intentionnées pénètrent dans l'enceinte du bâtiment, se connectent à un appareil et récupèrent des données. Il faut évidemment faire preuve de vigilance vis-à-vis des visiteurs ou intervenants se présentant dans la structure sans rendez-vous ou sans avoir été annoncés.

Un autre exemple d'ingénierie sociale en ligne est « l'arnaque au président » : un salarié est contacté par une personne mal intentionnée se faisant passer pour le Président de sa structure ou une personne haut placée. Celle-ci joue de son autorité (supposée) et de l'urgence de la situation pour abuser le salarié, qui panique ou n'ose pas refuser une demande de sa hiérarchie et met en danger l'entreprise en activant des process ou révélant des codes.

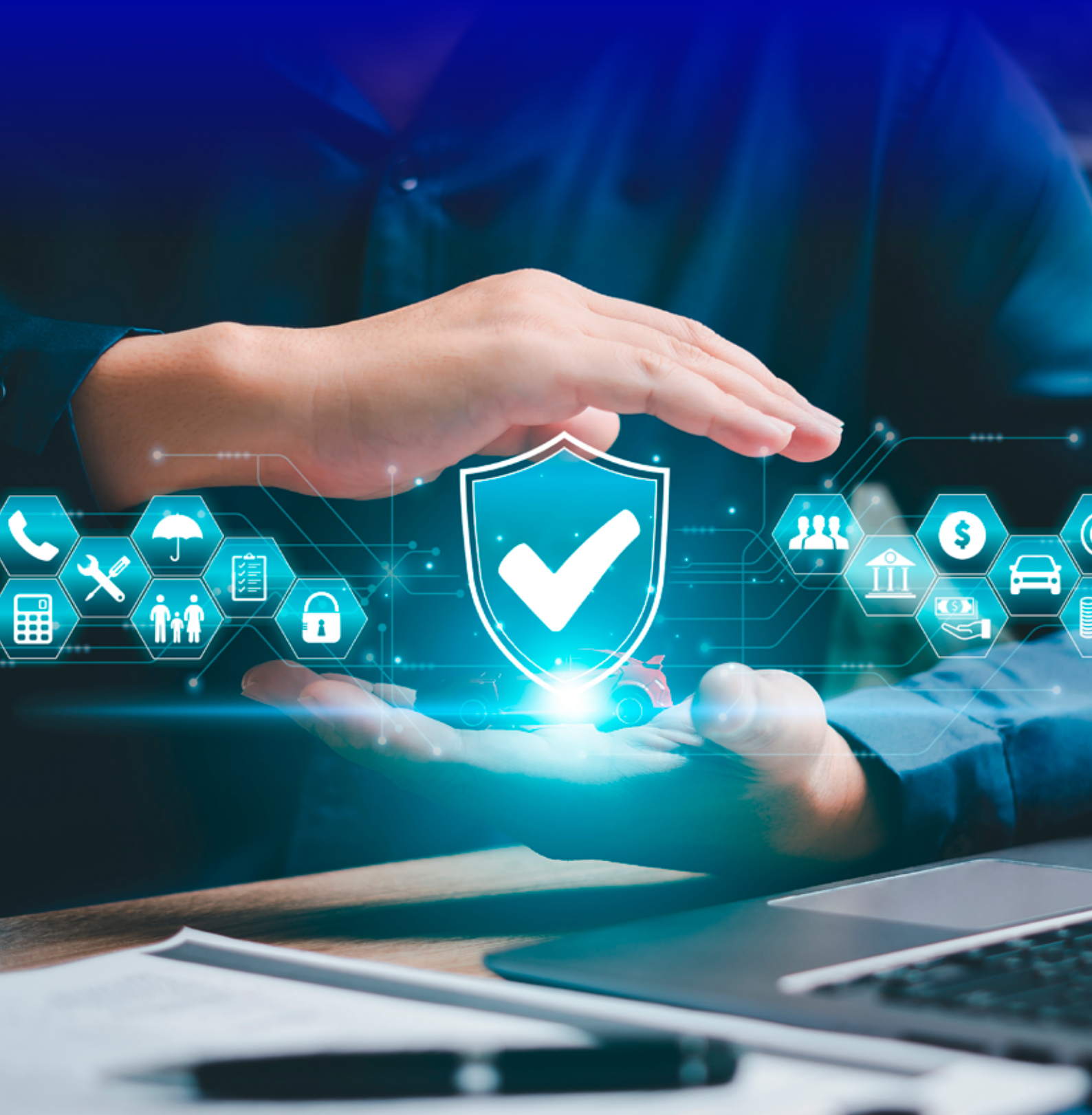
5. Les exercices de simulation d'attaque, un état des lieux du risque

Il est recommandé de réaliser des simulations d'attaque pour tester la capacité de l'entreprise à détecter et à répondre à une intrusion. Cela permet d'identifier les failles du système de sécurité et de mettre en place rapidement des actions correctives. Cette simulation peut prendre la forme d'une tentative de phishing (ou « hameçonnage »), d'une intrusion dans les systèmes internes ou encore d'une tentative d'accès aux informations sensibles.

L'analyse des résultats permettra à l'entreprise de mieux se préparer à une attaque réelle, de mettre en place un plan de sécurisation et de fournir des statistiques sur l'évolution du niveau de vigilance des collaborateurs.

Enjeu 2

PROTÉGER SON ENTREPRISE DES CYBERATTAQUES



1. Première étape : le diagnostic

Pour que toutes les parties soient impliquées, il faut trouver un juste équilibre entre ressources allouées, actions mises en place et niveau de risque réel à l'échelle de l'entreprise et au regard de l'évolution de la menace.

Il est indispensable pour toute entreprise de réaliser une analyse de l'ensemble des pratiques de sécurité mises en place dans l'entreprise, afin de déterminer les forces et faiblesses du système et les améliorations à apporter.

Ce diagnostic permet de dresser un état des lieux des politiques, procédures et outils de sécurité utilisés.

Il commence par l'identification des actifs qui consiste à lister les ressources informatiques (matériel, logiciel, données) de l'organisation et les classer par ordre de priorité selon leur niveau de risque, leur impact sur l'organisation et la facilité à exploiter les vulnérabilités.

Puis on identifie les menaces pesant sur ces actifs : il peut s'agir de menaces internes liées aux processus, aux systèmes, aux applications, aux réseaux... ou externes : virus, malwares, hacking... Enfin on évalue le niveau de risque associé à chaque menace de manière quantitative ou qualitative.

2. Prioriser, mettre en place et suivre les actions des lieux du risque

Les étapes de diagnostic et sensibilisation doivent être suivies d'actions permettant à chaque organisation d'atteindre le niveau de sécurité minimum. Cela nécessite de prévoir un budget dédié aux solutions actionnables à l'issue du diagnostic.

Un plan d'action inclut des mesures de correction immédiates et des mesures préventives à long terme. Il est nécessaire de mettre en place un suivi régulier du SI pour évaluer l'efficacité des mesures de correction mises en place et s'assurer que la sécurité reste optimale.

La méthode KANBAN est une méthode classique de gestion de projet qui est tout à fait adaptée aux sujets cyber. Cet outil en 4 étapes est intéressant car il permet de prioriser les actions à mettre en place en fonction de leur impact sur la sécurité de l'entreprise :

- **Identifier** les tâches à réaliser : mise en place d'un pare-feu, la sauvegarde régulière des données, la mise à jour des logiciels, etc.
- **Prioriser** les tâches en fonction de leur impact sur la sécurité de l'entreprise (par exemple, la mise en place d'un pare-feu peut avoir un impact plus important que la mise à jour des logiciels).
- **Faire apparaitre** les tâches sur un tableau KANBAN afin de suivre leur avancement et leur réalisation.
- **Affecter** les tâches à des membres de l'équipe : chaque tâche doit être attribuée à une personne responsable de sa réalisation.

Réviser le tableau KANBAN régulièrement permet de s'assurer que les actions sont réalisées dans les délais prévus et de faire des ajustements si nécessaire.

L'audit des systèmes d'information

Les audits permettent de vérifier le niveau de sécurité des mesures et si elles sont conformes aux exigences réglementaires du RGPD. Ils permettent de lancer une réflexion sur son propre niveau de protection. L'audit doit constituer une partie minoritaire du budget alloué à la cybersécurité. Il est recommandé de réaliser le contre audit avec le même prestataire afin de mieux retracer l'évolution du SI, mais de changer d'auditeur régulièrement afin d'apporter un regard neuf sur le travail effectué. L'audit est davantage conseillé pour les structures ayant une maturité cyber avancée car il permet d'analyser les mesures déjà mises en œuvre et demande un budget plus conséquent.

Il existe d'autre référentiels comme l'ISO 27002, norme internationale sur la sécurité de l'information, qui permet de certifier un certain niveau de protection.

3. Des mesures d'hygiène fondamentales

Les mesures d'hygiène constituent les mesures de base pour réduire le risque d'attaque. On peut également les compléter par la gestion des accès aux informations sensibles et l'installation d'outils types antivirus et de pare-feu.

Gestionnaire de mots de passe

La complexité des procédures de gestion des mots de passe fait partie des mesures mal acceptées en interne. Il est essentiel de donner des astuces pour créer et gérer les mots de passe efficacement. Il est possible d'utiliser un gestionnaire de mots de passe comme Keypass, qui est open source et permet de stocker de manière sécurisée des informations d'authentification (identifiants et mots de passe).

Il est également possible d'utiliser l'authentification multi-facteurs qui ajoute une couche de sécurité supplémentaire aux comptes en demandant une deuxième forme d'identification après la saisie du mot de passe (code généré par une application, code envoyé par sms, empreinte digitale...) pour réduire considérablement le risque de piratage.

Mise à jour régulières

Pour se protéger, il est important de mettre à jour régulièrement les logiciels métier afin de corriger les vulnérabilités connues et donc d'empêcher les cybercriminels d'exploiter les failles du système informatique.

Sauvegardes régulières et déconnectées.

Il est impératif de mettre en place des sauvegardes régulières de toutes les données importantes de l'organisation afin de minimiser l'impact d'une attaque. Ces sauvegardes doivent être stockées dans un endroit sécurisé et isolé du réseau informatique principal, pour éviter que les données sensibles soient corrompues ou perdues en cas d'attaque. Il faut vérifier l'intégrité de ces sauvegardes et capacité des équipes à les restaurer en cas de besoin (on peut mettre en place une simulation de restauration complète du système informatique par exemple).

4. Deuxième niveau de mesures de protection interne et externes des lieux du risque

Une fois les mesures de base effectuées, il est important de mettre en place des mesures de protection complémentaires :

- **Segmenter** le réseau pour limiter les dommages potentiels
- **Installer** des outils de surveillance pour détecter les activités suspectes sur les terminaux et dans le SI (EDR, XDR)
- **Vérifier** le risque et exiger la mise à niveau des parties prenantes (en demandant les éléments de preuve) en lien avec l'organisation (fournisseurs SAAS, hébergeurs, sous-traitants). Actuellement, il n'y a pas d'obligation de transparence du sous-traitant. Il existe un guide complet de la CNIL (https://www.cnil.fr/fr/securite-gerer-la-sous-traitance) permettant de jauger le niveau de garanties offert par le sous-traitant.

Le recours au SOC, service managé des alertes

La multitude des outils et des informations peut constituer un frein à la réaction contre les cyberattaques. En effet, il peut être difficile de tout surveiller et de repérer rapidement les signes d'une attaque, d'autant plus si les équipes de sécurité informatique sont déjà débordées. Selon la situation et les risques cyber de l'entreprise, le suivi des indicateurs cyber peut représenter un travail important, qui, s'il ne peut être réalisé en interne, nécessite une externalisation.

Les organisations ayant un niveau d'exposition au risque cyber élevé et des moyens financiers importants peuvent recourir à un service de gestion managé des alertes, Security Operations Center (SOC), qui sera suivi 24/7. Cela permet de détecter rapidement toute activité suspecte sur le réseau de l'entreprise et de pouvoir réagir rapidement. Les équipes en charge du SOC doivent travailler en étroite collaboration avec les équipes informatiques internes de l'entreprise.

5. Faire monter la DSI en compétences

Développer une équipe dédiée, en fonction des besoins, des risques ou de la menace. Lancer des actions de formation pour adapter les compétences des équipes existantes.

Formation des équipes IT

Il est nécessaire que les équipes IT effectuent une veille régulière afin d'être informées des nouvelles techniques de protection, détection et de l'évolution de la menace. Il existe des formations soutenues par l'ANSII comme Cyberedu, le label SecNumedu, ou le MOOC SecNumacadémie. La plateforme de formation et d'évaluation PIX permet de certifier ses connaissances numériques. Il est possible de se tenir informé de nouvelles menaces via une rubrique dédiée sur le site cybermalveillance.

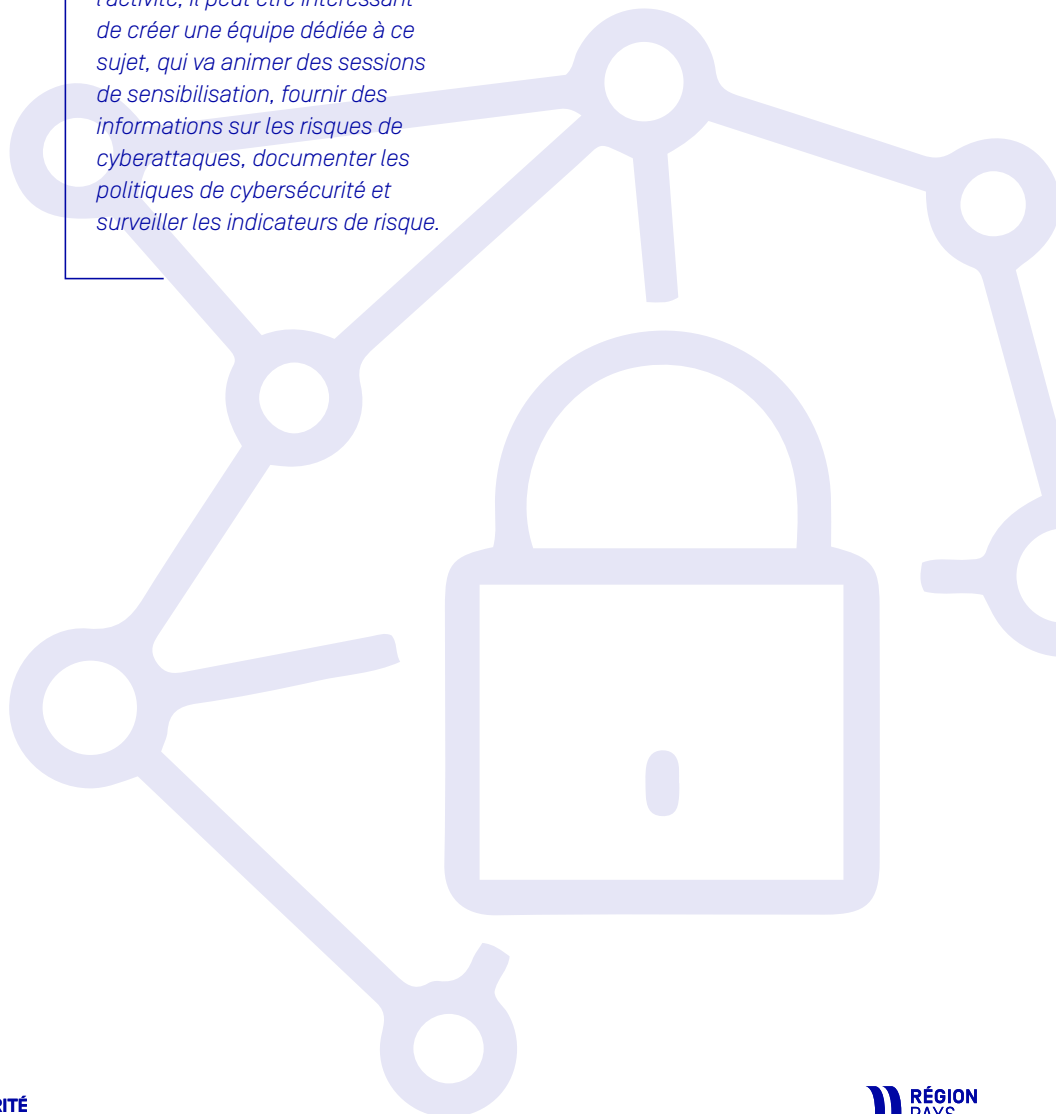
Il peut être intéressant de sonder les compétences et les ressources disponibles en interne, notamment s'il y a beaucoup de turnover ou que la compétence clé est détenue par une seule personne. Du fait de la difficulté actuelle de recruter en cybersécurité, il est intéressant de former les collaborateurs qui souhaiteraient monter en compétence (il existe notamment des formations finançables via le CPF).

Créer une équipe cyber dédiée

Si la sécurité informatique est un sujet clé pour la pérennité de l'activité, il peut être intéressant de créer une équipe dédiée à ce sujet, qui va animer des sessions de sensibilisation, fournir des informations sur les risques de cyberattaques, documenter les politiques de cybersécurité et surveiller les indicateurs de risque.

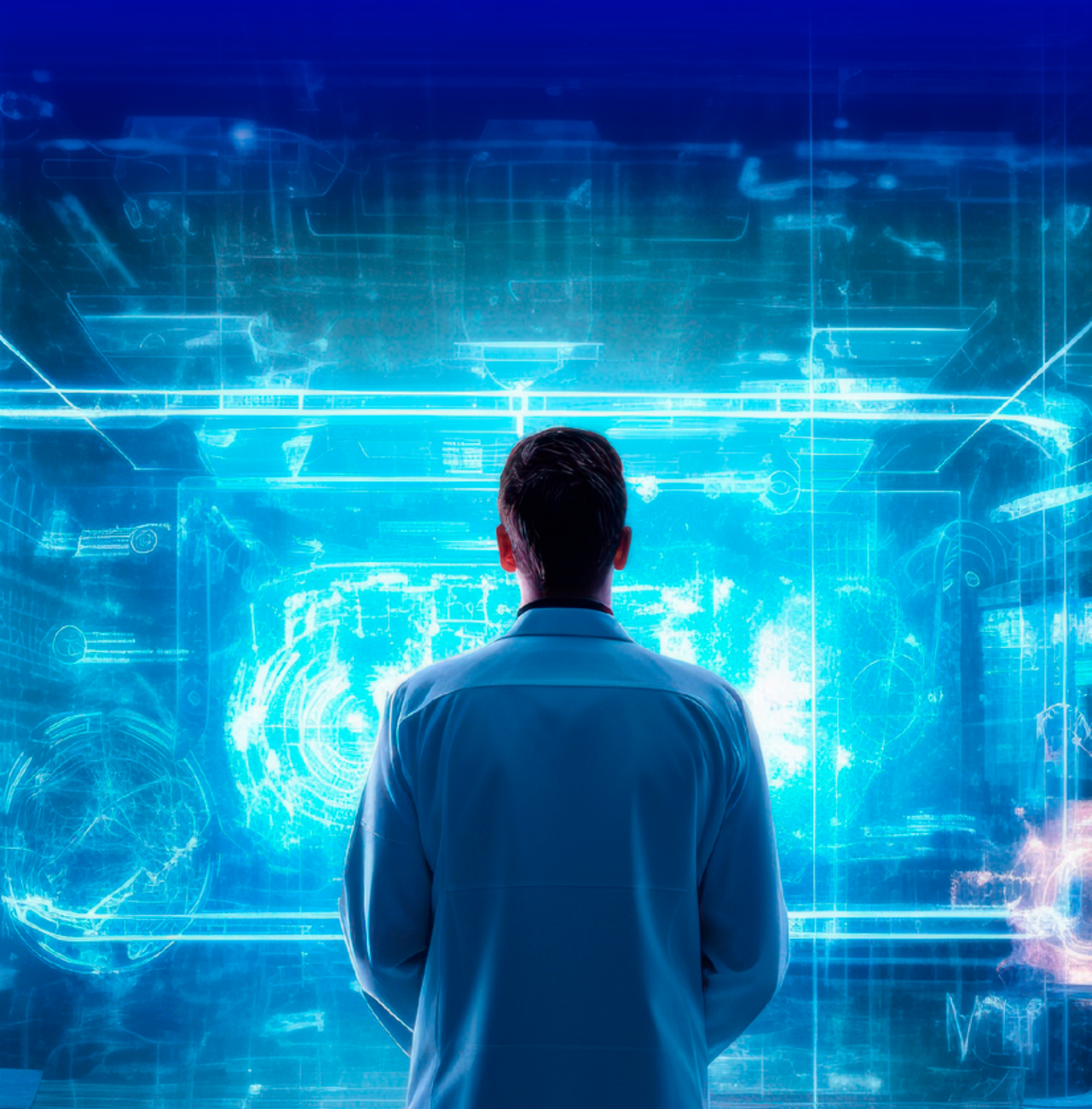
Méthode ITIL

Une autre solution, adaptée notamment aux entreprises ayant déjà une DSI structurée, consiste à réorganiser le service IT selon la méthode ITIL (Information Technology Infrastructure Library) : c'est une approche standardisée pour la gestion des services IT qui permet d'en optimiser l'efficacité opérationnelle. Avec cette méthode, il est possible de mettre en place des processus de gestion des risques et des incidents, ainsi que de maintenir une documentation complète pour la gestion des changements.



Enjeu 3

SE PRÉPARER ET S'ADAPTER



Malgré toutes les précautions prises, le risque d'attaque subsiste. Il est essentiel d'avoir une stratégie claire et efficace pour minimiser les pertes, réduire les impacts et se préparer à être attaqué. Cela permet de ne pas céder à la panique lorsque l'attaque survient et limiter les conséquences négatives. En cas de cyberattaque, ne pas oublier de tenir un registre des évènements et actions réalisées (main courante) pour pouvoir en conserver la trace à disposition des enquêteurs et tirer les enseignements de l'incident a posteriori.

1. Plans de Continuité (PCA) et Reprise d'activité (PRA)

Ils permettent de garantir la continuité et la reprise des activités en cas d'incident majeur et d'avoir des réflexes pour réagir en cas d'attaque, sans céder à la panique. Il s'agit d'un ensemble de procédures destinées à mettre en place une infrastructure informatique de secours puis assurer la reprise des activités de l'entreprise suite à un arrêt ponctuel du système d'information.

Le PCA a pour but d'éviter l'arrêt complet de l'activité. Il est construit de façon à garantir la disponibilité des structures informatiques de l'entreprise, que ce soient les réseaux, les serveurs ou les datacenters.

Tandis que le PCA a une fonction préventive pour réduire autant que possible la survenue d'une situation critique, le PRA intervient a posteriori, pour reconstruire un système d'information (SI) à partir de données répliquées. Il indique comment redémarrer les applications, et précise le système de sauvegarde à enclencher pour assurer la sécurité des données confidentielles. Le PRA contient également :

- **Le seuil tolérable du délai d'interruption,** appelé aussi RTO (Recovery Time Objective). Il s'agit de la durée maximale d'interruption que l'entreprise peut supporter avant que la situation ne soit critique.
- **Le seuil tolérable de la perte de données,** ou RPO (Recovery Point Objective). Il s'agit de la perte de données maximale admissible par l'entreprise.

2. La gestion de crise à tous les niveaux

Une attaque met en difficulté l'entreprise dès les premières minutes, causant un stress qui peut être intense. Tout comme le PCA, l'entreprise doit pouvoir mettre en place une cellule de gestion de crise qui sera opérante à tous niveaux en cas d'attaque, afin de maximiser ses chances d'appliquer les bonnes méthodes et d'avoir les bons réflexes. Les membres de cette équipe n'ont pas forcément un profil technique mais sont recrutés en fonction de leurs qualités humaines, comme la résistance au stress. Cette cellule aura alors pour mission de prévoir et mettre en œuvre :

- **des rôles et responsabilités** en interne et des back-ups
- **une organisation idéale** en cas d'attaque, (des cellules décisionnelles et opérationnelles par exemple)
- **des processus clairs et concis** à appliquer en fonction du déroulement des évènements (ressources à contacter, questions à se poser, actions à mettre en place, etc), à archiver de manière concise et facilement accessible.
- **la préparation des équipes de sécurité informatique** à répondre rapidement aux incidents de sécurité et à travailler de manière coordonnée pour limiter les impacts de l'attaque. Cela passe par la réalisation de tests pour évaluer les risques et les impacts potentiels des attaques. A noter qu'il peut être difficile de mobiliser les référents métier pour valider ces tests du fait du manque de temps notamment.
- **déclarer l'incident**
  En cas de fuite de données personnelles, notifier la CNIL dans les 72 h, et si besoin les services bancaires et financier de l'entreprise et Cybermalveillance.

  En cas de cyberattaque, il est possible de contacter un numéro d'urgence CERT (centre d'alerte et de réaction aux attaques informatiques) qui va établir une base de données des vulnérabilités, analyser les symptômes de l'attaque, diffuser des informations sur les précautions à prendre pour minimiser les conséquences de l'attaque.
- **bien communiquer pendant et après l'attaque**
  Avec la recrudescence des attaques, il est de plus en plus difficile de cacher les intrusions et cyberattaques. Les risques en termes d'image et de réputation peuvent être assez important pour les entreprises, notamment si l'affaire est médiatisée sans communication adéquate. Il est donc nécessaire d'associer les collaborateurs en charge de la communication et/ou des relations publiques à la cellule de crise, afin d'accompagner les différents développements des messages appropriés.

Il faut aussi encourager la DSI à communiquer en interne, sur le fait qu'elle ne soit pas imperméable, qu'il y a eu tel type d'attaque à quel moment... afin de repérer les failles et pouvoir les corriger.

Attention dans ce cadre à prendre en compte également les risques psychosociaux, et de prêter une attention particulière à la communication mise en œuvre (forme, cible, messages...). Une cyberattaque peut engendrer une surcharge exceptionnelle d'activité et un sentiment de sidération, d'humiliation, d'incompétence, voire de culpabilité, susceptible de peser sur les collaborateurs et de mettre à mal leur efficacité.

Cyber assurances

Certaines assurances disposent d'un SLA (Service Level Agreement). Ce type de contrat définit les termes précis et le niveau de service qu'est en droit d'attendre l'entreprise. Il permet de :

- ***réagir rapidement** en cas de cyberattaque,*
- ***contacter des experts** en sécurité informatique qui pourront aider à gérer la situation,*
- ***garantir certains niveaux de sécurité** dans le stockage et la gestion des données à caractère personnel.*

Ces souscriptions sont de plus en plus souvent conditionnées à un niveau minimum de sécurité au sein de l'entreprise (réalisation d'un diagnostic, mise en place de process de sécurisation, ...).

La souscription à une cyber assurance peut fournir une couverture financière en cas de dommages causés par une cyberattaque, tels que la perte de données, la responsabilité civile et les coûts de notification des atteintes à la protection des données. Il est important de bien comprendre les termes et les conditions de la cyber assurance, son périmètre, ainsi que de maintenir un contact régulier avec l'assureur pour s'assurer que les niveaux de couverture sont appropriés et adaptés à l'entreprise. Cette solution peut toutefois s'avérer onéreuse c'est pourquoi il est nécessaire de comparer besoins de sécurité, risques encourus et dégâts potentiels qu'une attaque pourrait causer.

L'assurance ne doit pas être une finalité. Il est nécessaire de trouver les moyens d'éviter les attaques et d'établir un plan de réaction afin de limiter les impacts en cas d'attaque.

3. Tirer les conséquences de l'attaque

A la suite d'une cyberattaque, il peut être pertinent d'adapter les process de l'entreprise, au regard de l'expérience.

Il est intéressant de se référer à la main courante tenue lors de la gestion de la crise et de faire un retour d'expérience avec les collaborateurs concernés pour restructurer l'organisation si besoin. Une analyse de la crise a postériori permettra de renforcer la sécurité des systèmes d'information. Cela peut inclure la mise en place de nouvelles politiques de sécurité, la révision des processus de gestion des incidents, la formation du personnel et la mise en œuvre de mesures de sécurité supplémentaires pour prévenir de futures cyberattaques

Ce qu'il faut retenir

La cybersécurité concerne tout le monde, peu importe la taille ou le type de structure, mais toutes les entités n'ont pas les mêmes priorités et enjeux. Il y a un arbitrage à faire entre les actifs qu'il est primordial de protéger, le budget que l'on est prêt à consacrer et les dégâts qu'une attaque pourrait engendrer.

1. En matière de cybersécurité et afin de concerner toute l'organisation, l'impulsion vient de la Direction Générale, qui doit être engagée et allouer les ressources nécessaires.
2. Il faut établir un diagnostic listant les actifs, leur niveau de protection, leurs vulnérabilités et leur niveau de criticité (impact en cas d'attaque) afin d'allouer efficacement les ressources disponibles.
3. Les mesures d'hygiène constituent la base de la protection contre les cyberattaques mais elles ne sont efficaces que si l'ensemble de la structure s'y conforme.
4. Pour maintenir et améliorer le niveau de connaissances cyber dans toute la structure on organise régulièrement des formations pour informer des nouvelles menaces et des campagnes de phishing tests, avec des retours d'expérience pour vérifier la vigilance des collaborateurs.
5. Il faut mettre en place un plan d'action de sécurisation pour assurer la continuité d'activité et ne pas être pris au dépourvu en cas d'attaque, qui contient des mesures pour réagir en cas d'attaque et de mesures à long terme.
6. Choisir son prestataire peut s'avérer compliqué, il faut comparer les offres et avoir établi un diagnostic détaillé pour comprendre ses besoins de cybersécurité.
   De nombreuses ressources sont mises à disposition des entreprises comme la plateforme nationale Cybermalveillance. Elle intègre un annuaire de professionnels référencés.
7. Il peut être intéressant de mutualiser les connaissances et ressources entre structures.

Annexes

RESSOURCES DISPONIBLES EN PAYS DE LA LOIRE EN MATIÈRE DE CYBERSÉCURITÉ :

Il existe des ressources gratuites en ligne, ce qui les rend facilement accessibles pour toutes les entreprises, quelle que soit leur taille ou leur niveau de maturité en matière de cybersécurité.

Institutionnelles

Guides de l'Agence nationale de la sécurité des systèmes d'information (ANSSI)

Des outils complets sur la sécurité informatique à destination des petites et moyennes entreprises. Permet de sensibiliser les employés aux bonnes pratiques de sécurité et donne des recommandations pour la gestion des incidents.

Cybermalveillance.gouv.fr

Une plateforme gouvernementale qui accompagner particuliers, entreprises et collectivités dans la prévention et la gestion des cyberattaques. Assistance en ligne gratuite en cas d'incident de sécurité.

Quelques acteurs de la cybersécurité présents en Pays de la Loire

Advens fournit un service de cybersécurité sur-mesure, peu importe la taille de votre organisation via une expertise 360° et une approche SaaS.

All4Tec, leader Français de l'outillage EBIOS (labellisé par l'ANSSI) et ISO 27005, propose 2 outils permettant d'analyser et manager les risques cyber.

Almond est un expert cybersécurité, cloud et infra qui permet de sécuriser les systèmes d'information.

ArcData Shield développe et commercialise des passerelles réseaux via un boitier électronique. Cela apporte aux entreprises et organisations une sécurité de leurs actifs matériels et immatériels contre les cyberattaques.

Digitemis est une solution complète pour se mettre en conformité vis-à-vis de l'ensemble des référentiels, et de le rester notamment grâce à une équipe d'experts cyber et de juristes. Make it Safe, Business Unit de Digitemis, édite un logiciel de cybersécurité et de conformité.

Nameshield, 1er bureau d'enregistrement certifié ISO 27001, est un acteur de la sécurisation de noms de domaines et services associés

Orange Cyberdefense acteur important de la cybersécurité, quel que soit le niveau de maturité, il couvre tous les aspects : anticipation, détection des menaces, protection et réaction. Une offre supplémentaire de protection des données et des équipements nouvelle génération pour les professionnels.

TranquilIT audite les infrastructures et propose une solution permettant de contrôler et d'administrer son parc informatique.

Comparer les prestataires

Les entreprises sans DSI peuvent manquer de ressources et d'expertise en matière de sécurité informatique, notamment pour choisir les bons prestataires offrant des services tels que l'analyse des vulnérabilités, la gestion des incidents de sécurité et la formation des employés :

- *difficultés à savoir quelles questions poser aux prestataires potentiels,*
- *difficultés à évaluer leur expertise ou leurs compétences au regard du besoin.*

Le fait d'avoir réalisé un diagnostic préalable permet de préciser les besoins de la structure.

D'autre part, il peut être intéressant pour les entreprises n'ayant pas de DSI structurée de se regrouper avec d'autres entreprises pour mutualiser les connaissances, les ressources en matière de cybersécurité et plus largement partager sur leurs besoins. Les groupes peuvent également partager des informations sur les menaces et les tactiques utilisées par les attaquants, ainsi que des solutions pour améliorer la sécurité des systèmes. Cela permet enfin de mieux savoir où l'on se situe par rapport à l'état de l'art, voire de se comparer directement avec des structures de taille similaire.

VOTRE CONTACT SOLUTIONS&CO :

Christophe GUILLAUME
c.guillaume@solutions-eco.fr

MISE EN ŒUVRE PAR :

adn ouest

solutions&co
L'agence de développement économique
RÉGION PAYS DE LA LOIRE

UNE DÉMARCHE SOUTENUE PAR :

RÉGION PAYS DE LA LOIRE