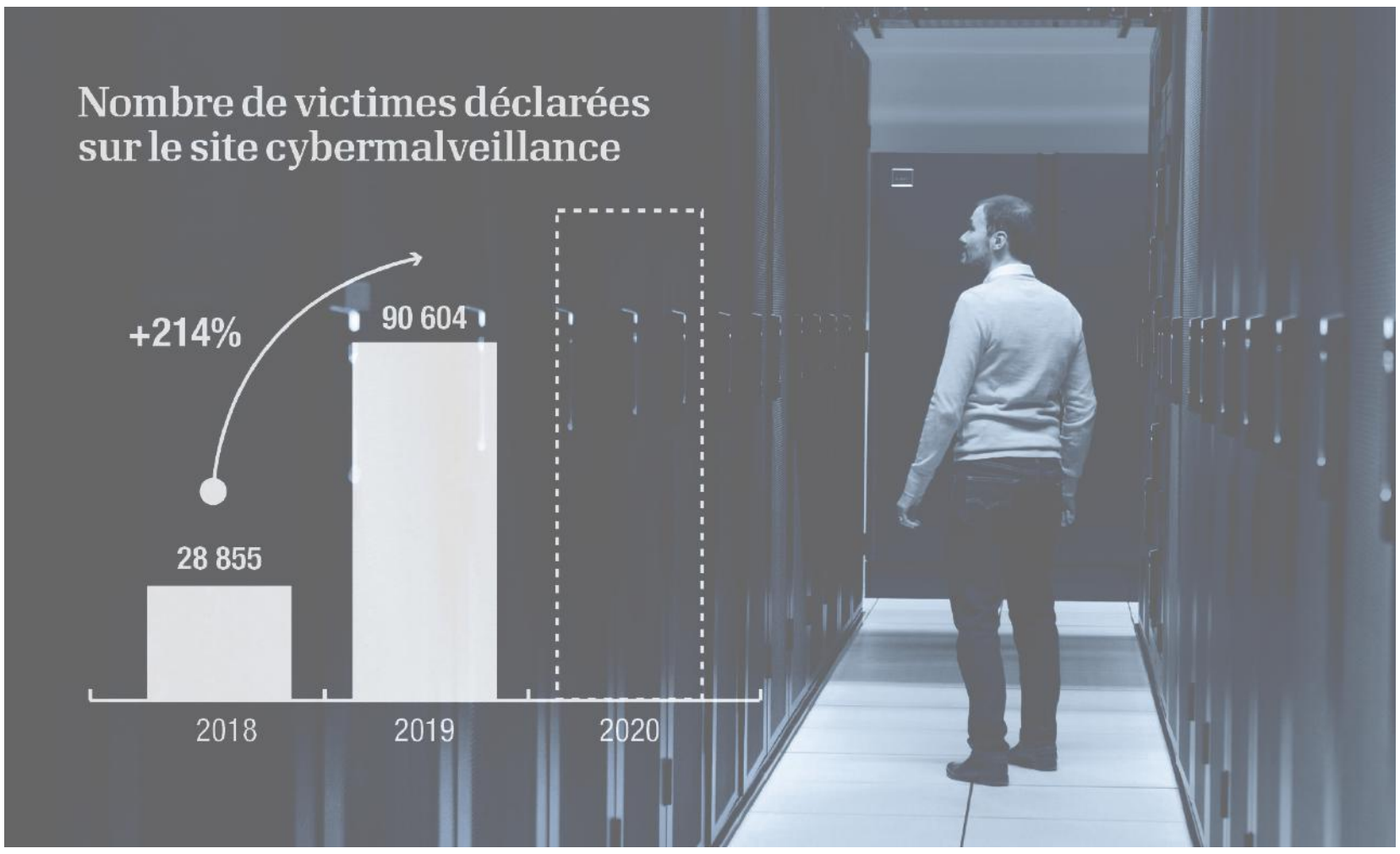
La sélection de l'Opinion

Risques d'entreprise

SÉLECTION DE L'OPINION DATÉ DU 21 JANVIER 2021 - NE PEUT ÊTRE VENDU SÉPARÉMENT

La cyber-protection, une urgence vitale



SHUTTERSTOCK

En 2020, l'Anssi a observé une forte augmentation du nombre **d'attaques majeures par ransomware**.

Chaque année depuis quinze ans, le Global Risk Report, publié par le Forum économique mondial, établit la liste des risques tels que les perçoivent des experts du monde entier. Et depuis cinq ans le cyber grimpe dans la hiérarchie des risques, se situant désormais dans le Top 5. Un classement qui illustre des faits concrets : la multiplication des attaques et leurs conséquences financières, matérielles et techniques. Ainsi, en 2020, entre janvier et fin août, l'Agence Nationale de la Sécurité des Systèmes d'Information (Anssi) a traité 104 attaques majeures via un ransomware (rançongiciel), contre 54 sur toute l'année 2019. Et encore, ce chiffre ne prend en compte que des attaques perpétrées contre de grands groupes ayant déclaré leur sinistre. Il faudrait sans doute multiplier par 100 voire davantage pour chiffrer l'étendue de la sinistralité cyber dans les entreprises françaises.

Une certitude. Celles-ci n'ont plus le choix : le cyber est devenu un risque à part entière de leur activité. Surtout en 2020. C'est ce que rappelle Philippe Cotelle, administrateur de l'Association pour le Management des Risques et des Assurances de l'Entreprise (Amrae) et risk manager d'Airbus Defence & Space. « La crise a entraîné une numérisation à marche forcée de toutes les structures, explique ce dernier. C'est devenu une question de survie. Cette dépendance accrue au digital a pour conséquence que l'impact en cas d'attaque va avoir des répercussions économiques plus importantes qu'avant. »

Mais si la menace progresse (les dépenses en matière de cybersécurité ont augmenté en moyenne de 39% en 2019), la situation est encore loin d'être satisfaisante. « Le risque cyber est bien réel en raison notamment de l'augmentation du nombre de cyberattaques », atteste Jérôme Gossé, cyber-manager Europe continentale de l'assureur Chubb, qui « a 20 ans d'expérience dans la gestion de ce type de risque, depuis sa première offre d'assurance Tous Risques Informatiques ».

Frilosité. A la décharge des entreprises, plusieurs éléments peuvent expliquer cette frilosité : il s'agit d'un risque récent (une dizaine d'années quand certains risques sont connus depuis des centaines d'années) ; il est complexe, polymorphe, évolutif, souvent peu perceptible (voire invisible) dans sa phase initiale et requiert pour le combattre de solides connaissances techniques. Mais ce n'est pas une raison pour l'ignorer. De par les dégâts qu'il entraîne (le coût médian d'une cyberattaque est estimé à plus de 50 000 euros), il est absolument fondamental pour les entreprises de mettre en place toutes les mesures nécessaires pour s'en protéger.

Dans le guide sur la maîtrise du risque numérique réalisé conjointement par l'Amrae et l'Anssi en 2019, Brigitte Bouquot, alors présidente de l'Amrae, exposait clairement la situation : « L'évolutivité et la transversalité de cette catégorie de risque obligent dorénavant les dirigeants à reconsidérer leur modèle de gestion des risques de telle sorte que le risque numérique rejoigne les préoccupations stratégiques, économiques ou juridiques des organisations. » Et celle-ci d'ajouter : « Demain, l'entreprise responsable et génératrice de confiance sera celle qui s'attache à maîtriser le risque numérique. »

Graves conséquences. Et de fait, les récentes attaques cyber ont montré qu'elles pouvaient avoir des graves conséquences non seulement sur l'entreprise touchée mais aussi sur son écosystème (clients, prestataires, donneurs d'ordre…). La confiance est devenue le mot d'ordre et pour la garantir, il faut protéger les données. Personne n'a envie de savoir que ses coordonnées de carte bancaire, confiées à un commerçant en ligne, ou son numéro de sécurité sociale transmis à un organisme public, ont été volées par un cybercriminel et sont revendues aux plus offrants sur le Dark Web, une pratique malheureusement assez répandue.

Si ces fuites ont longtemps été ignorées, leur dissimulation est aujourd'hui beaucoup plus difficile. Ainsi le fameux RGPD (Règlement général sur la protection des données) oblige les organisations à signaler aux autorités et notamment à la Cnil les atteintes aux données personnelles. Le RGPD stipule que dans certains cas, cette information doit même être rendue publique, ce qui a fortement contribué à sensibiliser les entreprises et leurs dirigeants à investir dans la sécurité de leurs réseaux. Et par conséquent à préserver leur réputation.

Après les grosses attaques informatiques comme Wannacry et NotPetya qui, en 2017, avaient frappé des entreprises du monde entier, le RGPD a marqué une nouvelle étape. Avec succès si l'on en croit le cabinet Wavestone qui a fait une étude comparative des grandes entreprises mondiales : 100% des entreprises du CAC 40 mentionnent le RGPD, la vie privée ou la protection des données personnelles dans leur communication financière (et seulement 93% pour les entreprises du Dow Jones américain).

Mais si des réglementations très rigoureuses (Loi de programmation militaire, directive européenne NIS…) ont obligé les grands groupes à investir pour leur sécurité numérique et à intégrer le risque cyber dans leur gouvernance, la situation est nettement plus nuancée dans les ETI et les PME. « La prise de conscience grandit mais il y a encore une éducation à faire », reconnaît Jérôme Gossé (Chubb).

Gestion globale des risques. Un avis partagé par Frédéric Chaplain, directeur IARD du courtier en assurances spécialisé dans la protection des entreprises Verlingue, et très bon connaisseur du sujet : « Prendre en compte le risque cyber, c'est la décision d'organiser sa résilience par rapport à ce type de risque. Cela devient une nécessité dans la gestion globale des risques. Si on n'en prend pas la mesure, on expose la responsabilité des dirigeants mais également celle de l'entreprise. Dans certains cas, l'entreprise peut se voir refuser une assurance responsabilité civile des mandataires sociaux (RCMS) si le risque cyber n'est pas considéré comme "embarqué dans la gestion des risques". » Et d'ores et déjà on commence à voir des compagnies d'assurances qui refusent d'assurer des entreprises n'ayant pas mis en place les mesures adéquates pour éviter, ou au moins limiter les sinistres.

Maria Cornu

> ***« Prendre en compte le risque cyber, c'est la décision d'organiser sa résilience par rapport à ce type de risque. Cela devient une nécessité. Si on n'en prend pas la mesure, on expose la responsabilité des personnes morales et aussi physiques »***

Une priorité pour les dirigeants

Il y a quelques années, la cybersécurité était un « objet inconnu » pour la plupart des dirigeants d'entreprise. La notion était plutôt synonyme de coûts et de « non, on ne peut pas vous mettre ce smartphone à disposition car il n'est pas suffisamment sécurisé ». Les attaques qui ont touché de grands groupes, avec de graves répercussions, ainsi que les réglementations de plus en plus sévères pour ceux qui ne prennent pas la mesure du risque, ont accéléré la prise de conscience. Ainsi en 2014, le PDG du groupe américain Target a dû démissionner à la suite du piratage informatique de son entreprise, quelques mois plus tôt. Une attaque dont le coût a été estimé à environ 250 millions de dollars (dont 90 millions pris en charge par les assurances).

Les cyberattaques Wannacry et NotPetya de 2017 ont également eu d'énormes répercussions financières : 250 millions d'euros de pertes de chiffre d'affaires pour Saint-Gobain ; plus de 300 millions de dollars pour le Danois Maersk ; environ 200 millions de dollars pour le géant de l'agroalimentaire Mondelez… Il ne s'agit que de quelques exemples, mais ils ont servi de catalyseurs pour de nombreux Comex. A l'instar de ce qui s'est fait dans les pays anglo-saxons, les grands groupes français ont déployé des DSSI (pour directeur de la sécurité des systèmes informatiques) qui, le plus souvent, sont directement rattachés à la direction générale de leur entreprise.

Prise de responsabilité. Parallèlement, l'arsenal juridique et réglementaire a accéléré la prise de responsabilité des organisations et de leur direction. La Loi de programmation militaire de 2013 impose ainsi aux « opérateurs d'importance vitale » (plus de 200 organisations en France) « le renforcement de la sécurité des systèmes d'information critiques qu'ils exploitent » sous la houlette de l'Anssi. En 2018, le RGPD a donné un cadre strict à la gestion des données personnelles avec des sanctions pouvant aller jusqu'à 4% du chiffre d'affaires annuel pour le contrevenant. Quant à la directive (européenne) NIS, celle-ci a étendu les obligations de sécurité renforcée aux « opérateurs de service essentiels » (OSE).

C'est pourquoi il devient urgent pour les plus hautes instances d'une entreprise, petite ou grande, de se pencher sur le sujet. Et de se préparer. C'est d'ailleurs le sens du message adressé par Guillaume Poupard, le directeur général de l'Anssi, lors des Assises de la cybersécurité, en octobre dernier. Rappelant les campagnes d'information et les réglementations mises en place, il a martelé que « les décideurs ne peuvent plus dire qu'ils ne savaient pas. Et s'ils le disent, ils sont fautifs ». De son côté, le cabinet d'analyse Gartner estime que, dans les prochaines années, « les répercussions d'un incident cyber sur des systèmes physiques vont incomber directement aux PDG ». Selon celui-ci, cela deviendra donc « une responsabilité personnelle et non plus une responsabilité de la société ». Un point auquel les assureurs sont très sensibles. Mais pas seulement. Avant toute opération, les analystes et investisseurs financiers sont de plus en plus nombreux à évaluer la maturité cyber des entreprises.

M.C.

La prise de conscience progresse

LONGTEMPS, LES ENTREPRISES victimes de cyberattaques sont restées discrètes sur le fait même qu'elles avaient été attaquées. Lorsqu'elles s'en rendaient compte ! Selon le cabinet Wavestone, le délai moyen observé entre une intrusion dans un système d'information et sa détection était, en France, de 94 jours en 2020, contre… 167 jours en 2019, où il fallait près de 6 mois pour que quelqu'un détecte une intrusion informatique ! Et encore fallait-il encore du temps pour évaluer ce qui avait pu se passer, s'il s'agissait d'un vol de données et desquelles, de l'installation d'un logiciel espion ou d'un malware qui attendait son heure pour agir. L'employé qui avait malencontreusement cliqué sur une pièce jointe possiblement infectée n'osait pas alerter les informaticiens de peur d'être soupçonné ou accusé de malveillance. La multiplication des attaques visant des entreprises de toutes tailles et de tous secteurs, conjuguée à la mise en œuvre de réglementations contraignantes, notamment du Règlement général sur la protection des données (RGPD) européen, et à la large diffusion d'informations de la part des organismes publics en charge de la cybersécurité a fait évoluer la situation.

Du point de vue juridique, les risques liés au numérique ne sont pas nouveaux et les textes existent. « Mais en même temps que les technologies et les attaques se sont multipliées, notre dépendance croissante au numérique a accentué le besoin de sécurité à la fois en amont, c'est-à-dire en conseil et en prévention, et en aval, en défense et en récupération de données », constate Me Garance Mathias, fondatrice du cabinet Mathias Avocats, spécialisé dans le droit des technologies innovantes.

Approche anglo-saxonne. Sensibles à ce besoin et conscientes que le risque numérique n'est plus seulement l'affaire d'experts techniques mais qu'il doit être traité au plus haut niveau des organisations, l'Agence nationale de la sécurité des systèmes d'information (Anssi) et l'Association pour le management des risques et des assurances de l'entreprise (Amrae) ont publié un guide (*Maîtrise du risque numérique - L'atout confiance*) en français et en anglais.

Car si les textes juridiques existent, les entreprises françaises n'ont pas la même approche que leurs homologues anglo-saxonnes. « La différence est culturelle. Nos systèmes juridiques ne traitent pas de la même façon les questions de la responsabilité ou du fonctionnement de la société, par exemple », précise Garance Mathias. Là où les organisations anglo-saxonnes considèrent leur département juridique ou leur avocat comme un conseiller, un partenaire, et l'impliquent le plus en amont possible d'une contractualisation ou d'une négociation, les entreprises "latines" ont parfois tendance à le tenir à l'écart, voire lui dissimulent certaines informations ou recopient des clauses sans être sûres qu'elles répondent à leurs besoins. « Cela évolue. Face aux sanctions de la Cnil, lorsqu'elles sont mises en cause pour une fuite de données, ou à l'importance des dommages, les entreprises appréhendent le risque différemment. Mais toutes n'ont pas un département juridique ni même parfois un juriste », poursuit-elle.

« Face aux sanctions de la Cnil, lorsqu'elles sont mises en cause pour une fuite de données, ou à l'importance des dommages, les entreprises appréhendent le risque différemment »

Le RGPD, entré en application en mai 2018, a été un accélérateur de la prise de conscience. Outre qu'il incite à la nomination d'un délégué à la protection des données (DPO), il prévoit des sanctions, appliquées par la CNIL en France, qui peuvent représenter en principe jusqu'à 4% du chiffre d'affaires de l'entreprise mise en cause. Mais c'est surtout l'importance des coûts et des pertes dus à une cyberattaque qui conduit aujourd'hui les organisations publiques ou privées à s'emparer de cette question du risque lié au numérique. L'impact financier des attaques par rançongiciel qu'ont subi Bouygues, CMA CGM ou Sopra Steria, pour ne citer que les plus récentes, se chiffre en dizaines voire en centaines de millions d'euros. Plus de quoi nier le problème ou tenter de le dissimuler !

Louise Chapry

SIPA PRESS

Le délai moyen observé entre une **intrusion** dans un système d'information et sa détection était, en France, de 94 jours en 2020, contre… 167 jours en 2019.

« Il faut sensibiliser encore et encore ! »

JÉRÔME NOTIN dirige le Groupement d'intérêt public Actions contre la cybermalveillance (GIP ACYMA), plus connu sous le nom de la plateforme cybermalveillance.gouv.fr. Créé en octobre 2017, ce GIP regroupe une cinquantaine de membres : institutionnels, entreprises privées, services publics, syndicats et associations des secteurs du numérique, de l'assurance et de la consommation. Ses missions : sensibilisation, prévention et assistance aux victimes.

Quels sont les faits marquants de 2020 pour la plateforme cybermalveillance.gouv.fr ?

Jérôme Notin : Je ne peux pas ne pas évoquer le recours au télétravail imposé par la crise sanitaire, qui a eu d'importantes conséquences, car pour beaucoup, une telle situation n'avait pas été anticipée et les cybercriminels en ont largement profité. Rien que pendant la première semaine de confinement, la plateforme a enregistré une augmentation de 400 % des attaques par hameçonnage, phishing en anglais, et une hausse similaire de l'utilisation de nos services ! Le nombre de visiteurs uniques, qui était de 460 000 en 2019, a dépassé le million en 2020. En ce qui concerne le GIP, l'année a été marquée par le lancement de notre label ExpertCyber, qui valorise l'expertise des professionnels de la cybersécurité.

En quoi cela consiste-t-il ?

Dès le lancement du site, en 2017, nous voulions recommander aux victimes des prestataires capables de les assister en fonction du type de malveillance subie. A ce jour, nous avons référencé plus de 1 000 prestataires sur tout le territoire, qui peuvent intervenir auprès des particuliers ainsi que des TPE et des PME locales. Nous voulions aller plus loin, notamment pour mieux assister les entreprises petites et moyennes, plus vulnérables car moins sensibilisées et moins préparées face à des attaques de plus en plus sophistiquées. Nous avons développé le label ExpertCyber, en partenariat avec les syndicats professionnels du secteur, la Fédération française de l'assurance et le soutien de l'Afnor, pour qualifier les prestataires informatiques les plus experts en cybersécurité. Ce label est attribué aux sociétés de services informatiques qui en font la demande après évaluation de leur expertise, de leurs bonnes pratiques et leurs compétences. En général ces sociétés comptent 2 ou 3 spécialistes de la cybersécurité. Nous en avons labellisé 50 en 2020. A terme, nous souhaitons en qualifier 200. Et nous espérons que les assureurs s'empareront du label, qui leur désigne les prestataires locaux les plus qualifiés, pour assister les victimes.

« Notre site répertorie 45 types de malveillance. Nous alertons régulièrement sur les nouvelles menaces. Récemment, nous avons ajouté l'escroquerie au Compte personnel de formation et les messages d'escrocs usurpant l'identité de la Police nationale »

Comment sensibiliser à la cybermalveillance les TPE et les PME, qui ne disposent pas toujours de personnel dédié à ce sujet ?

Effectivement, la quasi-totalité des entreprises qui consultent le site et se font assister sont des TPE et des PME, qui représentent 99% des entreprises françaises. Nombre d'entre elles sous-estiment ce risque. On sait que la cybersécurité repose sur des outils mais aussi - et peut-être surtout - sur le facteur humain. Or, pour que les salariés soient sensibilisés, il faut qu'ils soient formés. Ils le sont de plus en plus dans les grandes entreprises, mais encore pas assez dans les TPE et PME. C'est pour elles que nous avons lancé, en octobre dernier, un programme de formations gratuites en partenariat avec Google et la Fédération d'e-commerce et de la vente à distance, la Fevad. Trois modules sont proposés pour l'instant : une initiation générale à la cybersécurité, un module sur le commerce en ligne et un autre sur le télétravail.

DR

Jérôme Notin, directeur général du Groupement d'intérêt public Actions contre la cybermalveillance.

Quelles sont les principales menaces que vous avez identifiées ?

Au démarrage de la plateforme, il s'agissait beaucoup de faux virements, mais cela a beaucoup évolué. Aujourd'hui, le site répertorie 45 types de malveillance. Nous alertons régulièrement sur les nouvelles menaces. Récemment, nous avons ajouté l'escroquerie au Compte personnel de formation (CPF) et les messages d'escrocs usurpant l'identité de la Police nationale… Cela dit, le trio de tête reste les rançongiciels, les fameux ransomwares, les faux virements et les défigurations de sites. Les premiers sont loin devant les autres. C'est rageant, car il suffit de faire régulièrement des sauvegardes de ses données sur un support externe et déconnecté pour s'en protéger.

Interview Louise Chapry

RSSI, un métier clé au sein des organisations

EXPLOSION DES VOLUMES DE DONNÉES, numérisation croissante, prolifération des applications… Tout dans l'entreprise contribue à multiplier les risques et les points de vulnérabilité aux cyberattaques. Rien d'étonnant à ce que ce sujet fasse l'objet d'une attention particulière et qu'une fonction dédiée lui ait été consacrée, celle de responsable de la sécurité des systèmes d'information, le RSSI.

Si elle a longtemps régné seule sur l'informatique de l'entreprise, la DSI, direction des systèmes d'information, a vu son rôle évoluer de fonctions opérationnelles de production informatique vers une mission stratégique de développement du numérique. Son périmètre s'est élargi en fonction de la complexification des différents éléments qui composent un système d'information (architecture, interconnexion…) et de l'émergence des nouvelles technologies comme le cloud computing ou l'intelligence artificielle. Aujourd'hui que le numérique a percolé dans tous les métiers et toutes les strates des organisations, de nouveaux rôles ont émergé comme, par exemple, le « chief digital officer » (CDO) alias directeur de la stratégie numérique, ou le « data protection officer » (DPO), responsable de la protection des données, fonction qui a vu le jour en même temps que le Règlement général sur la protection des données (RGPD), entré en vigueur en mai 2018.

Bonnes pratiques. Comme eux, le RSSI a un rôle transversal, qui touche à toutes les activités, à tous les métiers de l'entreprise, mais aussi à tous les acteurs de son écosystème : employés, partenaires, clients, fournisseurs, prestataires. Car il ne suffit plus de sécuriser les processus internes dans leur strict aspect technologique. Il faut aussi sensibiliser et former les utilisateurs de tous les métiers, production, finance, marketing ou ressources humaines, les inciter à être vigilants, à être capables de détecter un risque et d'alerter en cas de suspicion. Il faut également distiller les bonnes pratiques auprès des fournisseurs et des clients, car le niveau de sécurité de l'écosystème est celui de son maillon le plus faible. « De plus en plus souvent, les donneurs d'ordre poussent les sous-traitants à prendre des assurances », observe d'ailleurs Jérôme Gossé, Cyber Manager Europe Continentale de l'assureur Chubb. Car le risque est omniprésent, il peut surgir dans une transaction e-commerce, survenir d'une pièce jointe à un e-mail, de la mise à jour d'un logiciel applicatif…

« Comment sont sécurisés les réseaux ? Comment sont segmentées les données ? Quels sont les outils de détection ? Comment est gérée la supply chain ? Quelle responsabilité ? Y a-t-il des audits sur les sous-traitants ? Autant de questions auxquelles il faut répondre »

Ces nouveaux rôles sont indissociables les uns des autres et entraînent une redéfinition des missions de chacun. Car les domaines de compétences ne sont plus délimités de manière stricte. La gouvernance numérique de l'entreprise repose sur la capacité de ces responsables à échanger, à partager renseignements, informations et données afin de rendre l'entreprise numérisée la plus résiliente possible. « Comment sont sécurisés les réseaux ? Comment sont segmentés les systèmes ? Quels sont les outils de détection ? Comment est gérée la supply chain ? Quelle responsabilité ? Y a-t-il des audits sur les sous-traitants ? » Autant de questions auxquelles il faut répondre, insiste Jérôme Gossé (Chubb). C'est en concertation que le DSI, le RSSI et le Risk manager doivent travailler pour garantir la gestion des cyber-risques, leur anticipation, leur compréhension et contractualiser l'assurance qui les couvre.

Louise Chapry

Les bons réflexes pour éviter une intrusion

COMME LE RAPPELLE Frédéric Chaplain, directeur IARD du courtier Verlingue, « la question n'est plus de savoir si les entreprises vont subir une cyberattaque, mais quand celle-ci va arriver ». Toutes les organisations, petites ou grandes, publiques ou privées ont été, sont ou seront victimes d'un sinistre informatique. Avec des conséquences plus ou moins graves mais jamais indolores. Pour se protéger, il est indispensable de mettre en place quelques bonnes pratiques qui, à défaut d'empêcher l'attaque, permettront d'en atténuer les effets.

« Il faut bien comprendre le risque cyber pour l'appréhender en amont et être prêt au moment de l'attaque, insiste Jérôme Gossé, cyber manager Europe continentale de l'assureur Chubb. Mais c'est un risque très évolutif. Donc il faut s'adapter. » L'Anssi fournit de nombreux conseils comme ce « Guide des bonnes pratiques de l'informatique » publié en collaboration avec la CPME. Le site cybermalveillance.gouv.fr est également une source d'information utile. Jérôme Gossé martèle les trois points incontournables : « Effectuer des sauvegardes régulières externalisées ; "patcher" (mettre à jour les logiciels) et sensibiliser les employés. » Cela peut passer par une charte informatique qui sera fournie avec le contrat de travail (ou via un avenant) édictant les bonnes pratiques (ne pas utiliser l'ordinateur professionnel à des fins personnelles, ne pas donner son mot de passe à un tiers…).

Pour Frédéric Chaplain, c'est néanmoins insuffisant. « Souvent, ces chartes sont trop longues, personne ne les lit. Il faut rendre long et difficile l'accès aux données. La plupart des hackers veulent aller vite. S'ils trouvent un obstacle, ils vont renoncer. Il faut donc leur compliquer la tâche et la plupart du temps, cela est suffisant. » Pour ce faire, l'entreprise doit connaître le degré critique de ses données, identifier celles qui sont les plus sensibles (qui doivent donc être le mieux protégées) et les autres… Mais aussi déterminer les points de vulnérabilité du système d'information.

Premières heures décisives. Les entreprises peuvent également s'appuyer sur des prestataires de conseil et de plus en plus souvent sur leurs assureurs et courtiers. Ces derniers disposent d'un réseau d'experts qui vont accompagner les clients dans la prévention des risques numériques et aussi pendant et après l'attaque. Chez Verlingue, les équipes sont très soucieuses de la prévention, qui va bien au-delà du questionnaire de l'état des lieux réalisé au moment de la souscription. « L'assurance cyber, c'est avant tout de l'assistance (cartographie des risques, mise en relation avec des experts, aide à la réparation, etc.). Un produit dont le cœur est un panel de services », explique Frédéric Chaplain qui, en cas de crise, se définit comme un « pompier » plutôt qu'un courtier.

Car quand l'attaque arrive, celle-ci pouvant paralyser tout le système d'information de l'entreprise et/ou empêcher l'accès aux données, il faut s'organiser rapidement, monter une cellule de crise et répartir les tâches de façon rigoureuse. Avoir souscrit une police d'assurance

« Les experts tentent de comprendre par où sont entrés les pirates et quel type de malware a été utilisé. Nous voulons documenter au maximum l'attaque pour fournir l'information aux assureurs »

cyber est alors d'un grand secours car le courtier (ou l'assureur) va être capable de mobiliser très vite les moyens nécessaires à la résolution de la crise (spécialistes techniques, avocat, communication…). Directeur général d'Inquest, un cabinet de gestion de crise, Alexis Nardonne sait que les premières heures sont décisives : « Il faut éviter la propagation. Les experts déconnectent les machines, essaient de récupérer les informations sur les systèmes compromis. Ils tentent aussi de comprendre par où sont entrés les pirates et quel type de malware a été utilisé. Nous voulons documenter au maximum l'attaque pour fournir l'information aux assureurs. »

Verlingue a vu ce type d'attaques se multiplier ces derniers mois, à l'instar de ce client qui, peu de temps après avoir souscrit une assurance cyber, a été victime d'un ransomware, via une faille dans les mots de passe : « tous les systèmes informatiques étaient bloqués et les collaborateurs ont dû communiquer avec leur téléphone portable personnel » rappelle Frédéric Chaplain. La revendication des attaquants ? Une rançon de 19 millions de dollars, une somme inimaginable pour l'ETI touchée. « Dans cette situation, il faut apporter immédiatement une réponse technique et essayer de comprendre l'intensité et les conséquences de l'attaque. Parallèlement, un négociateur a commencé à discuter avec les attaquants. En quelques jours, la demande de rançon est passée à 9 millions. Puis, finalement, l'entreprise a pu récupérer ses données sans avoir à payer. Mais il a fallu trois semaines de négociations » précise Frédéric Chaplain. Une histoire qui se termine plutôt bien, même s'il faut s'assurer que les données n'ont pas été compromises.

Louise Chapry

DR

Sauvegardes extérieures, mises à jour et sensibilisation des salariés : trois points incontournables pour se protéger des cyberattaques, selon **Jérôme Gossé**, cyber manager Europe de Chubb.

« Aucune entreprise n'est à l'abri d'une attaque ! »

NICOLAS ARPAGIAN est vice-président en charge de la stratégie d'Orange Cyberdefense. Face à la banalisation de la cybercriminalité, il insiste sur la nécessité pour les entreprises de prendre conscience des risques qu'elles courent, mettre en place les solutions pour s'en protéger et revenir à une situation stable en cas d'attaque.

La crise sanitaire a accéléré la transformation numérique, ce qui a augmenté l'exposition aux cyber-risques des entreprises, notamment des PME. Comment se protéger ?

Le premier pas vers la résilience consiste à admettre que l'on peut subir une cyberattaque. Cela concerne toutes les entreprises, dès lors qu'elles sont un tant soit peu connectées et informatisées. Rien, ni la nature de leur activité, ni leur taille, ni leur localisation géographique, ne les protège d'une attaque. Les exemples qui se sont multipliés tout au long de l'année écoulée l'ont montré. Il faut différencier les attaques ciblées et les attaques opportunistes. Les premières visent un équipement déterminé ou des données, comme un secret de fabrication, un processus de production ou des données financières. Dans ce cas, le pirate prend son temps, il procède par ingénierie sociale, se renseigne et accumule les informations avant d'attaquer. Pour les secondes, l'attaquant cherche à récupérer des informations monnayables (e-mails, données personnelles), de la puissance de calcul pour mener une attaque par déni de service (DdoS), ou une capacité d'hébergement pour héberger des fichiers frauduleux ou des sites de contrefaçons. Ce type d'attaques peut aussi cibler une entreprise ou une entité précise. Ces attaques opportunistes, comme leur nom l'indique, sont menées lorsqu'une occasion se présente : un mot de passe ou une information obtenue au hasard d'une conversation ou achetés dans le Dark Web, une faille dans un logiciel dont la version n'a pas été actualisée, etc.

On parle souvent de résilience. En matière de cybersécurité, en quoi cela consiste-t-il ?

La résilience est la capacité à se reconstruire après un traumatisme. Les entreprises doivent pouvoir faire face à un événement impromptu de type cyberattaque : détecter l'intrusion au plus tôt, la stopper et reconstituer leur patrimoine numérique pour revenir à une situation la plus normale possible. Cela dit, il faut résister à la tentation de tout protéger avec un haut niveau de sécurité. D'abord, parce que cela coûterait très cher et ensuite, parce que ce serait trop contraignant. Ce serait un peu comme si vous fermiez chacune des pièces de votre appartement à clé. La sécurité y gagnerait mais les habitants peineraient à respecter ces consignes. En fait, seuls certains domaines ont besoin d'être hautement sécurisés. Il faut adapter son organisation à ce qui doit être protégé et à l'usage qui en est fait. Cela suppose que les entreprises aient une connaissance précise et actualisée de leurs actifs, qu'elles aient identifié ce qui crée de la valeur pour leur activité et leur revenu, ce qu'elles doivent particulièrement protéger. La solution n'est pas de mettre des barreaux à toutes les fenêtres, mais d'identifier les actifs essentiels qui doivent être placés dans un coffre et ceux qui exigent moins de précautions. Une analyse stratégique doit donc précéder les choix techniques pour proportionner la protection des systèmes d'information.

« Il faut résister à la tentation de tout protéger avec un haut niveau de sécurité. D'abord, parce que cela coûterait très cher et ensuite, parce que ce serait trop contraignant »

Comment protéger ces éléments créateurs de valeur ?

La démarche se fait en plusieurs étapes. D'abord identifier, pour chaque métier, les fonctions qui peuvent accéder aux données ou aux applications, définir qui a accès à quoi et pour faire quoi. Qui peut les consulter, les modifier, les dupliquer voire les supprimer. Il s'agit d'attribuer à chacun les autorisations correspondant à son périmètre. Un stagiaire en comptabilité n'a pas les mêmes droits d'accès qu'un informaticien en CDI ou un manager. Au-delà de son apport à la sécurité, cette règle de bonne gouvernance précise le rôle et la contribution de chacun au patrimoine informationnel. Ensuite, il faut faire des sauvegardes régulièrement et grâce à des moyens décidés en fonction des besoins de chaque entreprise. Pour la troisième étape, il faut investir dans une solution de détection, sans laquelle il n'est pas possible d'intervenir suffisamment tôt, et donc de limiter les dégâts. Enfin, il faut former tout le personnel de l'entreprise, car la cybersécurité n'est pas seulement l'affaire du directeur informatique (DSI) ou du responsable de la sécurité (RSSI). Chacun doit connaître les bonnes pratiques et savoir donner l'alerte. C'est rarement le RSSI qui reçoit l'email avec une pièce jointe sur laquelle l'attaquant espère que le destinataire va cliquer…

Interview L.C.

PHILIPPE BRUCHOT

« Le premier pas vers la résilience consiste à admettre que l'on peut subir une cyberattaque », estime **Nicolas Arpagian**.

Une vigilance accrue avec le télétravail

DRÔLE DE PARADOXE. Selon une étude CyberArk*, plus de 9 employés sur 10 (93 %) affirmaient en décembre dernier vouloir continuer à travailler à distance. Pourtant, un sur deux (53 %) avouait ignorer les directives de sécurité de son entreprise. Le recours massif au télétravail imposé par la pandémie de Covid-19 a très vite mis en lumière les mauvaises pratiques et le manque de formation en cybersécurité des employés. Mixité des usages professionnel et personnel, mots de passe trop souvent réutilisés, installation d'applications non conformes à la politique sécurité de l'entreprise, contournements des règles les plus contraignantes… Le travail à domicile est rapidement devenu synonyme de cyber-risques accrus.

Formation. Les principaux risques sont purement techniques : vulnérabilités de logiciels, accès frauduleux aux postes de travail et aux serveurs, installation de malwares à l'insu des utilisateurs, etc. Ces risques existaient déjà avant le recours massif au télétravail. Mais celui-ci a également un impact important sur le comportement des collaborateurs et leur santé, tant physique que mentale. Isolés de leurs collègues et de leur management, distraits par leur environnement familial, ils sont moins vigilants et moins sensibilisés aux risques. Là où un échange impromptu avec d'autres collaborateurs lèverait leurs doutes sur un mail frauduleux ou une tentative de phishing, ils se retrouvent seul devant leur écran. L'isolement rend aussi difficile le rappel à la politique de sécurité de la société, rappel qu'ils retrouvent habituellement dans les couloirs ou à la machine à café.

Ces nouvelles conditions doivent conduire les entreprises et les managers à adapter leur communication sur le sujet et leur mode de management. Certes, les formations à la cybersécurité se sont généralisées dans les plus grandes entreprises, même s'il s'agit souvent de modules en ligne rapidement consultés. Il faut sensibiliser et former l'ensemble des collaborateurs de façon systématique et continue. Les tests d'intrusion et les simulations d'attaque par des cybercriminels éthiques contribuent à identifier les failles du système d'information, mais aussi à sensibiliser les employés, qui « tombent dans le piège » encore trop souvent. Pour qu'elles soient efficaces, la sensibilisation et la formation aux cyber-risques doivent devenir systématiques et pourquoi pas ludiques, voire récompensées d'une manière ou d'une autre. A fortiori dans la perspective d'un maintien d'un niveau élevé de travail à distance.

Il faut sensibiliser et former l'ensemble des collaborateurs de façon systématique et continue

La persistance du télétravail doit aussi s'accompagner du déploiement de solutions techniques qui ne posent pas d'interdit, sans quoi les collaborateurs les contourneraient, créant ainsi de nouveaux risques. **L.C.**

*Enquête menée par un cabinet indépendant pour le compte de CyberArk, en octobre 2020, auprès de 2000 télétravailleurs en France, en Allemagne, au Royaume-Uni et aux Etats-Unis.

« L'offre cyber va devenir l'assurance responsabilité civile ou incendie du XXIe siècle »

Gilles Bénéplanc est directeur général du Groupe Adelaide, spécialisé dans le conseil, l'intermédiation, la distribution et les services en assurances, et directeur général de Verlingue, courtier en assurances spécialisé dans la protection des entreprises.

Comment analysez-vous le risque cyber ?

Nous constatons clairement une montée en puissance de ce risque, surtout durant cette année marquée par la Covid-19. Il y a trois raisons principales : d'abord une digitalisation accrue de l'économie,puisque le numérique est présent dans tous les secteurs d'activité et tous les foyers. Ensuite, le développement du travail à distance, parfois insuffisamment préparé. Afin de permettre à tous les collaborateurs de travailler rapidement à distance, les entreprises ont baissé la garde sur la sécurité numérique. Et au début, elles ont fait des

« Heureusement, nous n'avons pas encore vécu de scénario complètement noir où tous les systèmes de fonctionnement seraient touchés en même temps, comme nous pouvons le vivre en ce moment avec la pandémie »

concessions que leurs experts n'auraient pas acceptées en temps normal. Enfin, il y a une vraie professionnalisation des attaquants. Ils ont de plus en plus d'outils, sont mieux structurés. On peut même parler d'industrialisation des attaques. Par conséquent, celles-ci sont plus fréquentes et plus complexes.

Comment les entreprises se comportent-elles face à ce risque ?

Il existe une vraie prise de conscience de leur part. Nos clients comprennent la complexité de ce risque car beaucoup de gens ont été attaqués. C'est devenu un sujet d'actualité relayé par un discours de sensibilisation porté par les pairs, par les instances publiques comme l'agence nationale de la sécurité des systèmes d'information (Anssi) et par les courtiers en assurance et les assureurs. Ces derniers font de gros efforts pour trouver des solutions assurantielles et fournir une aide réelle à la gestion des incidents et des sinistres.

Quel est le rôle d'un acteur comme Verlingue vis-à-vis de ses clients ?

Notre intervention est multiple. Elle se déroule avant et, s'il y a attaque, pendant et après le sinistre. Nous avons d'abord un rôle de prévention avec des questionnaires pour évaluer le risque. Nous sommes vraiment dans une démarche de conseil avec des spécialistes internes qui connaissent bien la problématique. Nous rappelons les règles d'hygiène informatique et nous insistons sur les bonnes pratiques (gestion des mots de passe, sensibilisation…). S'il y a une attaque et un sinistre, nous faisons appel à des experts. Nous travaillons avec des prestataires qui, si nécessaire, sont capables de monter et piloter une cellule de crise. L'important est d'assister le client et de pouvoir faire face très vite, avant même d'envisager de payer le sinistre lorsqu'il s'agit d'une attaque par rançongiciel. Quoi qu'il en soit, nous déconseillons de payer la rançon. L'objectif est de désamorcer l'attaque. Ensuite, avec d'autres experts, nous menons des investigations pour en comprendre les ressorts et estimer le sinistre.

Le marché de l'assurance a-t-il une bonne connaissance de ce risque ?

MAËLLE BERNARD

« Nous constatons clairement une montée en puissance du risque cyber », estime **Gilles Bénéplanc**.

La connaissance des assureurs et des courtiers progresse de manière significative car il y a beaucoup de sinistres. Mais c'est un risque complexe. Nous avançons et le marché va encore se développer. Nous travaillons à affiner les garanties et à améliorer les techniques de tarification. La qualité de rédaction des contrats évolue également. Il faut sortir des zones de flou et voir comment prendre en compte dans le contrat les multiples cas de figure rencontrés. Heureusement, avec le risque cyber, nous n'avons pas encore vécu de scénario complètement noir où tous les systèmes de fonctionnement seraient touchés en même temps, comme nous pouvons le vivre en ce moment avec la pandémie. Les primes sont orientées à la hausse. Dans la plupart des cas, l'assurance cyber constitue un nouveau budget pour les entreprises, mais également une nouvelle matière en termes de gestions des risques. Pour les nouveaux clients, les montants restent raisonnables. Et pour ceux qui possèdent déjà

« D'ores et déjà, nous voyons des assureurs refuser de coter une assurance responsabilité civile à des mandataires sociaux s'ils n'ont pas souscrit une assurance cyber »

une garantie, les tarifs ont augmenté compte tenu de l'exposition au risque qui peut se compter en millions d'euros, même pour une moyenne entreprise. C'est un risque avec beaucoup d'impact et cette tendance va continuer à croître.

Les entreprises qui font de la prévention sont-elles « récompensées » ?

Oui, il existe une prime à la prévention. Mais a contrario, si l'entreprise ne prend aucune mesure, elle va rencontrer de plus en plus de difficultés à trouver un assureur. Et de plus en plus souvent, pour opérer sur certains marchés, il faudra être assuré. L'assurance cyber va devenir l'assurance responsabilité civile ou incendie du XXIe siècle. Les donneurs d'ordre ne traiteront plus avec les entreprises qui n'ont pas contracté d'assurance cyber car il y a des risques sur la chaîne d'approvisionnement. D'ores et déjà, nous voyons des assureurs refuser de coter une assurance responsabilité civile à des mandataires sociaux s'ils n'ont pas souscrit une assurance cyber. Dans les appels d'offres, la sécurité numérique est devenue un critère d'une gestion responsable des risques.

Interview Maria Cornu

Quiz. Votre défense est-elle à jour ?

Que veulent dire, par exemple, les termes phishing ou ransomware ? Petit test (très facile) pour sonder votre degré de connaissance du risque cyber.

1. Par rapport à un ordinateur, un smartphone est :
a) Plus sécurisé.
b) Aussi sécurisé.
c) Moins sécurisé.

Bonne réponse : c. Les données contenues dans un smartphone sont en général moins protégées. Il est possible de mieux le sécuriser en limitant les téléchargements des applications, en activant le verrouillage automatique et en sauvegardant régulièrement les données.

2. Quel(s) terme(s) désigne(nt) une attaque informatique ?
a) Poinçonnage.
b) Bucéphale.
c) Ransomware.
d) Amorçage.
e) Advise.

Bonne réponse : c. Ransomware : Il s'agit d'un code malveillant qui empêche l'utilisateur d'accéder à ses données et lui demande une rançon pour libérer son système.

3. Mon ordinateur me demande d'effectuer une mise à jour :
a) Je ne le fais pas car je n'ai pas l'utilité des nouvelles fonctionnalités apportées par la mise à jour et cela va ralentir ma machine.
b) Je le ferai dans un jour futur quand j'aurai le temps. Il n'y a pas d'urgence.
c) Je le fais le plus vite possible.

Bonne réponse : c. Les mises à jour incluent généralement à la fois des nouvelles fonctionnalités, mais aussi des correctifs de sécurité. L'absence de mise à jour des systèmes est l'une des principales failles utilisées par les pirates lorsque ils effectuent une cyberattaque. Il est donc très important de faire ces mises à jour sur tous votre matériel professionnel des qu'on vous le propose : téléphone, tablette ou ordinateur.

4. Avec le télétravail, il m'arrive d'utiliser mon ordinateur professionnel pour des activités personnelles (stocker mes photos de vacances, télécharger un jeu, consulter mes comptes bancaires…).
a) Pas de soucis, je le fais depuis longtemps et il ne m'est jamais rien arrivé.
b) J'évite de mélanger les genres. Prudence !
c) Je fais attention. De toute façon, il n'y a que moi qui utilise cet ordinateur et il est protégé par un antivirus.

Bonne réponse : b. Cette pratique est proscrite et n'est pas sans risque pour l'ensemble de vos données. S'il pénètre dans la machine ou sur le réseau, l'attaquant peut avoir accès d'un coup à toutes vos informations non seulement professionnelles mais aussi professionnelles (dont les informations bancaires).

5. J'ai reçu une offre promotionnelle d'un de mes fournisseurs, qui a dû utiliser son mail personnel pour me l'adresser.
a) Je réponds tout de suite au message. Je le connais, je peux lui faire confiance.
b) Je détruis le mail.
c) Je me connecte sur son adresse pro pour lui demander s'il est l'auteur du mail.

Bonne réponse : b. Il faut absolument éviter les réseaux publics dont l'accès ne nécessite pas de mot de passe. Un pirate pourrait intercepter les mails, les mots de passe, et voir les pages Web que vous visitez.

6. Lors d'un voyage professionnel, j'ai besoin de travailler dans ma chambre d'hôtel. L'établissement permet de se connecter sans mot de passe au WiFi.
a) Super, je vais travailler sur mes fichiers !
b) J'évite de me connecter. J'attendrai d'avoir une connexion sécurisée.
c) Je suis prudent(e). Je me contente de regarder ma messagerie professionnelle.

Bonne réponse : c. D'une façon générale, il ne faut pas faire confiance machinalement au nom de l'expéditeur qui apparaît dans le message et ne jamais répondre sans un minimum de précaution. Dans ce cas, il faut garder le contact professionnel en général mieux sécurisé.

SIPA PRESS

Sur Internet, **le petit cadenas** dans la barre d'adresse est toujours l'un des signes d'une connexion sécurisée.

7. Je reçois un mail de ma banque me demandant de cliquer sur un lien afin de mettre à jour certaines informations confidentielles.
a) Je clique sur le lien. C'est ma banque, je peux avoir confiance.
b) Je vérifie l'authenticité du mail. C'est peut-être du phishing.
c) Encore une pub, je réponds que je ne suis pas intéressé(e).

Bonne réponse : b. Les arnaques aux faux mails sont des attaques informatiques très fréquentes. Les institutions comme les établissements bancaires ne demanderont jamais des informations confidentielles par mail. Et rendre à ce type de message permet d'enrichir les bases des pirates. Pour reconnaître, un faux mail, il faut tout de suite : vérifier l'orthographe et regarder dans la barre du navigateur, s'il y a https et non http qui distingue les sites sécurisés. Pour les pages de paiement en ligne, il faut s'assurer de la présence d'un petit cadenas vert.

8. Je dois changer mon mot de passe d'ordinateur mais je suis obligé(e) d'utiliser une combinaison compliquée.
a) Je l'écris sur un post-it caché sous mon clavier. Cette pratique n'est pas dangereuse car je travaille seul dans mon bureau.
b) Je le compose grâce aux prénoms de mes enfants et de leur âge. Je respecte ainsi les consignes : au moins 8 caractères avec des lettres et des chiffres.
c) J'utilise un mot de passe robuste que je stocke dans un coffre-fort.

Bonne réponse : c. Le post-it est à proscrire car des prestataires extérieurs (ou des collègues indélicats) peuvent intervenir dans votre bureau. Une référence à l'environnement familier est aussi facilement décelable par les spécialistes de l'ingénierie sociale. La méthode préconisée par l'Anssi est de stocker tous ses mots de passe dans un coffre-fort numérique.

9. Lors d'un salon, je récupère des clés USB avec les catalogues des vendeurs.
a) Plus besoin d'emporter de gros dossiers papiers ! Je vais pouvoir consulter les catalogues tranquillement depuis mon ordinateur.
b) Je ne la connecte pas sur mon ordinateur.
c) Je la connecte, mon ordinateur est protégé.

Bonne réponse : b. Les clés USB sont des sacs à virus. Et même si l'ordinateur intègre un antivirus, il peut être contaminé. Ne connectez une clé USB que si vous êtes certain de son intégrité ou si vous l'avez « désinfectée » au préalable.

10. Je viens d'installer une box Wifi chez moi.
a) Je change le code d'accès pour un code plus simple, c'est moins fastidieux.
b) Je garde le mot de passe donné par mon fournisseur de service scotché sous la box.
c) Je change le mot de passe.

Bonne réponse : c. Un réseau Wifi personnel peut être attaqué même si la box est insuffisamment protégée. Il faut avoir un mot de passe robuste, à l'abri des regards extérieurs, qui est changé régulièrement et avec un chiffrement WPA2.

M.C.