bpifrance
SERVIR L'AVENIR

CYBER MALVEILLANCE .GOUV.FR
Assistance et prévention en sécurité numérique

GUIDE CYBERSÉCURITÉ

À DESTINATION DES DIRIGEANTS DE TPE, PME ET ETI

BONNES PRATIQUES
ET RÉFLEXES À ADOPTER
EN CAS DE CYBERATTAQUES

PASSEZ
À L'ACTION

À travers ce guide, vous découvrirez les bonnes pratiques à adopter pour vous prémunir du risque cyber et les réflexes à adopter en cas de cyberattaques.

ÉDITO

La numérisation est un vecteur de croissance et de compétitivité pour les PME et ETI françaises. Les progrès technologiques, les changements de comportements et la diversité des services à disposition des entreprises contribuent à l'essor de la numérisation des entreprises. Les systèmes sont de plus en plus connectés et interdépendants.

Ces flux d'information quotidiens devenus indispensables exposent les entreprises à des cyberattaques. Force est de constater que la maturité de l'écosystème entrepreneurial français reste perfectible en matière de cybersécurité alors que les conséquences d'une cyberattaque peuvent s'avérer dramatiques.

Pour s'en prémunir, une prise de conscience collective est indispensable car les systèmes d'information des entreprises sont interconnectés avec leurs clients, fournisseurs, etc.

La prise en considération du risque cyber est souvent moins complexe qu'on ne le pense et des gestes simples de cyber-hygiène permettent de réduire considérablement les risques. Lorsqu'ils sont sensibilisés, les collaborateurs sont les premiers remparts face aux cyberattaques.

Jérôme Notin,
Directeur général de Cybermalveillance.gouv.fr

Pascal Lagarde,
Directeur exécutif en charge de l'International, de la Stratégie, des Études et du Développement de Bpifrance

PRÉSENTATION DU DISPOSITIF D'ASSISTANCE AUX VICTIMES DE CYBER-CRIMINALITÉ APPORTÉ PAR L'ÉTAT

Cybermalveillance.gouv.fr est la plateforme du dispositif national d'assistance aux victimes et de prévention des risques numériques.

Créé en 2017, ce dispositif est la réponse apportée par l'État pour informer et accompagner les victimes de cybermalveillance face à une cybercriminalité en forte croissance avec la démocratisation des usages numériques.

La plateforme Cybermalveillance.gouv.fr est pilotée et animée par un Groupement d'Intérêt Public (GIP), le GIP Acyma, qui regroupe plus d'une cinquantaine d'acteurs publics (ministères, secrétariats d'État, agences gouvernementales...) et d'acteurs privés (associations de consommateurs ou d'aide aux victimes, organisation et syndicats professionnels, opérateurs, éditeurs, assureurs, banques…) engagés ensemble dans la lutte contre la cybermalveillance.

Les services offerts par Cybermalveillance.gouv.fr s'adressent à toutes les catégories de publics (particuliers, associations, collectivités, administrations, entreprises) et plus spécifiquement aux moins aguerris d'entre eux qui sont souvent les plus susceptibles d'être victimes de la cybercriminalité ou d'avoir le plus de difficultés à faire face à une cyberattaque.

CYBER MALVEILLANCE .GOUV.FR

Assistance et prévention en sécurité numérique

Les services de Cybermalveillance.gouv.fr sont gratuits et organisés sur la base des missions confiées au dispositif :

L'observation de la menace,

qui repose sur un travail important de veille sur les modes opératoires de la cybercriminalité et la victimologie afin d'alimenter les différents acteurs impliqués et de produire des alertes ainsi que des contenus de sensibilisation adaptés aux différentes situations rencontrées par les victimes.

La prévention des risques numériques,

par la production de nombreux contenus pédagogiques et illustrés sur les bonnes pratiques de la sécurité numérique, ainsi que sur les principales cybermenaces et les moyens de s'en prémunir. Ces contenus sont directement et gratuitement accessibles sur la plateforme sous forme d'articles, de fiches, de mémos, d'infographies, de vidéos et même de kits de sensibilisation.

L'assistance aux victimes,

dispensée en ligne au travers de la plateforme, qui leur permet de diagnostiquer le problème qu'elles rencontrent, de recevoir les conseils adaptés pour y faire face et d'être orientées au besoin vers les services compétents pour les aider. La plateforme leur permet même d'être mises en relation avec plus de 1 000 prestataires spécialisés de proximité référencés et en mesure d'intervenir localement pour apporter leur appui.

Enjeu de société majeur, la sécurité numérique est l'affaire de tous et Cybermalveillance.gouv.fr est le premier réflexe sécurité que les citoyens, les entreprises et les collectivités connectés doivent développer pour apprendre à faire face aux risques.

AU SOMMAIRE

CYBER-SÉCURITÉ...

01.

... QUELS ENJEUX POUR LES TPE, PME ET ETI ?

Les PME et ETI sont ciblées par des cyberattaques mais restent très peu protégées.

L'ESSOR DE LA TRANSFORMATION NUMÉRIQUE

Depuis les années 2000, toutes les entreprises connaissent une transformation numérique de leur organisation et de leur mode de production.

En 2020, la crise sanitaire liée à l'épidémie de la Covid-19 a donné un élan supplémentaire à cette transformation à travers la digitalisation de nombreux processus et le recours massif au télétravail.

À l'avenir, ce mouvement continuera à prendre de l'ampleur sur tous les pans de l'économie, porté notamment par le développement de l'Internet des objets, du *Cloud Computing* [1] et du nomadisme qui ouvrent la voie à de nouveaux usages comme l'accès à distance à un nombre croissant de fonctionnalités des systèmes d'information (SI), y compris à des fonctions critiques jusqu'alors accessibles que sur site.

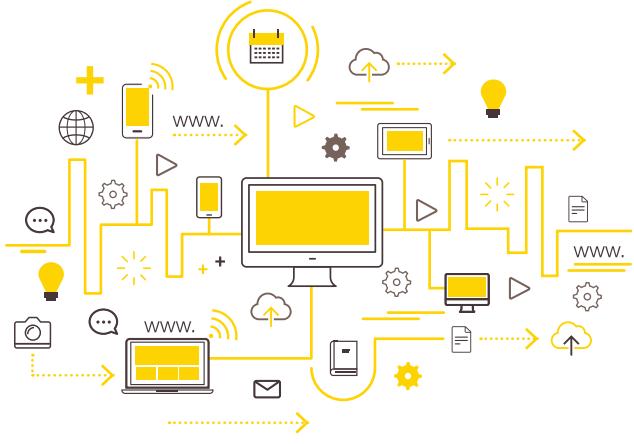
Le nombre d'objets connectés dans le monde devrait ainsi exploser au cours de la décennie à venir pour atteindre plusieurs dizaines de milliards. Corolairement, le cyberespace s'étend en connectant des systèmes jusqu'alors isolés et en créant des interdépendances entre eux, le déploiement du réseau 5G en sera un catalyseur.

[1] Le *Cloud Computing* est l'accès à des services informatiques en ligne, *via* Internet, hébergés sur des serveurs distants.

AUGMENTATION DE LA SURFACE D'ATTAQUE

Si la transformation numérique est synonyme de gain de productivité, elle a pour inconvénient majeur d'augmenter la surface d'attaque des entreprises. En effet, plus une entreprise est connectée au cyberespace[1], plus elle offre de portes d'entrées aux cybercriminels. Les entreprises qui se connectent au cyberespace en étant mal préparées et mal protégées constituent une cible de choix pour les actes de malveillance.

Des attaques d'envergure mondiale, ciblées ou non, telles que *WannaCry* ou *NotPetya*[2], ont affecté des centaines de milliers d'appareils à travers le monde et ont porté à la connaissance du grand public les menaces provenant du cyberespace.



[1] Le cyberespace est un espace de communication constitué des équipements numériques et des interconnexions qui les relient. C'est un vaste réseau d'infrastructures où circule un flux d'informations et au sein duquel chaque donnée emprunte un itinéraire qui lui est propre. Il regroupe l'Internet, l'Internet des objets, le *Deep Web*, les réseaux de téléphonie, etc.

[2] *WannaCry* et *NotPetya* sont des rançongiciels apparus en 2017 qui ont paralysé des centaines de milliers d'entreprises à travers le monde.

UN RETARD CHEZ LES TPE, PME ET ETI

Les grandes entreprises ont été touchées comme les autres, elles ont pris rapidement la mesure du risque cyber.

Encouragées entre autres par la réglementation et généralement habituées à solliciter l'expertise des entreprises de services du numérique, elles se sont dotées de moyens de protection et ont fait évoluer leur mode de fonctionnement.

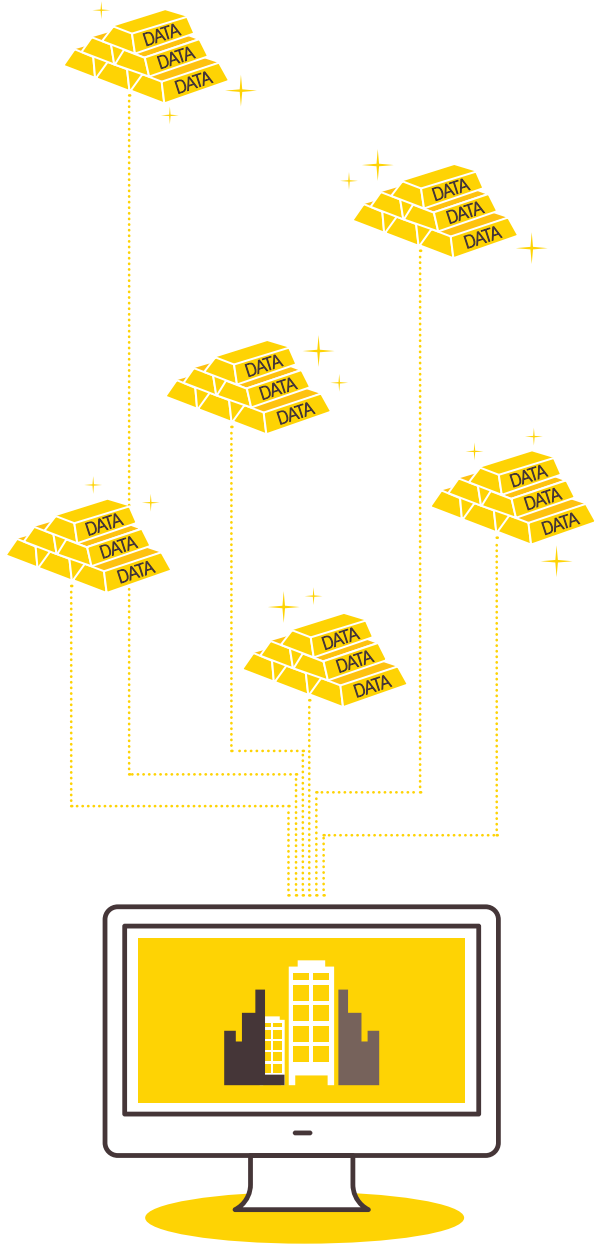
Se protéger de telles attaques est alors devenu un enjeu stratégique pour les Grands Groupes afin de préserver leur valeur financière et leur réputation. Les TPE, PME et ETI, ne sont pas aussi matures en termes de cybersécurité et peinent à entreprendre cette démarche par manque de moyens ou par méconnaissance.

LES TPE, PME ET ETI SONT POURTANT DES CIBLES D'INTÉRÊT

Les cyberattaques ne sont pourtant pas l'apanage des Grands Groupes. Sans même en avoir conscience, toutes les entreprises possèdent des informations de valeur (coordonnées bancaires, coordonnées clients, projet de R&D, etc.) qui se monnayent facilement auprès du bon acheteur (concurrent, *Dark web,* etc.). Nombre d'entre elles sont aussi victimes de rançongiciels qui rendent indisponibles leurs données et même leurs chaînes de production. Cela entraîne certaines d'entre elles jusqu'au dépôt de bilan.

Les entreprises peuvent être victimes d'attaques ciblées et très sophistiquées notamment lorsqu'elles sont sous-traitantes de Grands Groupes ou qu'elles font partie d'une filière industrielle. Elles constituent souvent le maillon faible de la chaîne de valeur en termes de cybersécurité. Comme lors d'un cambriolage, lorsque la porte est blindée le voleur passe par la fenêtre ! En outre, toutes les entreprises sont exposées à la cybercriminalité de masse, c'est-à-dire à des attaques non-ciblées diffusées à grande échelle et qui exposent tout appareil connecté au cyberespace, c'est ce que l'on appelle le « bruit cyber ».

Ces attaques, parfois basiques, peuvent provoquer des dommages considérables et paralyser une entreprise pendant des jours voire des semaines, sans même parler du préjudice financier et de la perte de réputation.



PRENDRE CONSCIENCE DU RISQUE ET SURTOUT PRENDRE DES MESURES : LA CYBER-HYGIÈNE

La prise de conscience du risque cyber commence à faire son chemin chez les dirigeants de TPE, PME et ETI. Pour autant, peu d'actions concrètes sont mises en œuvre pour prévenir le risque cyber au sein de leur entreprise.

Cette absence de passage à l'acte chez les dirigeants s'explique par plusieurs facteurs :

Facteur n°1

Une connaissance superficielle du risque cyber qui les conduit souvent à mésestimer les enjeux et à déléguer à leur équipe informatique considérant qu'il ne s'agit que d'un problème technique. Quand ils en ont conscience, les dirigeants ont tendance à se focaliser sur la menace externe émanant de groupes de cybercriminels motivés par l'argent, alors que les menaces externes issues de l'environnement de l'entreprise (fournisseurs, clients, partenaires) et internes (employés, consultants, etc.) sont nettement sous-estimées.

Solution : l'exposition des PME et ETI au risque cyber est pourtant bien réel. La menace émane aussi bien des cybercriminels directement que des fournisseurs, des clients ou des collaborateurs de l'entreprise qui peuvent servir de porte d'entrée aux cyberattaques. Ainsi la prise en compte du risque cyber ne se réduit pas à des solutions informatiques. Elle nécessite une prise de conscience commune et doit transparaître dans l'organisation et les comportements humains.

Facteur n°2

Le manque de solutions clé-en-main et une offre cyber qui est orientée vers des Grands Groupes. De plus, les solutions disponibles sur le marché ne sont pas toujours bien adaptées aux dirigeants de PME et ETI qui ont du mal à se les approprier.

Solution : il existe des solutions pour accompagner les entreprises dans l'appréhension et la gestion du risque cyber. Cet accompagnement peut prendre la forme de missions de conseil, de campagnes de sensibilisation, de formations, de diagnostics adaptés spécifiquement aux PME et ETI.

Facteur n°3

Le coût perçu d'un investissement en cybersécurité joue un rôle dissuasif. Le manque de moyens financiers est un obstacle souvent évoqué dans l'adoption de mesures de sécurisation pour les dirigeants, pourtant la perte de valeur en cas d'attaque peut se révéler bien plus élevée.

Solution : un investissement important dans des solutions techniques n'est pas toujours nécessaire car il existe des actions simples et peu onéreuses qui permettent de réduire significativement l'exposition au risque cyber. Il s'agit d'un ensemble de gestes simples et de comportements à adopter que l'on appelle **la cyber-hygiène.**

À RETENIR

La cyber-hygiène désigne l'ensemble des bonnes pratiques à observer par les collaborateurs pour limiter le risque d'attaques et de fuite d'information. L'ensemble de ces mesures sont détaillées dans la partie 3 de ce guide. Afin que ces bonnes pratiques se diffusent au sein de l'entreprise, il est indispensable que l'ensemble du comité de direction y soit sensibilisé. C'est en particulier au dirigeant de devenir le promoteur de ce sujet au sein de son entreprise en mobilisant l'ensemble de son comité de direction (DAF, DRH, DSI, etc.).

PRÉSERVER LA VALEUR DE VOTRE ENTREPRISE, UNE PRIORITÉ ABSOLUE

Prendre des mesures de cybersécurité présente des avantages en premier lieu desquels préserver la valeur de votre entreprise.

Valeur financière

En cas de cyberattaque, votre entreprise pourra être confrontée à un préjudice financier tel qu'une perte de chiffre d'affaires résultant de l'indisponibilité des systèmes de l'entreprise ou d'un arrêt de l'activité, voire un détournement de fonds. À ces pertes s'ajouteront des dépenses exceptionnelles parmi lesquelles :

- les diagnostics techniques et la remise en service des systèmes et équipements affectés ;
- les compensations clients et fournisseurs ;
- les frais juridiques ;
- les amendes et/ou la mise en conformité ;
- les relations publiques et la communication de crise ;
- l'augmentation de vos primes d'assurance.

Ces coûts directs ne sont pourtant que la partie émergée de l'iceberg, à ceux-ci viendront s'ajouter tous les coûts cachés qui sont très difficiles à estimer mais qui impacteront de manière certaine la valeur de l'entreprise sur le long terme.

Valeur réputationnelle

Vos clients, fournisseurs, partenaires financiers ont construit avec vous une relation de confiance.

La réputation de votre entreprise est un gage de confiance qui sera mis à mal en cas de cyberattaque. Cela se traduira par la perte de notoriété et la détérioration de l'image de marque, la perte de chiffre d'affaires engendrée par la perte de confiance des clients et des prospects, etc.

Par ailleurs, l'entrée en vigueur du Règlement Général sur la Protection des Données (RGPD), en 2018, rend obligatoire la déclaration d'incident auprès de la CNIL en cas de fuite de données et l'information des personnes concernées par cette fuite. Il n'est donc plus possible de garder secrète une fuite de données personnelles.

Cette déclaration peut entraîner des sanctions financières conséquentes si des manquements sont constatés. Ayez conscience que vous avez aussi une réputation « miroir » au sein des communautés de cybercriminels.

Si vous êtes une cible facile ou connue pour payer les rançons, vous risquez d'être plus souvent la cible d'attaques. Les vulnérabilités identifiées dans vos systèmes seront partagées au sein de la communauté des cybercriminels pour être réexploitées ultérieurement tant qu'elles n'auront pas été corrigées.

Valeur intangible

À travers une cyberattaque, ce sont bien plus que des données qui peuvent vous être dérobées. Les impacts néfastes sur vos actifs intangibles peuvent s'inscrire dans la durée avec la perte de propriété intellectuelle, le vol ou la perte d'un projet de R&D, la récupération de votre portefeuille de clients, la perte d'un avantage concurrentiel.

Valeur humaine

L'impact humain est souvent sous-estimé. Pourtant, la soudaineté et la gravité d'une cyberattaque sont éprouvantes pour les collaborateurs.

La situation de crise est une source de stress immense pour le dirigeant et ses équipes dont les effets sont perceptibles sur le court terme (état de choc, *burn-out*) comme sur le long terme (perte de motivation, traumatisme, paranoïa).

L'arrêt d'activité causé par une cyberattaque peut donner lieu à une période de chômage technique voire à des plans de licenciements lorsque les pertes sont trop importantes.

Une démarche créatrice de valeur

Au-delà d'une parade contre la cybermenace, vous pouvez trouver dans la cybersécurité un véritable vecteur de création de valeur pour votre entreprise.

En externe :

Prendre des dispositions pour sécuriser vos données contribue à renforcer la confiance de vos partenaires et à valoriser l'image d'une entreprise fiable et digne de confiance. Un bon niveau de maturité en termes de cybersécurité peut devenir un argument commercial supplémentaire pour vous différencier de vos concurrents.

D'une manière générale, les enjeux de cybersécurité prennent une place de plus en plus importante dans les prises de décisions :

- **contrats commerciaux :** de nombreux sous-traitants sont visés par des attaques de façon à s'introduire, *in fine,* dans le réseau des grands donneurs d'ordres, généralement plus difficiles à pénétrer directement. Les donneurs d'ordres sont de plus en plus attentifs au niveau de sécurité de leurs prestataires et n'hésitent pas à intégrer la maturité en matière de cybersécurité dans les critères de choix de leurs sous-traitants ainsi que dans les contrats commerciaux. Cela est même devenu la norme dans les secteurs à forts enjeux comme l'aéronautique et la défense ;
- **obtention de financements :** les banquiers, les investisseurs et les assurances sont de plus en plus en plus regardants sur le niveau de maturité des entreprises qu'ils financent. En effet, lorsqu'ils financent un projet de R&D par exemple, ils sont en droit d'attendre que la création de valeur qui en résulte soit préservée au sein de l'entreprise ;
- **attente des consommateurs :** la sécurité devient un argument de vente pour certains produits, en complément fort de l'ergonomie.

En interne :

La cybersécurité introduit de nouveaux défis pour votre entreprise, vous donnant l'occasion de vous questionner sur votre organisation interne.

La prise en compte du risque cyber permet de mettre en lumière les adaptations possibles pour améliorer le fonctionnement de votre entreprise. Se saisir du risque cyber, c'est aussi l'occasion de moderniser votre organisation, vos pratiques internes, et vos systèmes d'information.

En somme, la prise en compte du risque cyber peut donc être créatrice de valeur pour votre entreprise à la fois en interne pour améliorer l'organisation et moderniser les systèmes d'information, et en externe comme facteur différenciant pouvant servir d'argument commercial.

Évidemment, un bon niveau de maturité en cybersécurité n'est pas une garantie infaillible contre les cyberattaques et il faut garder à l'esprit que si le risque zéro n'existe pas, il le réduit fortement.

PRENDRE DES MESURES DE CYBERSÉCURITÉ POUR PROTÉGER L'ENTREPRISE SUR :

- Sa valeur financière
- Sa valeur réputationnelle
- Sa valeur intangible
- Sa valeur humaine

C'est créer de la valeur pour son entreprise en externe et en interne

02.

CONNAÎTRE ET IDENTIFIER...

... LES CYBER-ATTAQUES

Il est important de connaître les cyberattaques et de savoir en identifier les signaux lorsqu'elles surviennent. Cette partie vous permettra de vous familiariser avec les types d'attaque les plus fréquents.

Le facteur humain est au cœur de toutes les cyberattaques. Elles utilisent de manière quasi-systématique des ressorts **d'ingénierie sociale.**

L'ingénierie sociale est un ensemble de techniques de manipulation visant à influencer un individu en vue de commettre un acte malveillant. Elle s'appuie sur des comportements et des sentiments humains comme la peur, la confiance, la curiosité, l'appât du gain et tire profit des failles d'une organisation sociale, comme par exemple, les relations hiérarchiques au sein d'une entreprise.

Les cybercriminels ont très souvent recours à ces mécanismes pour mener leurs attaques. **Les témoignages qui suivent sont inspirés de faits réels.**

LES PRINCIPALES CYBERATTAQUES ET LEURS IMPACTS	FRÉQUENCE ↓	FINANCIER ↓	RÉGLEMENTAIRE ↓	IMAGE ↓
1. Rançongiciel	22 %	●●●	●●	●●
2. Intrusion dans les systèmes d'information	20 %	●●	●●	●
3. Piratage de compte	14 %	●	●	●●
4. Usurpation d'identité	10 %	●●	●	●●
5. Hameçonnage	8 %	●●	●	●
6. Déni de service	5 %	●●	●	●●
7. Fraudes au virement (FOVI)	4 %	●●●	●	●
8. Défiguration de site Internet	2 %	●	●	●●

1. RANÇONGICIEL

FRÉQUENCE : 22 % - **FINANCIER :** ● ● ●
RÉGLEMENTAIRE : ● ● - **IMAGE :** ● ●

Définition

Un rançongiciel (ou *ransomware*) est un logiciel malveillant qui chiffre les données d'un appareil, ce qui les rend inaccessibles. Une rançon est réclamée, le plus souvent en cryptomonnaies, avec la promesse de restaurer l'accès aux données. Ce type d'attaque vise à créer le sentiment de panique chez la victime en menaçant de divulguer publiquement les données ou de les supprimer, en imposant un ultimatum pour le paiement de la rançon et en faisant augmenter le montant de la rançon au fil du temps (doublement du prix toutes les dix minutes par exemple).

Bon réflexe

Si vous êtes victime d'une attaque par rançongiciel, commencez par déconnecter votre appareil d'Internet et du réseau informatique. Demandez une assistance spécialisée et identifiez clairement l'origine de l'attaque pour pouvoir corriger ce qui doit l'être **avant la remise en production.** N'entrez pas en contact avec les cybercriminels et ne payez pas la rançon car vous n'avez aucune garantie que vos données vous seront restituées. De plus, vous encourageriez les cybercriminels à vous cibler à nouveau. Il existe parfois des solutions de déchiffrement mises à disposition par les autorités.

À titre préventif, mettez à jour vos systèmes, logiciels et antivirus, ayez une vigilance accrue sur les pièces jointes et liens contenus dans les e-mails, évitez de naviguer sur des sites ou d'installer des logiciels de source douteuse, durcissez la sécurité de vos accès externes, effectuez des sauvegardes régulières et déconnectées de votre réseau principal.

Témoignage

Équipementier automobile

Richard dirige une entreprise de fabrication de pièces métalliques à destination de l'industrie automobile et aéronautique. Son catalogue contient plus de 50 000 références de pièces allant de vis haute résistance au châssis de semi-remorque. Il compte plusieurs centaines d'industriels parmi ses clients et fournisseurs avec qui il a interfacé son système d'information pour le suivi des commandes.

Un jour, un collaborateur lui signale un problème informatique et lui montre un message d'erreur qui s'affiche à l'écran. Celui-ci indique que les bases de données ont été chiffrées et que l'accès aux informations ne sera restitué qu'en échange du versement d'une rançon qui s'élève à plusieurs milliers d'euros et qui doit être payée en cryptomonnaies. Un compte à rebours s'affiche à l'écran. Après plusieurs heures à tenter de restaurer les systèmes, les données sont toujours inaccessibles. Sans système d'information, le passage et le suivi des commandes est interrompu et la chaîne de production est immobilisée. Le compte à rebours vient d'arriver à son terme et le montant de la rançon a doublé, ce sont maintenant plusieurs dizaines de milliers d'euros qui sont réclamés.

Les sauvegardes de secours ont été réalisées sur des serveurs non sécurisés qui ont également été chiffrés par le rançongiciel rendant impossible toute tentative de restauration. Devant la gravité de la situation, Richard décide de verser la rançon dans l'espoir de récupérer l'accès à son système d'information. En vain, ses données ne lui seront jamais restituées.

Les investigations qui ont suivi ont permis d'identifier la source de l'attaque qui s'est propagée par l'un des fournisseurs de l'entreprise avec lequel elle avait interfacé son système d'information. Il a fallu trois semaines pour rétablir les systèmes et que la situation revienne à la normale.

2. INTRUSION DANS LES SYSTÈMES D'INFORMATION

FRÉQUENCE : 20 % - **FINANCIER :** ●●
RÉGLEMENTAIRE : ●● - **IMAGE :** ●

Définition

Des individus malveillants s'introduisent dans le système d'information de l'entreprise et en altèrent le fonctionnement ou dérobent des données.

L'infection peut provenir de l'ouverture d'une pièce jointe, d'un lien hypertexte, d'une navigation sur des sites Internet compromis, d'un réseau public non sécurisé, d'une intrusion directe dans le système en exploitant une faille de sécurité, d'une clé USB contenant un logiciel malveillant, d'un collaborateur mal intentionné, ou encore du système d'information d'un client ou d'un fournisseur compromis.

Par la suite, le cybercriminel peut chercher à s'introduire dans les autres équipements du réseau attaqué.

Bon réflexe

Paramétrez et mettez régulièrement à jour les équipements de sécurité de votre système informatique (antivirus, pare-feu), les systèmes d'exploitation ainsi que les logiciels installés sur vos équipements. Il ne faut jamais installer de logiciels, programmes, applications ou équipements « piratés » ou dont l'origine ou la réputation est douteuse.

Les comptes administrateurs ne doivent être utilisés qu'en cas de nécessité et les droits des utilisateurs limités au strict nécessaire.

Pensez à identifier les appareils ayant accès aux réseaux externes à l'entreprise, à mettre en place un suivi automatisé du trafic.

Ayez une surveillance régulière de votre système d'information pour détecter toute activité anormale (connexion suspecte, sortie d'information illogique) et faites-le auditer.

Témoignage

Site de rencontre en ligne

Aurélie a fondé un site de rencontre en ligne qui connaît un succès fulgurant. Il rassemble aujourd'hui plusieurs milliers de célibataires à la recherche du (ou de la) partenaire idéal(e). Le site d'Aurélie s'appuie sur un moteur innovant, basé sur de l'intelligence artificielle permettant d'établir une correspondance entre les utilisateurs à partir du profil détaillé qu'ils ont renseigné sur le site.

Un jour Aurélie reçoit plusieurs réclamations de la part de clients mécontents. Ceux-ci se plaignent que leurs informations personnelles se trouvent en libre accès sur Internet dévoilant une partie importante de leur vie privée (âge, sexe, centres d'intérêt, orientation sexuelle, religion, etc.).

Il s'avérera plus tard qu'un cybercriminel est parvenu à s'introduire dans les systèmes d'information de l'entreprise et à dérober l'intégralité de la base de données contenant les profils détaillés des utilisateurs avant de les publier en ligne.

3. PIRATAGE DE COMPTE

FRÉQUENCE : 14 % - **FINANCIER :** ●
RÉGLEMENTAIRE : ● - **IMAGE :** ● ●

Définition

Le piratage de compte désigne la prise de contrôle par un individu malveillant d'un compte au détriment de son propriétaire légitime. Il peut s'agir de comptes de messagerie, de comptes administrateurs, de réseaux sociaux, de sites, de plateformes, etc. Pour prendre possession de votre compte, les cybercriminels peuvent forcer votre mot de passe s'il est trop simple, installer des logiciels espions enregistreurs de frappe, utiliser des techniques d'hameçonnage, attaquer un site qui détient votre mot de passe si vous l'utilisez sur plusieurs sites.

Bon réflexe

Utilisez des mots de passe complexes et différents pour chaque usage, vous pouvez avoir recours à un gestionnaire de mots de passe. De cette manière, si un de vos comptes est compromis les cybercriminels ne pourront pas prendre possession de vos autres comptes en utilisant le même mot de passe.

L'authentification multi-facteurs est sans aucun doute la meilleure parade contre ce type d'attaque. Elle requiert de valider plusieurs points de contrôle pour accéder à vos comptes (mot de passe, confirmation par e-mail et/ou par sms, empreintes digitales, clé sécurisée) ce qui complique considérablement la tâche des cybercriminels.

Témoignage

Hôtellerie-Restauration

Jacques dirige une entreprise d'Hôtellerie-Restauration qui gère une dizaine d'établissements en France.

Son positionnement lui permet d'attirer une clientèle haut de gamme. Il a su nouer de nombreux partenariats avec des agences de voyage présentes en Europe à qui il propose des tarifs préférentiels.

En fin d'année, le directeur financier effectue le rapprochement comptable avec les comptes bancaires de l'entreprise et s'étonne d'un écart de trésorerie important. En remontant l'historique des règlements, il remarque des mouvements suspects sur les comptes de l'entreprise qui ont eu lieu tout au long de l'année. Les volumes de transactions réalisées par l'entreprise étant importants, les petites sommes dérobées sont restées inaperçues.

Après une enquête minutieuse, il a pu être établi que des cybercriminels ont eu accès aux identifiants et mots de passe du directeur financier, leur permettant ainsi d'initier des virements vers un compte à l'étranger. Le préjudice s'élève à plusieurs dizaines de milliers d'euros.

4. USURPATION D'IDENTITÉ

FRÉQUENCE : 10 % - **FINANCIER :** ●●
RÉGLEMENTAIRE : ● - **IMAGE :** ●●

Définition

L'usurpation d'identité consiste à prendre l'identité d'une personne dans le but de réaliser des actions frauduleuses. Cependant, de plus en plus de cybercriminels usurpent l'identité d'entreprises afin de passer des commandes de biens et de services dans des quantités importantes ou de contracter des emprunts en leur nom. Les fraudeurs sont très organisés, ils ouvrent de fausses lignes téléphoniques, créent des adresses électroniques similaires à celles de l'entreprise cible, falsifient des bons de commandes voire procèdent à des enregistrements auprès du registre du commerce. L'identité numérique peut aussi être usurpée avec la mise en ligne d'un site miroir, en tout point identique à celui de l'entreprise qui sera utilisé pour escroquer ses clients.

Bon réflexe

Veillez à conserver en sécurité toutes les informations liées à l'identité des collaborateurs, de l'entreprise elle-même et de ses mandataires.

Accordez une attention particulière aux signaux faibles qui pourraient révéler que votre identité a été usurpée (remontées étranges de la part des clients ou fournisseurs, site Internet similaire au vôtre, etc.) et changez régulièrement vos mots de passe.

Témoignage

Commerce de matériel informatique

Gabriel a repris l'entreprise familiale qui commercialise du matériel informatique à destination des professionnels et des particuliers. Il propose ses équipements à la location, à la vente, et développe également une activité de services de maintenance et de formation.

En fin de semaine, il reçoit une relance sur une facture impayée de la part d'un de ses fournisseurs. Celui-ci lui réclame plusieurs milliers d'euros pour la livraison d'équipements informatiques qui aurait eu lieu un mois plus tôt. Gabriel n'a jamais effectué cette commande.

En tentant d'obtenir des explications, Gabriel se heurte à l'incrédulité de son fournisseur qui est bien déterminé à se faire payer. Ce dernier lui présente un bon de commande au nom de son entreprise signé de sa main ainsi qu'une copie de sa pièce d'identité.

Au cours de l'enquête, il s'avérera que des cybercriminels sont parvenus à se procurer la pièce d'identité de Gabriel pour passer en commande en son nom et à se faire livrer plusieurs milliers d'euros de matériel informatique.

5. HAMEÇONNAGE

FRÉQUENCE : 8 % - **FINANCIER :** ● ●
RÉGLEMENTAIRE : ● - **IMAGE :** ●

Définition

L'hameçonnage (ou *phishing*) n'est pas une attaque à proprement parler mais un vecteur pour une attaque ultérieure. Comme son nom l'indique, cette technique consiste à « appâter » une victime en l'incitant à fournir des informations confidentielles ou en mettant à sa portée des codes malveillants et en attendant qu'elle les active à son insu en ouvrant une pièce jointe ou en cliquant sur un lien hypertexte. Une fois activés, ces codes malveillants serviront de base pour un piratage de compte qui permettra à son tour une intrusion dans un système d'information, une fraude au faux ordre de virement, une usurpation d'identité voire une attaque par rançongiciel quand il s'agit d'une récupération d'identifiants d'un compte permettant un accès distant au réseau de l'entreprise.

Bon réflexe

Méfiez-vous des messages inattendus ou alarmistes. Vérifiez toujours l'adresse du site sur lequel vous êtes redirigé. N'ouvrez jamais les pièces jointes et liens suspects ou d'origine inconnue. Gardez en tête que les offres trop alléchantes sont souvent trop belles pour être vraies !

Témoignage

Agence de communication

Sarah travaille dans une agence de communication qui propose un accompagnement marketing aux entreprises du secteur de l'habillement. L'agence a mis en ligne un site vitrine présentant ses prestations et ses équipes marketing.

Sarah reçoit une invitation à participer à une cagnotte en ligne pour le mariage de sa collègue Ophélie. Il est précisé dans le message que l'initiative doit rester secrète pour ne pas gâcher la surprise. Sarah n'était pas informée du mariage de sa collègue mais décide de participer à la cagnotte. Elle complète la carte de vœux en ligne et renseigne ses informations bancaires.

Sans le savoir, Sarah vient d'être victime d'hameçonnage et de communiquer ses informations personnelles à des cybercriminels.

6. DÉNI DE SERVICE

FRÉQUENCE : 5 % - **FINANCIER :** ●● **RÉGLEMENTAIRE :** ● - **IMAGE :** ●●

Définition

Une attaque en déni de service ou en déni de service distribué (DDoS pour *Distributed Denial of Service*) consiste à rendre inaccessible un site ou un service en ligne en saturant le serveur de requêtes. Cette sur-sollicitation du serveur provoque une panne ou un fonctionnement fortement dégradé du service. Le déni de service a des conséquences particulièrement graves lorsqu'il porte sur un site marchant car il engendre une interruption immédiate des ventes. Il arrive même que ce type d'attaque ne constitue qu'une diversion pour mener une attaque visant à voler des données sensibles.

Bon réflexe

Les solutions pour se prémunir contre le déni de service sont essentiellement d'ordre technique.

Sécurisez le serveur qui héberge vos services en ligne et configurez-le en fonction de vos besoins. Un bon paramétrage permettra d'ignorer les sollicitations trop nombreuses du serveur, d'imposer la validation d'un *captcha,* de limiter le nombre d'utilisateurs connectés en même temps et ainsi de conserver votre serveur opérationnel.

Pour mettre en place ces mesures vous pouvez avoir recours à une solution anti-DDoS proposée par votre hébergeur ou votre opérateur.

Témoignage

Boutique de vêtements en ligne

Catherine dirige une boutique de vente de vêtements en ligne. Elle commercialise plus de 500 articles et accessoires à destination des particuliers en France et en Europe. À l'approche des fêtes de fin d'année, au cours desquelles elle réalise la plus grande partie de son chiffre d'affaires, Catherine met en ligne sa nouvelle collection.

Quelques jours plus tard, alors que l'activité bat son plein, le site de l'entreprise est indisponible. Les serveurs ne sont plus en mesure de répondre aux trop nombreuses tentatives de connexions. Il s'agit en réalité d'une cyber-attaque par déni de service visant à mettre à mal son site Internet.

Ne pouvant assurer la prise de commandes pendant cette période clé, l'entreprise a enregistré une perte de chiffre d'affaires de plusieurs millions d'euros.

7.a. FRAUDE AU VIREMENT PAR CHANGEMENT DE RIB

FRÉQUENCE : 4 % - **FINANCIER :** ● ● ●
RÉGLEMENTAIRE : ● - **IMAGE :** ●

Définition

Le changement de RIB consiste pour les cybercriminels à contacter un employé du service de comptabilité ou de trésorerie de l'entreprise en se faisant passer pour un fournisseur ou un client et en prétextant un changement de relevé d'identité bancaire. Il arrive même que les cybercriminels se fassent passer pour les salariés de l'entreprise pour percevoir leur salaire à leur place par exemple. Les nouveaux comptes bancaires sont en réalité ceux des fraudeurs qui sollicitent ensuite des virements en urgence pour des factures impayées et récupèrent d'importantes sommes d'argent avant que l'entreprise victime ne prenne conscience de la supercherie. Le changement de RIB est, avec la fraude au président, l'un des deux types de fraude aux faux ordres de virement « FOVI ». Il s'agit d'une escroquerie très répandue où les cybercriminels privilégient l'envoi d'e-mails et les appels téléphoniques pour mener une arnaque basée sur l'abus de confiance. Il peut s'écouler plusieurs mois entre le changement de RIB et la demande de paiement frauduleuse.

Bon réflexe

Ne réalisez jamais un changement de RIB ou un virement dans l'urgence. Ils doivent systématiquement faire l'objet des vérifications d'usage. Une demande pressante et imprévue doit éveiller les soupçons surtout si l'interlocuteur se montre insistant. Plus largement, ce sont toutes les données administratives relatives à vos fournisseurs (notamment téléphone et e-mail) qui doivent faire l'objet d'une vigilance accrue et d'une procédure précise pour toute modification.

La seule méthode réellement efficace pour déjouer une fraude par changement de RIB est l'appel téléphonique directement à votre fournisseur, ce qui nécessite que vous disposiez de ses coordonnées et que celles-ci soient fiables.

Les collaborateurs qui ont accès à ces données ou qui sont en capacité d'effectuer des virements au sein de votre entreprise doivent faire l'objet d'une sensibilisation et d'une formation spécifique pour leur apprendre les bons réflexes.

Il est aussi recommandé de ne pas prendre en compte automatiquement les RIB qui figurent directement sur les factures.

Témoignage

Entreprise de transport et d'entreposage

Matthieu dirige une entreprise de transport routier qui propose des services logistiques. Sa large flotte de véhicules et son réseau de centres logistiques lui permettent de gérer l'approvisionnement de ses clients partout en Europe.

Un jour, le comptable de l'entreprise s'inquiète de nombreux retards de paiement de la part de plusieurs clients, malgré les relances. Certains clients assurent même avoir déjà réglé les factures en question.

Matthieu réalise que les factures émises ont bien été réglées par les clients mais sur un autre compte bancaire que celui de l'entreprise. En amont de l'émission des factures, le RIB a en effet été changé par des individus malveillants se faisant passer pour l'entreprise auprès des clients. En l'absence de procédure relative au changement de RIB, les clients ont effectué les règlements sur le compte des cybercriminels en pensant régler l'entreprise de Matthieu.

7.b. FRAUDE AU PRÉSIDENT

FRÉQUENCE : 4 % - **FINANCIER :** ● ● ●
RÉGLEMENTAIRE : ● - **IMAGE :** ●

Définition

La fraude au Président est un autre type de fraude aux faux ordres de virement « FOVI ». Des cybercriminels contactent un employé dans l'entreprise en se faisant passer pour le dirigeant ou un de ses représentants et lui demandent d'exécuter des virements sur des comptes à l'étranger. Les cybercriminels sont extrêmement bien renseignés sur l'entreprise et très bien préparés. Ils sont même capables de maquiller leur voix. Ils élaborent des scénarios crédibles et ciblent la plupart du temps les employés des services financiers et comptables. Les cybercriminels présentent souvent l'opération comme confidentielle et urgente afin d'isoler leurs victimes de sorte à ne pas leur laisser le temps de réagir. Ils n'hésitent pas non plus à harceler la personne par téléphone plusieurs fois par heure sous diverses identités.

Bon réflexe

Un virement qui ne suit pas la procédure habituelle doit toujours éveiller des soupçons. Il arrive que certaines situations imprévues nécessitent de déroger aux règles habituelles et les cybercriminels utilisent cette faille en échafaudant un scénario très crédible.

Pour identifier son interlocuteur avec certitude il est important d'utiliser des canaux de communication fiables (vérifier, *a minima,* l'adresse e-mail de l'expéditeur, rappeler le dirigeant en utilisant l'annuaire d'entreprise, s'assurer que la situation est avérée auprès de ses collègues, et ne pas hésiter à poser des questions). En cas de doute, il ne faut surtout pas procéder au virement.

Il est indispensable de mettre en place une procédure de saisie et de contrôle des virements à laquelle il ne faut jamais déroger.

Témoignage

Fabricant d'appareils électroménagers

Dominique travaille au service comptable d'une entreprise industrielle d'appareils électroménagers, en charge du règlement des factures.

Un vendredi en fin de journée, alors qu'il est seul au bureau, il reçoit un appel urgent de la part du dirigeant de l'entreprise en personne. Celui-ci est en voyage d'affaires en Europe du Nord pour négocier un important contrat avec un distributeur local. Il demande à Dominique d'effectuer immédiatement un virement pour finaliser la signature du contrat. Il insiste sur l'urgence et sur la confidentialité de la situation allant jusqu'à menacer Dominique s'il refuse de coopérer.

Intimidé, celui-ci finit par accéder à sa demande et effectue le virement sur le compte communiqué par téléphone. L'interlocuteur était en fait un cybercriminel se faisant passer pour le dirigeant.

Les cybercriminels étaient particulièrement bien préparés pour mener cette attaque. Ils avaient identifié précisément qui étaient les collaborateurs clés dans l'organigramme et avaient scruté les réseaux sociaux pour être informés des déplacements du dirigeant, celui-ci participait à un salon à l'étranger ce qui rendait le scénario crédible.

8. DÉFIGURATION DE SITE INTERNET

FRÉQUENCE : 2 % - **FINANCIER :** ●
RÉGLEMENTAIRE : ● - **IMAGE :** ● ●

Définition

La défiguration est une attaque informatique qui consiste à modifier l'apparence ou le contenu du site Internet de l'entreprise cible. Cette attaque peut rendre le site Internet inutilisable entraînant ainsi une interruption d'activité et porte aussi atteinte à l'image et à la crédibilité de l'entreprise. Les cybercriminels agissent pour des motivations politiques, idéologiques, par goût du challenge, chantage, vengeance, ou pour des raisons économiques (concurrence par exemple).

Bon réflexe

La sécurisation et le bon paramétrage du serveur qui héberge votre site est à nouveau une mesure essentielle.

En complément, il faudra utiliser un mot de passe long et complexe pour les profils administrateurs, réaliser des mises à jour de sécurité et des sauvegardes régulières de votre site, limiter le nombre d'utilisateurs et leurs privilèges.

Enfin, surveillez l'activité de votre site régulièrement et faites-le auditer.

Témoignage

Entreprise de transformation agroalimentaire

Katia dirige une entreprise de transformation agroalimentaire spécialisée dans les produits à base de viande. Elle fournit les grandes surfaces et les petits détaillants et exporte ses produits en Europe.

Un jour, Katia découvre que le site Internet de son entreprise a été détourné. Il affiche désormais des images d'animaux morts et des messages militants en faveur de la cause animale.

Les opérations de l'entreprise n'ont pas été impactées par cette attaque et aucune demande de rançon n'a été formulée, pourtant, l'image de l'entreprise a été mise à mal.

Des cybercriminels ont utilisé le site de l'entreprise à des fins idéologiques, ils ont vraisemblablement eu accès à l'identifiant et au mot de passe permettant d'éditer le site.

POUR ALLER PLUS LOIN :
Pour découvrir les cybermenaces et les moyens de s'en prémunir, rendez-vous sur : https://www.cybermalveillance.gouv.fr/cybermenaces

SE PRÉMUNIR

03.

La prévention du risque cyber passe par la diffusion d'une culture de la cybersécurité au sein de votre entreprise qui doit se traduire par une attitude de méfiance raisonnable.

ADOPTER LA CYBER-HYGIÈNE COMME CULTURE D'ENTREPRISE

Il est essentiel que vos collaborateurs adoptent les bons comportements au quotidien pour limiter au maximum les risques. Gardez à l'esprit que chaque collaborateur est un maillon à part entière de la chaîne d'information. Il peut être aussi bien le vecteur par lequel une cyberattaque pénètre vos systèmes qu'un acteur vigilant capable de signaler les activités suspectes vous permettant ainsi de déjouer des cyberattaques.

La sensibilisation de vos collaborateurs est donc une mesure essentielle pour les accompagner dans la prise de conscience des comportements à risques et dans l'adoption des bons réflexes. Pour que cette culture de la cybersécurité se diffuse au sein de votre entreprise, il importe qu'elle soit incarnée par le dirigeant et son comité de direction.

Au-delà de votre entreprise c'est tout votre écosystème qu'il faut fédérer dans cette démarche : fournisseurs, sous-traitants, clients, partenaires commerciaux, prestataires…

À chaque fois que vous sollicitez un prestataire, que vous demandez un devis à un fournisseur ou que vous entrez en relation d'affaires, c'est l'occasion de questionner les pratiques en place chez vos partenaires. En effet, leurs systèmes d'information peuvent être connectés aux vôtres et une vulnérabilité chez eux peut avoir un impact chez vous. Ils possèdent, *a minima,* des informations confidentielles sur votre entreprise comme votre RIB par exemple et il est tout à fait légitime que vous les interrogiez sur la manière dont ils protègent vos données car un grand nombre d'attaques ont recours à de fausses factures ou à une usurpation d'identité. Vous pouvez demander à consulter leur Plan d'Assurance Sécurité et l'annexer au contrat.

LA CYBER-HYGIÈNE : DES RÈGLES SIMPLES ET EFFICACES

POUR COMMENCER : NOMMEZ UN RÉFÉRENT CYBERSÉCURITÉ AU SEIN DU COMITÉ DE DIRECTION

Il sera le relai du dirigeant en matière de cybersécurité, et ce, même si les prestations informatiques sont externalisées. Il aura pour rôle de réaliser l'analyse des risques et de concevoir un plan d'action et d'investissement.

6 RÈGLES
SIMPLES ET EFFICACES
POUR ADOPTER
LA CYBER-HYGIÈNE :

1

Sensibilisez vos collaborateurs

- Menez des actions de sensibilisation avec l'appui de votre comité de direction (diffusion des bonnes pratiques, de documentation, campagnes de prévention, etc.).
- Acculturez et formez vos collaborateurs en leur proposant des formations dédiées.
- Établissez un code de bonne conduite, qui pourra prendre la forme d'une charte informatique et assurez-vous qu'il est bien assimilé par vos collaborateurs. Cette charte sera signée par chaque utilisateur lors de la remise de son matériel.
- Désignez un point de contact cybersécurité parmi vos collaborateurs qui sera l'ambassadeur des bonnes pratiques au sein de votre entreprise.
- Valorisez vos collaborateurs, faites-en les acteurs de votre cyberdéfense.

2

Gérez vos mots de passe

- Pour être efficace, un mot de passe doit être long et complexe. On évitera ceux qui peuvent être devinés facilement (« azerty », « mot de passe », etc.). Privilégiez les « pass phrases », en prenant les initiales des mots d'une phrase.
- Un mot de passe doit être individuel et rester confidentiel. Aucun interlocuteur de confiance ne vous demandera jamais de lui communiquer votre mot de passe par quelque moyen que ce soit même pour une maintenance, un dépannage informatique ou une vérification de sécurité.
- Un mot de passe différent doit être créé pour chaque usage. Ainsi en cas de perte ou de vol d'un de vos mots de passe, seul le service concerné sera vulnérable. Dans le cas contraire, tous les services pour lesquels vous utilisez le même mot de passe compromis seraient impactés.
- Utilisez des gestionnaires ou coffres-forts de mots de passe qui vous aideront à les stocker de manière sécurisée.
- Un mot de passe doit être changé régulièrement, tous les 3 mois. En moyenne pour les services les plus critiques, un renouvellement plus fréquent est à privilégier. Celui-ci peut généralement être imposé automatiquement par certains systèmes (système d'exploitation par exemple).

3

Mettez à jour vos appareils, vos logiciels et vos antivirus

- Vérifiez régulièrement que vos appareils et logiciels ont été mis à jour et que vous utilisez bien les dernières versions disponibles.
- Lorsque votre système d'exploitation est à jour, activez les mises à jour automatiques si votre éditeur le permet.
- Installez uniquement les mises à jour proposées par votre éditeur ou fournisseur, provenant d'une source officielle fiable.
- Privilégiez deux éditeurs d'antivirus différents : un pour vos serveurs et un autre pour vos postes de travail.
- Pour vous aider dans cette action, cartographiez l'ensemble de vos appareils et de vos logiciels ainsi que leur version dans un registre. Des applications d'inventaire existent.

4

Évitez les comportements à risque

- Beaucoup d'attaquants comptent sur la curiosité et la naïveté de leurs victimes. Ainsi n'ouvrez jamais une pièce jointe suspecte ou provenant d'un expéditeur inconnu. Ne connectez jamais une clé USB en apparence abandonnée que vous auriez trouvée dans le parking ou devant l'entrée de l'entreprise car il y a fort à parier qu'elle a été laissée là intentionnellement, bien en évidence, dans l'attente qu'une future victime s'en saisisse.
- Avant de cliquer sur un lien, passez votre souris dessus pour apercevoir le nom de domaine. Ne vous aventurez pas sur des sites douteux.
- Lorsque vous êtes en déplacement, ne vous connectez jamais à un réseau public (cafés, hôtels, aéroports, etc.).
- Séparez les usages personnels et professionnels.

5

Sauvegardez !

- Réalisez des sauvegardes régulières. En cas de vol, de panne, de piratage ou de destruction de vos appareils électroniques, vous perdrez les données enregistrées sur ces supports. Ayez le réflexe de réaliser régulièrement une sauvegarde de vos données. Identifiez les appareils et supports qui contiennent des données puis déterminez celles qui doivent être sauvegardées. Pensez également à sauvegarder les logiciels nécessaires à l'exploitation de vos données.
- Choisissez une solution de sauvegarde adaptée à vos besoins. Déterminez quelles sont les fonctionnalités nécessaires (chiffrement par exemple), l'espace de stockage requis et la facilité d'utilisation de la solution. Sachez qu'il est également possible de réaliser une sauvegarde manuelle de vos fichiers en les copiant sur un disque dur externe en veillant à les chiffrer et à les protéger par un mot de passe.
- Planifiez vos sauvegardes. La plupart des solutions de sauvegarde intègrent une fonctionnalité permettant de planifier la sauvegarde à échéance régulière. Lorsque vous l'activez, elle vous permettra de restaurer vos fichiers dans leur version la plus récente.
- Déconnectez votre support de sauvegarde de votre système d'information. S'il est corrompu, cela évitera que l'infection ne se propage à votre espace de sauvegarde. Avant de restaurer vos données il faudra vous assurer que le système d'information est désinfecté de tout logiciel malveillant.
- Protégez vos sauvegardes. Il est recommandé de conserver vos sauvegardes sur des sites différents de celui qui héberge vos données à sécuriser. Il est plus prudent de ne pas mettre tous ses œufs dans le même panier.
- Testez vos sauvegardes. Assurez-vous régulièrement que vos sauvegardes sont conformes et exploitables. Prévoyez aussi de quelle manière elles seront restaurées le moment venu en faisant des tests de restauration.

6

Mettez en place des garde-fous

- Restreignez les accès Internet uniquement aux sites nécessaires à vos collaborateurs.
- Mettez en place une politique de gestion des droits d'accès (accès informatiques mais aussi accès physiques à vos locaux en particulier pour les entrées et sorties du personnel). Il faut également prévoir une politique de mise à jour et de re-certification de ces droits.
- Sécurisez les accès wifi et utilisez un VPN pour vous connecter à distance lors de vos déplacements.
- Bloquez les ports USB de vos appareils si vous n'en avez pas l'utilité. Cela évitera à la fois d'exposer vos systèmes à une clé infectée et le vol massif de vos données par un collaborateur mal intentionné.
- Mettez en place une authentification forte multi-facteurs (confirmation d'un code reçu par SMS ou par e-mail par exemple).

POUR ALLER PLUS LOIN :
Retrouverez toutes ces bonnes pratiques ainsi que des supports de sensibilisation sur : https://www.cybermalveillance.gouv.fr/bonnes-pratiques

PRÉPAREZ-VOUS AU PIRE

Sans tomber dans le catastrophisme, il faut tout de même envisager les scénarios possibles et leurs impacts pour vous préparer dès à présent à y faire face lorsqu'ils surviendront. « Lorsque » et non pas « si » car en matière de cybersécurité,

la question n'est pas de savoir si vous serez attaqué, mais quand !

Face à une cyberattaque il n'y a qu'un maître mot : résilience !

Définition

La cyber résilience est votre capacité à maintenir une activité à la suite d'une attaque, même de manière dégradée, et à vous rétablir rapidement pour reprendre le cours normal de vos opérations. Pour y parvenir il est indispensable d'établir un plan d'action pour vous préparer en amont et pour réagir face à une cyberattaque.

Une préparation en seulement 3 étapes :

1. **Établir un diagnostic** de votre entreprise est la première étape, il vous permettra d'avoir une vision d'ensemble de la maturité de votre entreprise en matière de cybersécurité.
2. Dans un second temps, il donnera lieu à un **plan d'action pour renforcer la sécurité** de votre entreprise.
3. Enfin, il faudra s'atteler à la **préparation d'un plan de continuité de l'activité** pour pouvoir réagir face à une cyberattaque.

Bpifrance et Cybermalveillance.gouv.fr mettent à votre disposition plusieurs dispositifs pour vous accompagner dans cette démarche.

Autodiag Cybersécurité Bpifrance

Bpifrance met à votre disposition un outil d'autodiagnostic en ligne pour vous permettre d'évaluer le niveau de maturité de votre entreprise en termes de cybersécurité. Simple et pédagogique, il vous permettra d'établir un diagnostic de votre entreprise et d'accéder à de nombreuses ressources en ligne. Il est accessible gratuitement après inscription en ligne.

POUR EN SAVOIR PLUS :
https://mon.bpifrance.fr

Module de Conseil Cybersécurité

Ce module se déroule sur 10 jours avec l'appui d'un consultant spécialisé. Il vous permet de réaliser un état des lieux de votre situation, d'établir un plan de sécurisation de vos systèmes informatiques et de sensibiliser vos collaborateurs aux meilleures pratiques. Pour en bénéficier, contactez votre chargé d'affaires ou l'agence **Bpifrance** dans votre région.

POUR EN SAVOIR PLUS :
Contactez votre chargé d'affaires

Diagnostic Cyber Défense

Pour protéger les entreprises du secteur de la Défense face aux risques numériques, la Direction Générale de l'Armement (DGA) et **Bpifrance** vous proposent un accompagnement sur mesure, par un expert en matière de cybersécurité, et participent au financement de sa prestation. Il est accessible aux PME exerçant des activités liées au secteur de la Défense et ayant obtenu un pré-accord de la DGA.

POUR EN SAVOIR PLUS :
https://www.bpifrance.fr/Toutes-nos-solutions/Accompagnement/Conseil/Diagnostic-Cyber-Defense

Label ExpertCyber

Développé par **Cybermalveillance.gouv.fr,** en partenariat avec les principaux syndicats professionnels du secteur **(Fédération EBEN, Cinov Numérique, Syntec Numérique), la Fédération Française de l'Assurance et le soutien de l'AFNOR,** le label ExpertCyber est destiné à valoriser les professionnels en sécurité numérique qui ont démontré un niveau d'expertise technique et de transparence dans l'accompagnement de leurs clients pour la sécurisation de leurs systèmes d'information et la remédiation de leurs incidents de sécurité.

POUR EN SAVOIR PLUS :
https://www.cybermalveillance.gouv.fr/tous-nos-contenus/label-expertcyber/decouvrir-le-label-expertcyber

04.

...
LES ÉTAPES
À SUIVRE

RÉAGIR FACE À UNE CYBER-ATTAQUE...

Cette partie vous donnera les bons réflexes à adopter pour réagir face à une cyberattaque. Elle détaille les actions à mener dès les premiers instants de l'attaque pour sécuriser, alerter et remédier.

SÉCURISER

Pas de panique ! La soudaineté et l'ampleur d'une cyberattaque peuvent déstabiliser mais quelques actions simples, réalisées dans le calme, vous permettront de désamorcer la situation. Comme lorsqu'on arrive sur un lieu d'accident, la première mesure à prendre est d'éviter que la situation ne s'aggrave.

- Pensez en premier lieu à la sécurité de vos collaborateurs, s'ils évoluent dans un environnement à risque dont les équipements pourraient dysfonctionner (automates industriels, systèmes de ventilation, verrouillage automatique des issues, etc.). Il faut les faire évacuer sans délai.

- Identifiez les équipements infectés et déconnectez-les du système d'information et d'Internet en déconnectant le câble réseau et le wifi pour éviter la propagation de l'attaque.

- N'éteignez pas et ne redémarrez pas les machines infectées car vous risqueriez d'effacer les traces de l'attaque. Ces informations pourront permettre aux enquêteurs de remonter la piste et d'identifier les failles de sécurité exploitées par les attaquants.

- N'entrez pas en contact avec les attaquants et ne donnez pas suite à l'éventuelle demande de rançon.

ALERTER

Une fois la situation figée, il faut donner l'alerte rapidement et prévenir les services compétents.

- Alertez vos collaborateurs et indiquez-leur la procédure à suivre. Ils seront plus à même d'adopter les bons réflexes s'ils ont été formés au préalable.

- Contactez la personne en charge de votre système d'information et expliquez-lui la situation de manière détaillée. Il peut s'agir du DSI (interne ou en temps partagé) ou d'un prestataire informatique. Si vous n'avez pas de contact identifié, **Cybermalveillance.gouv.fr** vous mettra en contact avec un intervenant qualifié à proximité de votre entreprise. Pour vous faire assister en cas de cyberattaque, rendez-vous sur www.cybermalveillance.gouv.fr/diagnostic/accueil

- Si vous suspectez que vos données bancaires ont été exposées, contactez immédiatement votre banque pour suspendre toutes les opérations de transferts.

- Alertez les autorités et déposez plainte car à défaut les cybercriminels pourront poursuivre leurs activités en toute impunité. Il vous suffit de vous rendre au commissariat de police ou à la gendarmerie le plus proche qui vous orienteront vers les services dédiés à la lutte contre la cybercriminalité.

  Vous pouvez également déposer plainte par courrier adressé au Procureur de la République. Tenez à la disposition des enquêteurs tous les éléments recueillis en votre possession ou en cours d'extraction (captures d'écran, traces informatiques et fichiers suspects, documents chiffrés par un logiciel malveillant, numéro de téléphone, e-mails, faux RIB utilisé pour la fraude). Faites-vous assister d'un avocat spécialisé au besoin afin d'identifier les infractions dont vous êtes victime.

- Effectuez votre déclaration de sinistre auprès de votre assureur. Les dommages causés par une cyberattaque sont généralement couverts par les polices d'assurance en responsabilité civile au titre des incidents informatiques mais ce type d'assurance ne protège que les tiers des préjudices résultant de l'attaque sur vos systèmes d'information (clients, fournisseurs, voisinage, etc.).

  Certains assureurs prennent en charge les frais engendrés par les cyberattaques et proposent même des services d'accompagnement par des prestataires qualifiés. Référez-vous à votre contrat d'assurance pour connaître vos droits.

- Si des données personnelles ont été exposées, vous devez avertir la **CNIL** dans un délai de 72h à la suite de la détection de l'incident. Vous avez la possibilité de réaliser cette notification en plusieurs étapes, de manière itérative, si des investigations sont nécessaires pour évaluer l'étendue de l'attaque (https://www.cnil.fr/fr/notifier-une-violation-de-donnees-personnelles). Il vous faudra également informer toutes les personnes dont les données personnelles ont été exposées.

  En outre, si votre entreprise est soumise à une réglementation particulière en matière de sécurité (Opérateur d'Importance Vitale (OIV), Opérateur de Services Essentiels (OSE), Fournisseur de Service Numérique (FSN)), vous avez l'obligation d'en informer l'ANSSI (https://www.ssi.gouv.fr/en-cas-dincident/).

- Enfin, informez les autres parties prenantes que vous jugerez pertinentes (clients, fournisseurs, actionnaires, conseil d'administration) et prévoyez une communication de crise si nécessaire mais en prenant garde aux informations que vous rendrez publiques car les attaquants en auront connaissance.

REMÉDIER ET REPRENDRE L'ACTIVITÉ

En fonction de la criticité de l'attaque et de la complexité de vos systèmes d'information, la remédiation peut durer de quelques heures à quelques semaines.

- Mobilisez une équipe de réponse à la crise et déclenchez votre Plan de Continuité de l'Activité (PCA). Pour être fonctionnel, le PCA doit avoir été testé en amont.

- Appuyez-vous sur votre équipe informatique pour évaluer la situation et organisez des points d'avancement réguliers.

- Avant d'envisager toute reprise d'activité même partielle, il est absolument primordial d'**identifier la source et l'étendue de l'attaque.**

  Trop souvent, les systèmes sont remis en service en supposant l'origine probable de l'attaque sans en avoir la confirmation. Cela se solde souvent par une perte de temps et d'argent car des répliques d'attaques ou une réactivation d'un logiciel malveillant peuvent survenir peu de temps après la remise en production. Seule une investigation minutieuse réalisée par des experts en sécurité informatique permettra d'identifier les failles ou vecteurs d'attaque et d'y apporter les correctifs nécessaires.

- La remise en service doit être progressive de manière à contenir une potentielle récidive, avec une surveillance accrue pour s'assurer que la menace a bien été écartée.

FAITES FACE AUX CYBERATTAQUES EN 3 ÉTAPES

Sécuriser

Figez la situation pour éviter la propagation de l'attaque et l'aggravation de la situation.

Alerter

Signalez la situation à toutes les parties prenantes, en interne comme en externe, et assurer la bonne circulation de l'information.

Remédier et reprendre l'activité

Identifiez avec certitude l'origine de l'attaque avant d'envisager la reprise d'activité.

Ce guide est le fruit de la collaboration entre **Bpifrance** et **Cybermalveillance.gouv.fr**

Membres du comité de relecture :

- **Daniel Demeulenaere,**
  directeur de la Stratégie et du Développement - **Bpifrance ;**
- **Ronan Laratte,**
  responsable Conseil - **Bpifrance ;**
- **Jean-Jacques Latour,**
  responsable Expertise - **Cybermalveillance.gouv.fr ;**
- **Olivier Stassi,**
  directeur Sécurité des Systèmes d'Information - **Bpifrance.**

Rédaction :

- **Guillaume Cali,**
  responsable de Développement - **Bpifrance.**

Remerciements :

Nous adressons nos sincères remerciements aux dirigeants d'entreprises et aux experts en cybersécurité qui ont accepté de partager leur expérience et sans qui la préparation de ce guide n'aurait pas été possible.

SERVIR L'AVENIR

Réf. : 1008-440.

Bpifrance

27-31, avenue du Général Leclerc
94710 Maisons-Alfort Cedex
Tél. : 01 41 79 80 00