LIVRE BLANC

PROGRAMME D'ASSURANCE CYBER

LES BONNES PRATIQUES POUR SÉCURISER LA SANTÉ FINANCIÈRE DE VOTRE ENTREPRISE

Servyr
ASSURANCE ET ENTREPRISE

2020 S'EST RÉVÉLÉE ÊTRE UNE ANNÉE DE TRANSITION POUR LES RISQUES LIÉS À LA CYBER CRIMINALITÉ.

LA PANDÉMIE COVID-19 A ÉPROUVÉ LES SYSTÈMES INFORMATIQUES DES ENTREPRISES, NOTAMMENT AVEC LA MISE EN PLACE MASSIVE DU TÉLÉTRAVAIL. DEVENUES DES CIBLES IDÉALES POUR LES HACKERS, NOMBREUSES D'ENTRE ELLES ONT ÉTÉ VICTIMES L'AN PASSÉ DU BUSINESS DU « HACKING », UNE ORGANISATION À GRANDE ÉCHELLE, BIEN AU-DELÀ DU DARKNET.

AU MÊME TITRE QUE DE NOMBREUX RISQUES AYANT ÉMERGÉ CES 20 DERNIÈRES ANNÉES, IL EST PRIMORDIAL DE PRENDRE CONSCIENCE QUE LES CYBER RISQUES SONT GRANDISSANTS ET DE PLUS EN PLUS MENAÇANTS POUR LES ENTREPRISES DE TOUTE TAILLE. LES COURTIERS DOIVENT DONC ÊTRE EN MESURE DE TROUVER DES SOLUTIONS ADAPTÉES POUR LES EN PROTÉGER.

DU CÔTÉ ASSUREURS, LEURS TEXTES DE GARANTIES ET LEURS TARIFICATIONS SONT EN COURS DE RÉVISION, À LA DEMANDE DE LEURS RÉASSUREURS. ILS INSISTENT ÉGALEMENT SUR LA PRÉVENTION, UN POINT NÉVRALGIQUE SUR LEQUEL LES COURTIERS DOIVENT SENSIBILISER LEURS CLIENTS.

IL EXISTE DEUX MANIÈRES DE SE PROTÉGER CONTRE LA CYBER CRIMINALITÉ.

LA PREMIÈRE REPOSE SUR LE VERROUILLAGE DE SON SYSTÈME INFORMATIQUE ; PARTIRIEZ-VOUS DE CHEZ VOUS EN LAISSANT LA PORTE OUVERTE ? LA DEUXIÈME CONSISTE À SE COUVRIR EN CAS D'ATTAQUE EN FAISANT CONFIANCE À SON COURTIER, SPÉCIALISTE DANS LE DOMAINE, POUR LA MISE EN PLACE DE MOYENS DE PRÉVENTION NÉCESSAIRES POUR ÉVITER D'EN ÊTRE VICTIME.

MAGALY DORIA,
CHARGÉE DE CLIENTÈLE EN RISQUES D'ENTREPRISE

LES CYBERATTAQUES, UN PHÉNOMÈNE GRANDISSANT 1

COMMENT PROTÉGER VOTRE ENTREPRISE DU RISQUE CYBER ? 2

LA MISE EN PLACE D'UN CONTRAT D'ASSURANCE CYBER : SOMMES-NOUS TOUS CONCERNÉS ? 3

CONTRATS D'ASSURANCE CYBER : DÉCRYPTAGE ET EXPLICATIONS 4

LES CYBERATTAQUES

UN PHÉNOMÈNE GRANDISSANT

L'ÉTAT DES LIEUX

Une cyberattaque est un acte malveillant qui vise les systèmes d'information ou les entreprises qui utilisent la technologie et les réseaux, dans le but de voler des données ou modifier, voire détruire un système.

Ce type d'incident informatique peut avoir de graves conséquences sur la protection des données à caractère personnel ou sur la survie économique de la société.

- LA CYBER MALVEILLANCE EST UN PHÉNOMÈNE QUI SE RÉPAND PARTOUT DANS LE MONDE ET QUI GRANDIT, NOTAMMENT DEPUIS LA CRISE LIÉE À LA COVID-19 QUI A ACCENTUÉ LES IMPACTS EN MATIÈRE DE CYBERSÉCURITÉ.

D'après le Gouvernement, « les cybercriminels cherchent à tirer profit de la précipitation et de la baisse de vigilance des personnes directement ou indirectement concernées pour les abuser et qui va se retrouver amplifiée par l'accroissement de l'usage numérique lié aux mesures de confinement. ».

D'après l'entreprise Acronis (solution de sauvegarde des données), les cyberattaques en 2021, viseront surtout les télétravailleurs et les fournisseurs de services gérés.

Certaines recherches suggèrent que le travail à distance est devenu la source de 20 % des incidents de cybersécurité et que les rançongiciels sont en augmentation.

CHIFFRES CLÉS

42 %

DES ENTREPRISES TOUCHÉES PAR DES CYBERATTAQUES EN 2019 SONT DES PME

1,3 M€

EST LE COÛT MOYEN D'UNE CYBERATTAQUE (POUR 15 JOURS D'INTERRUPTION D'ACTIVITÉ)

31 %

DES MULTINATIONALES ONT ÉTÉ VICTIMES D'UN CYBERCRIMINEL AU MOINS UNE FOIS PAR JOUR EN 2020

+ 1 000

ENTREPRISES ONT CONSTATÉ DES FUITES DE DONNÉES PROVOQUÉES PAR UN RANSOMWARE (RANÇONGICIEL) EN 2020

Ces chiffres alarmants mettent en lumière la nécessité de réfléchir à la protection de son entreprise contre les cyberattaques.

À travers ce livre blanc, Servyr vous invite à découvrir les bonnes pratiques pour vous protéger des attaques informatiques auxquelles toute entreprise peut être confrontée.

Que vous soyez une TPE, PME ou une entreprise de plus grande taille, nous sommes tous concernés !

QUELQUES EXEMPLES DE CYBERATTAQUES

JANVIER 2020

LES DONNÉES INTERNES D'ESTÉE LAUDER ONT FUITÉ

Plus de 440 millions de données du Groupe de cosmétique Estée Lauder se sont retrouvées en libre accès au début de l'année 2020.

Ces données ne concernaient pas les clients de la marque mais des informations internes à l'entreprise telles que des audits, rapports, adresses mails professionnelles, etc. Le cyber incident en est resté là. Mais l'attaque aurait pu avoir de graves conséquences indirectes en affectant notamment la réputation du Groupe.

Selon un rapport d'Hiscox Assurances France sur la gestion des cyber risques, publié en décembre 2020, de nombreuses entreprises victimes de cyberattaques ont constaté une perte de confiance auprès de leurs prospects (15 %), de leurs clients (11 %) mais également de leurs partenaires commerciaux (12 %).

MAI 2020

EASYJET SE FAIT HACKER LES DONNÉES PERSONNELLES DE SES CLIENTS

En mai 2020, lors du premier confinement lié à la crise sanitaire du COVID-19, Easyjet, compagnie aérienne britannique, a subi une attaque informatique. Les hackers ont eu accès aux informations personnelles de 9 millions de clients à travers le monde. Les pirates informatiques ont obtenu des adresses électroniques et détails de voyage, ainsi que les données des cartes de crédit de plus de 2 000 passagers.

Easyjet a réussi à faire preuve de réactivité et a pu entrer rapidement en contact avec les clients concernés pour les tenir informés des mesures de protection à suivre.

« Depuis que nous avons pris conscience de l'incident, nous avons compris qu'en raison du Covid-19 il y a de fortes craintes sur l'utilisation de données personnelles pour des arnaques en ligne. », a déclaré Johan Lundgren, Directeur Général du Groupe.

JUIN 2020

L'UNIVERSITÉ DE CALIFORNIE À SAN FRANCISCO EST CONTRAINTE DE VERSER UNE RANÇON

La célèbre Université UCSF située à San Francisco a été victime d'un ransomware paralysant l'accès aux données de son réseau informatique.

Les spécialistes informatiques de l'établissement n'ont pas été en mesure de stopper à temps la propagation du virus dans leurs systèmes d'information, malgré leur réactivité et la déconnexion des ordinateurs. L'Université a finalement dû se résoudre à payer une rançon d'environ un million d'euros.

En 2019, 18% des entreprises françaises ont déclaré avoir payé une rançon à la suite d'une cyberattaque.

SEPTEMBRE 2020

CMA CGM SUBIT SA SECONDE CYBERATTAQUE DE L'ANNÉE

En l'espace de six mois, la compagnie de transport maritime CMA CGM a subit deux cyberattaques dont l'une en septembre liée à l'intrusion d'un logiciel malveillant. Celle-ci visait les serveurs périphériques du Groupe.

Immédiatement alertés par la faille, les services de la compagnie ont suspendu tous les accès externes pour éviter la propagation du virus informatique.

Une demande de rançon a été émise par le hacker, l'enquête est toujours en cours. Une attaque peut donc toucher deux fois la même entreprise à quelques mois d'intervalle.

Pourtant, seulement un tiers des entreprises déclarent effectuer une évaluation régulière de la sécurité à la suite d'une cyberattaque et 26 % adoptent de nouvelles exigences en matière de cyber protection.

DÉCEMBRE 2020

L'ÉDITEUR SOLARWINDS EST VICTIME D'UNE CYBERATTAQUE MONDIALE

La mise à jour du logiciel Orion, logiciel de surveillance réseau et informatique, de l'éditeur américain SolarWinds contenait un cheval de Troie.

Près de 18 000 clients, en installant la mise à jour compromise, sont devenus victimes de cette attaque.

Aux États-Unis, l'intrusion a donné accès aux systèmes de plus de 250 administrations, ministères (dont le Pentagone et la NNSA, qui gère l'arsenal nucléaire du pays) et grandes entreprises (Intel, Cisco, Nvidia, ou Microsoft). Depuis début janvier 2021, il apparaît que de nombreux pays sont en réalité concernés, au Moyen-Orient, en Asie et en Europe.

Compte-tenu de l'ampleur du phénomène, qualifié de « cyberattaque historique », certains assureurs cyber refusent de garantir les entreprises utilisatrices du logiciel Orion, ou conditionnent la mise en place de la garantie.

FOCUS

RÈGLEMENT GÉNÉRAL SUR LA PROTECTION DES DONNÉES (RGPD)

ENTRÉ EN VIGUEUR EN MAI 2018, CE RÈGLEMENT EUROPÉEN RELATIF À LA PROTECTION DES DONNÉES A POUR OBJECTIFS DE RENFORCER LE DROIT DES PERSONNES ET DE RESPONSABILISER LES ACTEURS TRAITANT DES DONNÉES, QU'ILS SOIENT DIRECTEMENT RESPONSABLES OU SOUS-TRAITANTS.

EN FRANCE, LA COMMISSION NATIONALE DE L'INFORMATIQUE ET DES LIBERTÉS (CNIL), CRÉÉE EN 1978 PAR LA LOI INFORMATIQUE ET LIBERTÉS, SE CHARGE DE LA PROTECTION DES DONNÉES PERSONNELLES DES FICHIERS ET TRAITEMENTS INFORMATIQUES OU PAPIER, QU'ILS SOIENT PUBLICS OU PRIVÉS. CETTE RÈGLE REND LES ENTREPRISES RESPONSABLES DES DONNÉES PERSONNELLES QU'ELLES DÉTIENNENT ET PRÉVOIT DES AMENDES « PROPORTIONNÉES ET DISSUASIVES » (CHAPITRE VIII, ARTICLE 83 DU RÈGLEMENT (UE) 2016/679 DU PARLEMENT EUROPÉEN ET DU CONSEIL DU 27 AVRIL 2016) POUVANT ATTEINDRE 4 % DE LEUR CHIFFRE D'AFFAIRES EN CAS DE VOL OU DE COMPROMISSION. LES ENTREPRISES SUPPORTENT DÉSORMAIS UNE OBLIGATION DE NOTIFICATION SI UNE VIOLATION DES DONNÉES PERSONNELLES SURVIENT.

QUELLES SONT LES CONSÉQUENCES DE CETTE NOUVELLE RÉGLEMENTATION ?

AU-DELÀ DE L'ASPECT ORGANISATIONNEL, L'IMPACT POUR LES ENTREPRISES EST FINANCIER. UN EXEMPLE : L'ENSEIGNE DARTY

EN 2017, LA CNIL A RELEVÉ UNE RÉELLE DÉFAILLANCE DE SÉCURITÉ PERMETTANT D'ACCÉDER LIBREMENT À L'ENSEMBLE DES DONNÉES RENSEIGNÉES PAR LES CLIENTS DE LA SOCIÉTÉ VIA UN FORMULAIRE EN LIGNE DE DEMANDE DE SERVICE APRÈS-VENTE : 912 938 FICHES ÉTAIENT POTENTIELLEMENT ACCESSIBLES, AVEC DES NOMS, DES PRÉNOMS, DES ADRESSES POSTALES, DES ADRESSES DE MESSAGERIE ÉLECTRONIQUE ET DES COMMANDES.

EN TANT QUE RESPONSABLE DE TRAITEMENT, L'ENSEIGNE AURAIT DÛ REMÉDIER À LA SITUATION, MÊME EN CAS DE RECOURS À UN SOUS-TRAITANT, PUISQU'EN SA QUALITÉ DE « RESPONSABLE DE TRAITEMENT », L'ENSEIGNE AVAIT L'OBLIGATION DE S'ASSURER ET DE VÉRIFIER QUE L'OUTIL DÉVELOPPÉ PAR SON SOUS-TRAITANT RÉPONDAIT À L'OBLIGATION DE CONFIDENTIALITÉ ÉNONCÉE À L'ARTICLE 34 DE LA LOI INFORMATIQUE ET LIBERTÉS.

À LA SUITE DE CES CONSTATATIONS, ELLE A ÉCOPÉ, DÉBUT 2018, D'UNE SANCTION ADMINISTRATIVE À HAUTEUR DE 100 000 € POUR NE PAS AVOIR SUFFISAMMENT SÉCURISÉ LES DONNÉES DE SES CLIENTS.

AUJOURD'HUI, AVEC L'ENTRÉE EN VIGUEUR DU RGPD, LA SANCTION REPRÉSENTERAIT 4 MILLIONS D'EUROS MINIMUM, POUVANT ATTEINDRE JUSQU'À 19 MILLIONS D'EUROS.

FAQ - LES RÉPONSES À VOS QUESTIONS

QU'EST-CE QU'UNE DONNÉE PERSONNELLE ?

Selon l'article 2 de la loi n° 78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés, une donnée à caractère personnel représente toute information à propos d'une personne physique identifiée ou qui peut être identifiée, directement ou indirectement, à l'aide d'un numéro d'identification ou d'un ou plusieurs éléments qui lui sont propres.

QUELLES SONT LES CYBERATTAQUES LES PLUS FRÉQUENTES ?

Les dénis de service, les crypto logiciels, les rançongiciels ainsi que les logiciels malveillants sont les moyens les plus fréquents d'attaque informatique.

QU'EST-CE QU'UN DÉNI DE SERVICE ?

Une attaque par déni de service, ou attaque par déni de service distribué, consiste à saturer les capacités de traitement d'un système d'information ou d'un site internet à partir d'autres machines infectées afin de le rendre incapable de répondre aux requêtes des utilisateurs.

QU'EST-CE QU'UN CRYPTO LOGICIEL OU RANÇONGICIEL ?

Un crypto logiciel, un rançongiciel ou encore un ransomware, sont des programmes malveillants qui cryptent, qui codent des données d'un système d'information. La clé de décryptage est le plus souvent transmise après paiement d'une somme sous forme virtuelle (telle que les bitcoins).

QU'EST-CE QU'UN LOGICIEL MALVEILLANT ?

Un logiciel malveillant est un programme qui affecte le fonctionnement d'un système d'information. Ils sont également appelés « virus », « vers », « chevaux de Troie », etc.

MON ENTREPRISE EST-ELLE TOTALEMENT PROTÉGÉE SI MON ENVIRONNEMENT BUREAUTIQUE EST SÉCURISÉ ?

Non, pas totalement. Selon les cibles visées, les pirates de l'informatique, ou « hackers » en anglais, peuvent aussi s'attaquer à votre informatique de gestion, telle que la comptabilité ou les fichiers du personnel, à votre informatique de process, comme les automates, mais également à vos installations de sécurité et de sûreté.

LE WIFI, LE BLUETOOTH OU LES OBJETS CONNECTÉS REPRÉSENTENT-ILS UN RISQUE ?

Oui, ce sont des failles exploitables.

Vos données entrantes et sortantes de votre système d'information sont très facilement accessibles, via le wifi ou le bluetooth, si elles ne sont pas cryptées de manière suffisamment sécurisée. Les objets connectés, quant à eux, multiplient les voies d'accès aux données et aux systèmes d'information de votre entreprise. Ce sont donc des failles que les pirates de l'informatique sont susceptibles d'exploiter.

QU'EST-CE QUE LE «BYOD» ? QUELS SONT LES RISQUES LIÉS À SON UTILISATION ?

« Bring Your Own Device », ou « BYOD », signifie en français « apportez vos appareils personnels » afin de les utiliser à des fins professionnelles. La sphère personnelle, présumée bien moins protégée et hors du contrôle de l'entreprise, mélangée au cadre professionnel multiplie les risques d'incidents informatiques. Les moyens d'accès aux données et aux systèmes d'information de votre entreprise, et donc les failles exploitables par des pirates de l'informatique, se multiplient à la suite de l'utilisation de « BYOD ».

LE CLOUD REPRÉSENTE-T-IL UN RISQUE ?

Oui. L'exploitation de systèmes d'information distants par l'intermédiaire d'un réseau, notamment interne, se traduit par l'hébergement de données à distance. Cette externalisation peut compromettre la maîtrise de données ou de tâches. Les risques de cette démarche doivent être analysés par votre entreprise. Une réflexion doit également être menée sur les conditions et les outils essentiels pour garantir la sécurité de ce service fourni par une entreprise prestataire.

COMMENT LA CYBERCRIMINALITÉ EST-ELLE JURIDIQUEMENT PUNIE ?

En France, un ensemble d'articles qualifie les infractions spécifiques aux technologies de l'information et de la communication, notamment :

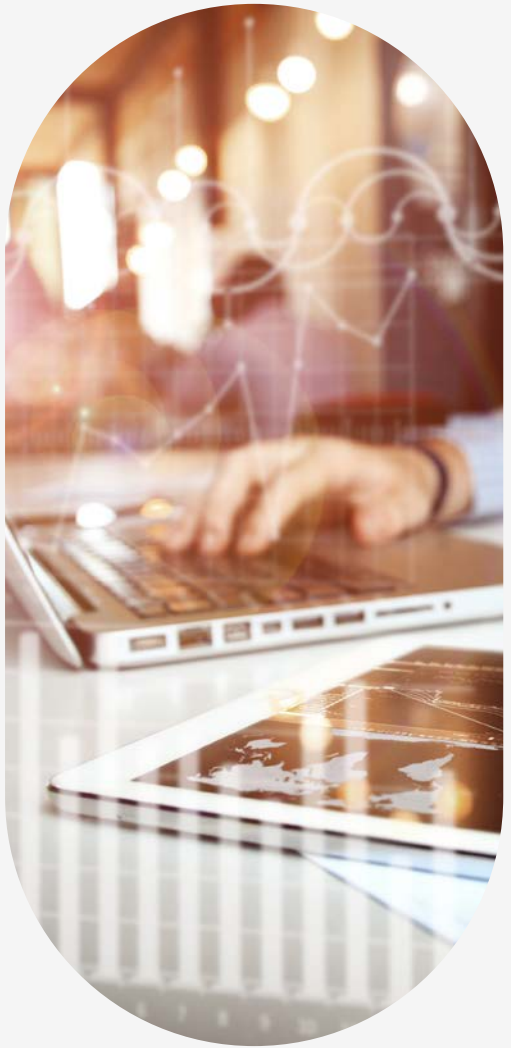
- Les articles 323-1 à 323-7 du Code Pénal concernant les atteintes aux systèmes de traitement automatisé de données (accès ou maintien frauduleux, entrave au fonctionnement, détention de matériel ou logiciel spécifique, groupement formé ou entente établie)
- Les articles 226-16 à 226-20 du Code Pénal à propos des infractions à la loi n°78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés (collecte frauduleuse, traitement de données à caractère personnel, usurpation d'identité numérique)
- Les articles L163-3 à L163-12 du Code Monétaire et Financier concernent les infractions aux cartes bancaires (contrefaçon, falsification de moyens de paiement, détention de matériel ou logiciel spécifique)
- L'article 434-15-2 du Code Pénal relatif aux infractions au chiffrement (refus de remettre une clé de déchiffrement ou de la mettre en œuvre)
- Et les articles 226-1 à 226-4 du Code Pénal sur la violation de la vie privée par captation via un dispositif technique, la divulgation publique d'un enregistrement privé, la conception, l'importation, la location, la détention et l'offre d'outils de captation de la vie privée et des correspondances.

QU'EST-CE QUE L'ANSSI ?

L'ANSSI est l'acronyme pour l'Agence Nationale de la Sécurité des Systèmes d'Information. Créée en 2009, c'est l'autorité nationale pour la sécurité et la défense des systèmes d'information en France. Elle aide également les administrations, les acteurs économiques et le grand public dans la transition numérique. Aussi, elle se charge de la promotion des technologies, des systèmes et des savoir-faire français en France et en Europe.

QU'EST-CE QUE LA CNIL ?

La Commission nationale de l'Informatique et des Libertés, ou CNIL, a été créée en 1978 par la loi n° 78-17 relative à l'informatique, aux fichiers et aux libertés afin de contrôler l'utilisation des données personnelles. Elle doit s'assurer, en tant qu'autorité administrative indépendante, de la protection et de la bonne gestion des données personnelles tout en accompagnant les entreprises et particuliers lors de l'utilisation des nouvelles technologies. La CNIL travaille main dans la main avec ses homologues européens du G29 et internationaux afin d'harmoniser la régulation du traitement des données personnelles.



COMMENT PROTÉGER VOTRE ENTREPRISE

DU RISQUE CYBER ?

LES 3 POINTS CLÉS

L'ANALYSE DE VOTRE EXPOSITION À CES NOUVEAUX RISQUES AINSI QUE LA MISE EN PLACE D'UNE POLITIQUE DE PRÉVENTION SONT LES PREMIÈRES DÉMARCHES À RÉALISER AVANT DE TRANSMETTRE LE RISQUE À VOTRE ASSUREUR. UNE PERSONNE AU SEIN DE VOTRE ENTREPRISE, CLAIREMENT IDENTIFIÉE, DOIT ÊTRE EN CHARGE DE LA MISE EN PLACE ET DU SUIVI DE CETTE POLITIQUE DE MANAGEMENT DE CYBER RISQUE.

1 DES FACTEURS HUMAINS ET ORGANISATIONNELS

SENSIBILISER SES COLLABORATEURS ET PARTIES PRENANTES

Il est nécessaire de sensibiliser et de former vos collaborateurs aux bons réflexes contre les risques cyber, tout comme vos sous-traitants et vos prestataires afin d'éviter qu'ils deviennent la faille de votre protection cyber.

N'hésitez pas à régulièrement leur rappeler ces règles simples mais primordiales :

- NE PAS UTILISER DES APPAREILS PERSONNELS comme des clefs USB ou des disques durs externes ou des accès distants non sécurisés (Wifi ou Bluetooth).
- NE PAS DIVULGUER SON MOT DE PASSE.
- METTRE EN PLACE DES RÈGLES pour la consultation des mails ou pièces jointes douteux tels que les liens hypertextes ou inexplicables, les extensions .pif, .com, .exe, .bat ou .lnk.

LIMITER LA CRÉATION DE FAILLES

La mise en place d'une véritable politique de gestion des droits adaptée à la situation de votre entreprise est nécessaire à sa protection. Vos mots de passe se doivent d'être individualisés, secrets, complexes (tel que 8 caractères avec des majuscules, des minuscules et des caractères spéciaux, par exemple) et modifiés régulièrement afin d'éviter leur usurpation.

Vos logiciels sont également des accès pour des intrusions malveillantes. Leur mise à jour est donc essentielle pour limiter la création de failles.

2 DES OUTILS DE PROTECTION

PROTÉGER VIA DES OUTILS ADAPTÉS

La mise en place d'outils adaptés à votre activité permet également de protéger au mieux votre entreprise.

- LES ANTI-VIRUS, OU PARE-FEUX, SONT INDISPENSABLES pour la protection de votre système d'information. Ils doivent être régulièrement et automatiquement mis à jour.
- L'ANTI-VIRUS PEUT ÊTRE COMPLÉTÉ par des outils de filtrage de type « Intrusion Détection Système » (IDS) et « Intrusion Protection Système » (IPS) qui sondent les entrées et sorties dans le but d'écarter une intrusion malveillante.

Enfin, des outils de détection comportementale peuvent vous aider à détecter d'autres intrusions malveillantes que les outils de surveillance n'arrêteraient pas.

- LES TÉLÉCHARGEMENTS QUI ONT FRANCHI L'ANTI-VIRUS SONT ANALYSÉS AFIN DE DÉCELER CEUX QUI AGISSENT DE MANIÈRE SUSPECTE, COMME, PAR EXEMPLE, LES LOGICIELS QUI INTERROGENT UN NOMBRE IMPORTANT DE RÉPERTOIRES DE L'ORDINATEUR, LES « CRYPTO LOGICIELS ».

3 DES OUTILS DE RÉSILIENCE, POUR UNE ANTICIPATION DE LA GESTION DE CRISE

ANTICIPER AVEC UNE MÉTHODE ÉPROUVÉE

Afin que votre entreprise reprenne rapidement son activité après une attaque, vous devez anticiper.

1. LA SAUVEGARDE DE VOS DONNÉES

- Sauvegarder régulièrement vos données sur des supports et systèmes distincts de votre système d'information, c'est-à-dire un site différent de celui hébergeant déjà vos systèmes et données.
- Tester, au moins une fois par an, les restaurations afin qu'elles soient opérationnelles.

Ces sauvegardes de vos systèmes d'exploitation et progiciels doivent suivre les recommandations des sites éditeurs ainsi que celles de vos prestataires informatiques.

2. LE PLAN DE CONTINUITÉ D'ACTIVITÉ

- Rendre vos données, systèmes d'exploitation et applications critiques confidentielles ou personnelles.
- Réfléchir à une procédure de gestion de crise en cas d'intrusion malveillante.
- Identifier des collaborateurs (responsables, experts et communicants) mobilisables sans délai à tout instant, qui seront chargés de mettre en place les mesures d'urgences nécessaires afin d'assurer la continuité ou la reprise de l'activité de votre entreprise.

QUE FAIRE EN CAS D'INCIDENT ?

1 VIS-À-VIS DES POUVOIRS PUBLICS

PORTER PLAINTE

Toute cyberattaque représente une infraction aux technologies de l'information et de la communication définies par le Code Pénal et le Code Monétaire et Financier.

Vous devez déposer une plainte au plus vite auprès du service territorial de police ou de gendarmerie le plus proche de l'entreprise ou par courrier auprès du procureur de la République du Tribunal de Grande Instance de votre ressort géographique.

En tant qu'entreprise victime d'une attaque ou d'une suspicion d'attaque informatique, vous devez relever des preuves numériques de l'incident à l'aide de constatations techniques. Un spécialiste en cybercriminalité, nommé par les services de police, peut venir compléter vos observations lors de l'enquête.

NOTIFIER L'INCIDENT

EN CAS DE VIOLATION DE DONNÉES PERSONNELLES

Selon l'article 34 bis de la loi n° 78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés, les fournisseurs de services de communications électroniques sont dans l'obligation de notifier l'incident à la Commission Nationale de l'Informatique et des Libertés (CNIL). En cas de risque d'atteinte aux données personnelles ou à la vie privée, le(s) intéressé(s) doivent être averti(s).

Depuis mai 2018, les entreprises ayant des activités de traitement de données personnelles sont également concernées par cette obligation de notification à l'autorité compétente et aux intéressés.

EN CAS D'ATTEINTE AU SYSTÈME D'INFORMATION

Selon l'article 22 de la loi n° 2013-1168 du 18 décembre 2013 relative à la programmation militaire pour les années 2014 à 2019, le Premier Ministre et l'Agence Nationale de la Sécurité des Systèmes d'Information (ANSSI) doivent être informés de l'incident informatique pour les opérateurs d'importance vitale.

À la suite de la directive européenne 2016/1148, relative à la sécurité des réseaux et des systèmes d'information dans l'Union Européenne (SRI), les entreprises dites « d'opérateur de services essentiels » ou de « fournisseur de services numériques » sont aussi concernées par l'obligation de notification à l'autorité compétente.

2 VIS-À-VIS DE VOTRE ASSUREUR

Contactez votre assureur et/ou courtier au plus vite afin d'être accompagné face aux risques informatiques. Informez votre interlocuteur dédié avant toute décision qui pourrait impacter les conséquences de l'incident et la gestion de votre déclaration de sinistre.

LA MISE EN PLACE D'UN CONTRAT D'ASSURANCE CYBER :

SOMMES-NOUS TOUS CONCERNÉS ?

COMPRENDRE LES PROBLÉMATIQUES POUR DÉFINIR SON BESOIN

Les programmes d'assurance cyber font partie d'un processus global de maîtrise du risque cyber : la cyber résilience s'inscrit dans un panorama plus global de gouvernance impliquant des décisions managériales, techniques, comportementales, gouvernementales.

Il est donc nécessaire de définir ce processus en s'appuyant notamment sur les principaux enjeux de l'entreprise :

- Préservation des intérêts de l'entreprise (sécurisation financière, intérêts économiques, conformité règlementaire).
- Maîtrise de l'image de l'entreprise.
- Globalisation de la gestion du risque cyber.

Le tableau qui suit constitue un outil d'aide à la décision qui vous permettra de déterminer la nécessité de mise en place d'un programme d'assurance cyber et d'évaluer votre degré de maturité à ce sujet.

ENJEUX	QUESTION	RÉPONSE OUI	RÉPONSE NON
PRÉSERVATION DES INTÉRÊTS DE L'ENTREPRISE (sécurisation financière, intérêts économiques, respect des valeurs éthiques et conformité règlementaire)	Une impossibilité d'accès à vos systèmes d'information peut-elle affecter le fonctionnement de l'entreprise dans sa globalité ?	3	0
	Possédez-vous des données confidentielles ? (clients, collaborateurs, fournisseurs)	3	0
	Les données informatiques sont-elles stratégiques au sein de l'entreprise ?	3	0
MAÎTRISE DE L'IMAGE DE L'ENTREPRISE	La fuite de données informatiques peut-elle entraîner une perte de confiance des fournisseurs, clients, actionnaires ou toute autre partie prenante ?	2	0
	Pensez-vous qu'une attaque cyber puisse porter atteinte à la réputation de l'entreprise ?	3	0
GLOBALISATION DE LA GESTION DU RISQUE CYBER	Avez-vous ou envisagez-vous la mise en place d'une politique globale de prévention des risques ?	2	0
	Une analyse de vulnérabilité de l'entreprise est-elle devenue essentielle ?	3	0
	Envisagez-vous la mise en place d'outils de transfert de risques de l'entreprise ?	2	0
	Avant de lire ce livre blanc, étiez-vous en mesure de définir précisément la notion de risque cyber ?	2	0

INTERPRÉTATION DES RÉSULTATS

MOINS DE 7

Les enjeux relevés sont essentiels pour vous et nécessitent un accompagnement particulier en ce qui concerne la gestion de vos risques, notamment en matière de conseils.

La mise en place d'un processus global de cyber résilience est vraisemblablement prématurée. Des solutions plus simples et adaptées peuvent être mises en place.

ENTRE 7 ET 18

Vous êtes à mi-chemin de votre réflexion concernant la globalisation de la gestion du risque cyber.

Un programme d'assurance global pourrait répondre à la plupart de vos besoins essentiels et prioritaires ; il faudra cependant rester attentif au degré de maturité de l'ensemble des parties prenantes de votre entreprise.

Vos choix en matière d'assureur et intermédiaires seront déterminants pour la réussite de votre projet.

PLUS DE 18

Vos besoins en matière de cyber résilience sont importants et nécessitent une analyse approfondie de la nature du programme à mettre en place.

Votre maturité à ce sujet est évidente, ce qui vous permettra de vous orienter plus librement vers un programme global de gestion de vos risques.

Des montages plus complexes peuvent également être envisagés.

CONTRATS D'ASSURANCE CYBER :

DÉCRYPTAGE ET EXPLICATIONS

LA MISE EN PLACE

UN CONTRAT D'ASSURANCE CYBER PRÉSENTE DE NOMBREUX AVANTAGES POUR L'ENTREPRISE.

SÉCURITÉ FINANCIÈRE

Tout d'abord, il s'agit d'un outil de transfert de risques, qui sécurise financièrement l'entreprise. Même si le risque zéro n'existe pas, la mise en place d'une police d'assurance cyber permet de limiter l'exposition financière de l'entreprise en cas d'attaque.

EXPOSITION

Le processus de mise en place d'un contrat d'assurance cyber nécessite la réalisation d'une cartographie des risques au sein de l'entreprise. Cette démarche est un réel atout pour l'entreprise qui lui permet d'identifier clairement et de façon plus globale les risques auxquels elle est exposée, mais également d'évaluer quels risques peuvent être transférés à l'assurance et de construire avec des experts leur(s) plan(s) de continuité d'activité (PCA) en cas de sinistre.

COUVERTURE ADAPTÉE

Le risque cyber est complexe et protéiforme, le contrat d'assurance doit donc disposer de plusieurs volets pour couvrir au mieux ses diverses typologies et ses diverses conséquences.

Il doit permettre d'assurer les dommages subis par les tiers et les dommages subis par les entreprises assurées, tout en fournissant à l'entreprise assurée des prestations d'assistance et de gestion de crise.

Le volet assurance comprend trois parties :

- UN MODULE D'ASSISTANCE, qui fait intervenir des experts cyber et des experts en communication de crise
- LA PRISE EN CHARGE DES COÛTS DIRECTS : les opérations, les pertes d'exploitation et de chiffre d'affaires
- LES DOMMAGES AUX TIERS

ZOOM SUR LES GARANTIES PROPOSÉES

DOMMAGES

Les garanties dommages couvrent les pertes de l'assuré à la suite du sinistre, en dehors de toute réclamation de tiers : frais de restauration de données et de remise en état du système d'information, les frais de notification, les frais de surveillance, les frais d'enquêtes et de sanctions administratives, les frais de cyber extorsion et les pertes de revenus consécutives au sinistre.

FOCUS SUR LES FRAIS DE SURVEILLANCE (MONITORING) ET DE NOTIFICATION

En cas de vol ou d'atteinte des données bancaires, l'assureur prend en charge les frais de monitoring liés à la surveillance du marché en cas de revente et/ou utilisation frauduleuse de ces données.

Les entreprises sont également soumises à une obligation de notification qui s'applique en cas de violation de données à caractère personnel, sur la base du Règlement Général européen sur la Protection des Données à caractère personnel effectif depuis le 25 mai 2018. Le coût moyen est estimé à 7€/notification (l'estimation inclut les frais d'investigation informatiques, les frais de notification, mise en place d'une cellule de relation client, experts juridiques). Les frais de notification sont également pris en charge au titre contrat cyber.

Le manquement à l'obligation de notifier peut également engager la responsabilité du responsable de traitement, qui devra être couverte par le volet de responsabilité civile du contrat cyber.

RESPONSABILITÉ CIVILE

Ce volet garantit les conséquences financières et les frais de défense de l'assuré résultant de réclamations de tiers pour atteinte à des données ou systèmes d'information.

Il existe de nombreuses formes de dommages subis par les tiers : contamination du système d'information par la transmission par l'assuré d'un fichier infecté d'un virus, déni de service du fait de l'inaccessibilité des services de l'assuré, violation du droit fondamental au respect de la vie ou des obligations de confidentialité, de transparence et de durée de conservation, contenu d'un site Internet.

GESTION DE CRISE

En cas de cyberattaque, c'est une course contre la montre qui se joue et la mise à disposition auprès de l'entreprise assurée par l'assureur d'un réseau de partenaires experts en gestion de crise (experts informatiques, relations publiques et communication, juridique) constitue un réel atout pour l'entreprise.

Le volet gestion de crise intègre la prise en charge des frais de recherche de la cause du sinistre et de rétablissement du système d'information, des frais de communication et de relations publiques, de restauration des données et de notification et/ou monitoring.

FOCUS

TOUS RISQUES INFORMATIQUES, FRAUDE ET CYBER : LE TRIO GAGNANT

UNE ASSURANCE TOUS RISQUES INFORMATIQUE (TRI) COUVRE UNIQUEMENT LES DOMMAGES MATÉRIELS SUBIS PAR LES ÉQUIPEMENTS INFORMATIQUES À LA SUITE D'UN INCENDIE, UNE EXPLOSION, UN DÉGÂT DES EAUX OU DES DOMMAGES ÉLECTRIQUES. CETTE GARANTIE EST DONC COMPLÉMENTAIRE AU CONTRAT CYBER, QUI RAPPELONS-LE, N'INTERVIENT QU'EN CAS D'ATTAQUE CYBER ET EN DEHORS DE TOUT DOMMAGE MATÉRIEL AU PARC INFORMATIQUE.

LA FRAUDE EST UN ACTE INTENTIONNEL RÉALISÉ PAR UN SALARIÉ OU UN TIERS DE FAÇON ILLICITE POUR EN RETIRER UN AVANTAGE FINANCIER. ELLE PEUT REVÊTIR DE NOMBREUSES FORMES : USURPATION D'IDENTITÉ, ARNAQUE AU FAUX PRÉSIDENT, ESCROQUERIE, ABUS DE CONFIANCE…

LA CYBER CRIMINALITÉ EST UNE FORME DE FRAUDE, PAR INTRUSION DANS LES SYSTÈMES D'INFORMATION DANS L'ENTREPRISE. SI LE CONTRAT D'ASSURANCE FRAUDE GARANTIT LES PERTES PÉCUNIAIRES DIRECTES ET FRAIS SUPPLÉMENTAIRES D'EXPLOITATION EN CAS DE FRAUDE, IL N'INTERVIENDRA AU TITRE D'UNE FRAUDE INFORMATIQUE QUE DE FAÇON LIMITÉE, QUE CE SOIT EN MATIÈRE D'ORIGINE DU SINISTRE OU DES MONTANTS D'INDEMNISATION.

LES CONTRATS D'ASSURANCE COMBINÉS CYBER ET FRAUDE N'OFFRENT PAS DE GARANTIES AUSSI ÉTENDUES QUE LA SOUSCRIPTION DE DEUX CONTRATS D'ASSURANCE DISTINCTS, DONT LES MONTANTS DE GARANTIES SERONT D'AILLEURS BIEN PLUS IMPORTANTS.

4 RAISONS DE SOUSCRIRE À UN CONTRAT CYBER

1 SE PROTÉGER
DES CONSÉQUENCES FINANCIÈRES

Les contrats Responsabilité Civile et Dommages classiques ne garantissent pas les conséquences financières d'un sinistre lié à un acte de malveillance ou à une erreur humaine. Le risque de fraude n'est pas couvert également.

Une protection supplémentaire est donc nécessaire pour vous protéger de toutes conséquences financières d'un incident informatique.

2 SÉCURISER
L' ACTIVITÉ DE VOTRE ENTREPRISE

La sécurisation de votre activité en cas d'attaque est un enjeu majeur pour votre entreprise. En effet, lors des premiers mois de l'année 2019, les cyberattaques ont causé une perte financière de 327 797 € en France.

Se protéger face aux incidents informatiques est vital pour le futur économique de votre entreprise.

3 ANTICIPER
LES RISQUES LIÉS À LA NOUVELLE RÉGLEMENTATION

Entré en vigueur en mai 2018, le RGPD, mis en application par la CNIL, renforce le droit des personnes et responsabilise les acteurs traitant des données personnelles.

Cette règle rend les entreprises responsables des données à caractère privé qu'elles détiennent et prévoit des amendes pouvant atteindre 4 % de leur chiffre d'affaires en cas de manquement.

4 METTRE EN PLACE
UNE PROCÉDURE DE GESTION DE CRISE

L'accompagnement et la coordination des prestataires experts dans leur domaine en cas de crise sont indispensables à la bonne gestion d'une attaque.

Il est fortement conseillé de mettre en place une procédure de gestion de crise en cas d'incident informatique afin d'assurer la continuité de l'activité de votre entreprise.

CONCLUSION

SERVYR VOUS ACCOMPAGNE DANS L'ANALYSE DE VOS RISQUES, LA MISE EN PLACE ET LA GESTION DE VOS PROGRAMMES D'ASSURANCE CYBER

La souscription d'un contrat d'assurance cyber permet aux entreprises de limiter l'impact financier en cas d'attaque et de disposer d'un accompagnement de partenaires experts pour affronter la crise.

SERVYR A DÉVELOPPÉ UNE OFFRE PACKAGÉE COMPRENANT 3 VOLETS

GESTION DE CRISE

- Avec un accompagnement de consultants spécialisés en cas d'attaque

DOMMAGES

- Pour la prise en charge des pertes d'exploitation, des frais de notification, des sanctions légalement assurables et des frais de défense

RESPONSABILITÉ CIVILE

- Pour indemniser les réclamations des tiers à la suite d'une atteinte aux données personnelles ou à un manquement à l'obligation de notification

POUR ALLER PLUS LOIN...

Servyr peut vous mettre en relation avec un prestataire référencé par le site cyber malveillance du gouvernement (https://www.cybermalveillance.gouv.fr/), qui pourra vous proposer la réalisation d'un audit identifiant les principales menaces pour votre entreprise.

Afin de vous accompagner dans l'évolution de vos besoins, les équipes de Servyr sont à votre disposition pour répondre aux questions que vous pourriez vous poser et vous accompagner dans la mise en place des outils de transfert de risque.

SERVYR
EST

3 rue Clément Ader
CS 60005
51688 Reims Cedex 2
T. : +33 (0)3 26 48 49 50

SERVYR
NORD

Parc de la Haute Borne
2-6 avenue de l'Horizon - bât 6
59650 Villeneuve d'Ascq
T. : +33 (0)3 21 78 13 00

SERVYR
ÎLE-DE-FRANCE

43-45 rue de Naples
75008 Paris
T. : +33 (0)1 45 62 20 90

SERVYR
INTERNATIONAL

6-8 rue Léon Trulin
59800 Lille
T. : +33 (0)3 21 14 21 20

Servyr
ASSURANCE ET ENTREPRISE

www.servyr.com Servyr Servyr_courtage