Face aux cyberattaques, quelle cyberdéfense ?

30 octobre 2023

Nous le savons bien, les médias s'en font l'écho régulièrement, les cyberattaques se multiplient. Nous avons des exemples récents contre les entreprises, les collectivités locales, les hôpitaux ou encore cet été : Pôle emploi. Autant d'entités qui peuvent détenir beaucoup de nos données personnelles, y compris les plus sensibles.

Le citoyen que nous sommes n'est pas à l'abri, ciblé lui aussi, arnaqué quand une faille le permet. On connaissait le phishing, le smishing… toutes ces techniques qui ont pour but de nous soutirer nos données personnelles en cliquant sur un lien. Se faire passer pour les impôts, la CAF, nous proposer d'acheter une vignette Crit'Air, mettre notre carte vitale à jour, par mail, par texto… Ce que le consommateur craint le plus ? Le détournement de ses comptes bancaires. Bien sûr. Mais toutes nos données sont précieuses et à protéger.

La parade ne passera pas par l'évitement des relations digitales, elles font partie de notre vie. Alors à défaut de renoncer au net, aux réseaux et aux objets connectés , nous devons nous informer, rester vigilants et attentifs à nos droits et à nos pratiques.

Petit tour d'horizon des différentes attaques et des moyens de s'en défendre.

Des attaques incessantes toutes cibles confondues

Des cyberattaques contre les états, les professionnels et aussi contre les consommateurs que nous sommes, il y en a en permanence.

Elles sont de plusieurs types et elles n'ont pas fini de prospérer tant les pirates sont inventifs. Ils ont les compétences, les moyens et ils ont du temps. Inutile désormais d'aller braquer des banques, il est tellement moins risqué de mener un cyber attaque. Quelques exemples :

Le déni de service consistera à bombarder un serveur de demandes qu'il ne pourra pas traiter. La défiguration consistera à changer l'apparence du site. Le piratage bien sûr, qui aura pour but, une fois entré, de prendre le contrôle de l'appareil et voler les informations confidentielles qu'il contient. Mais c'est le rançongiciel ou ransomware, qui constitue la cyberattaque la plus signalée à la CNIL l'an passé . Cette fois, il s'agit de crypter toutes les données et de faire du chantage pour pouvoir reprendre la main et récupérer les données.

Alors ces attaques nous seraient-elles épargnées à titre individuel ? Pas du tout. Ne nous berçons pas de l'illusion que nous sommes trop insignifiant pour les pirates, c'est faux. Notre ordinateur peut parfaitement servir à provoquer un déni de service. Les photos provenant de nos comptes sur les réseaux peuvent être copiées pour créer de faux profils et arnaquer les autres…. Usurper notre identité ? Un cauchemar. Les escrocs en ligne peuvent passer des mois à se faire prendre pour une personne qu'ils ne sont pas et nous soutirer de l'argent. C'est si facile de se cacher derrière un faux profil, sur les réseaux. Ou de se prétendre un de vos amis en détresse à l'étranger grâce à la récupération de son adresse mail. Tout ça, on connaissait. C'est sans fin. Et désormais sans limite car dans la catégorie « chantage » (*qu'on connaissait déjà avec le vol de photos intimes etc.*.), nous pouvons désormais ajouter la « menace de mort ». Le simple citoyen que nous sommes n'est pas à l'abri de recevoir un mail menaçant, émanant d'un prétendu « *tueur à gages* », contactés par un voisin, un collègue ou un proche qui nous veut du mal. La solution ? Payer bien sûr…Notre adresse mail est pourtant, comme notre nom, prénom, numéro de téléphone etc. une donnée personnelle protégée.

Protéger et faire protéger *(par ceux qui les collectent)* nos données personnelles est notre meilleure cyberdéfense.

Notre vie privée nous appartient, on peut trouver de quoi la défendre dans le code civil. Mais nous n'avons pas d'équivalent pour nos données personnelles. Collectées abondamment, elles peuvent être conservées, vendues par ceux qui les détiennent… Elles ne nous « *appartiennent* » pas d'un point de vue juridique. Mais elles sont « *protégées* ». Depuis la loi du 6 janvier 1978, tous les responsables de traitement ont l'obligation de « *prendre toutes les précautions utiles…pour préserver la sécurité des données et, notamment empêcher qu'elles ne soient déformées, endommagées, ou que des tiers non autorisés n'y aient accès* ». Donc la protection ne date pas d'hier et elle s'est enrichie depuis. On vous a beaucoup parlé du RGPD (*règlement général de la protection des*

données).

Ce règlement européen de 2018 a fixé un cadre strict pour une collecte transparente, autorisée, rectifiable, limitée dans le temps… La CNIL est l'autorité qui veille au respect du texte avec un rôle de contrôle et un pouvoir de sanction (https://cnil.fr). N'hésitez pas à lui faire des signalements. Sans compter que vous trouverez sur son site de précieuses informations. On nous propose des options allant d'« *accepter tout* » à « *refuser tout* », en passant par « paramétrer » ou « *personnaliser » (certains cookies sont en effet « indispensables », à ceux-là, nous pouvons dire oui*). Mais le réflexe est tenace d'« *accepter* » pour aller vite…. Soyez patients et pour vos données bancaires, sensibles, ne les enregistrez jamais.

Après le RGPD, l' Union européenne a adopté deux règlements au second semestre 2022. Le règlement sur les services numériques *(Digital Services Act ou DSA*), publié le 12 octobre 2022 intéresse directement les citoyens et consommateurs « *en ligne* ». Il oblige les plateformes numériques, les réseaux sociaux, les moteurs de recherche à nous protéger de la désinformation, des contenus haineux et illicites. Il interdit la publicité ciblée sur les mineurs et celle basée sur des données personnelles sensibles (*à moins que nous ne donnions notre accord explicite).* Ces acteurs ont l'obligation de mettre en place un système de signalement des contenus litigieux, ils devront réagir rapidement, supprimer les comptes qui en publient. Du côté des places de marché, elles devront s'assurer de l'identité des vendeurs, effectuer des contrôles, et mieux nous informer. Pour les plus grands acteurs (*plateformes et moteurs de recherche à plus de 45 millions d'utilisateurs européens actifs par mois*[1]*)*, le texte s'applique depuis le 25 août dernier. Les autres acteurs numériques doivent déjà se préparer, pour eux, les obligations sont applicables à compter du 17 février 2024.

Des mesures nationales vont venir accompagner la mise en œuvre de ce nouveau règlement. Ainsi, bientôt, vous devriez disposer d'un filtre anti-arnaque. C'est ce que prévoit le projet de loi de sécurité numérique actuellement en débat ….. En cas de tentatives frauduleuses d'accès à nos coordonnées personnelles ou bancaires, par mail ou sms, nous pourrons être alertés. Pour peu que nous ayons téléchargé l'application et à la condition que le site ait déjà été signalé et identifié. Connaissant l'imagination sans fin des pirates, la vigilance restera de mise.

Quelle autre actualité en France ?

La loi Cyberscore du 3 mars 2022, applicable à compter du 1er octobre 2023, a introduit un nouvel article L 111-7-2 dans le code de la consommation. Mais nous attendons encore des textes d'application (*seuils de définition des professionnels, critères à prendre en compte*). Ce nouvel article impose aux plateformes en ligne de procéder à un audit de cybersécurité en le faisant réaliser par un prestataire indépendant qualifié par l'Agence nationale de la sécurité des systèmes d'information (ANSSI). Le résultat étant « *présenté au consommateur de façon lisible, claire et compréhensible …. au moyen d'un système d'information coloriel » (dernier alinéa).* Comme le nutriscore (*même présentation du vert au rouge…)*, le cyberscore nous permettra de nous permettra de choisir en connaissance de cause. Le procédé devrait avoir la vertu de pousser les sites concernés à plus d'efforts de sécurité.

Bon à savoir : L'Agence Nationale de Sécurité des Systèmes d'Information (ANSSI) est un service à compétence nationale dédié à la sécurité numérique créé en 2009. Rattachée au Secrétariat général de la défense et de la sécurité nationale, elle dispose d'experts et assure la protection des infrastructures critiques. Elle propose un dispositif spécifique pour recueillir les signalements de lanceurs d'alerte.

Victimes de cybermalveillance, que faire ?

Alerter bien sûr. Prévenez vos contacts, votre banquier …

Porter plainte contre les pirate . Pour eux, des sanctions pénales sont applicables en fonction des infractions commises. Notre code pénal nous offre des outils en fonction des situations, quelques exemples : pour l'atteinte au secret des correspondances (*notre boite mail),* l' article 226-15 du code pénal prévoit un an de prison et 45.000 € d'amende. Pour l'usurpation d'identité par voie de télécommunication qui trouble la tranquillité ou porte atteinte à l'honneur, l'article 226-4-1 du code pénal prévoit un an de prison et 15.000 € d'amende. Pour l'entrave à un système de traitement automatisé de données (*s'introduire, modifier, extraire, entraver fonctionnement*), l'article 323-1 à 323-7 du code pénal prévoit trois à sept ans de prison et 100. 000 à 300.000 € d'amende. Pour une simple tentative, c'est la même chose. Pour la collecte données à caractère personnel, l'article 226-18 code pénal prévoit cinq ans de prison et 300.000 €

***Bon à savoir** : si vous êtes victime d'une escroquerie sur internet, d'un piratage, de chantage, vous pouvez porter plainte « en ligne » sur la plateforme THESEE (traitement harmonisé des enquêtes et signalements pour les e-escroqueries) accessible via France Connect.*

Agir contre les tiers qui détiennent nos données et les protègent mal

Les entreprises, les collectivités qui détiennent nos données ont une obligation de sécurité. S'ils échouent à les protéger correctement, ils peuvent avoir à rendre des comptes devant la CNIL.

La responsabilité peut être également être recherchée au civil pour réparer le préjudice subi. Le code civil permet de l'engager pour faute (*article 1240*) bien sûr mais aussi pour négligence ou imprudence (*art 1241*). Sans compter la possible responsabilité pénale (*art 226-17 du code pénal*).

***Le saviez-vous ?** un tiers des sanctions prononcées en 2022 par la CNIL concernait des manquements à l'obligation de sécurité !*

Savoir que nous avons des outils juridiques pour nous défendre, c'est bien ! Mais pouvoir s'en servir, c'est mieux. Car c'est tout le problème avec les pirates et les escrocs du net, ils sont difficiles à attraper, souvent à l'étranger. Mieux vaut prévenir.

Notre cybersécurité passera par nous. On ne le dira jamais assez, nous sommes le premier rempart face à la cybermalveillance. Cela peut étonner mais de nombreux citoyens ne prennent pas la précaution élémentaire de protéger l'usage de leur outil par un mot de passe… C'est le B.A. BA, Il vous faut un mot de passe solide, unique (*un par site)* et absolument confidentiel. La CNIL conseille 12 caractères au moins, mêlant des lettres (*majuscules et minuscules*), des chiffres, des caractères spéciaux. Rien qui ne soit facile à deviner (*suite, dates importantes pour nous*). Il faut toujours se déconnecter et éviter le WIFI public. Toujours télécharger à partir de sites officiels… Personne ne doit pouvoir entrer dans notre ordinateur, dans nos données…

Protégeons nos outils. Tous doivent être protégés, codés, mis à jour régulièrement. Il faut user d'antivirus, faire des sauvegardes… Contrôler régulièrement les connexions (*date et heure*), ainsi que les données (*numéro de*

téléphone et adresse mail) de récupération. Pour être certain que personne ne prend la main. À chaque fois que l'authentification renforcée est possible, il faut l'activer.

[1] La Commission Européenne a déjà publié des noms : Alibaba AliExpress , Amazon Store, Apple AppStore, Booking.com, Facebook, Google Play, Google Maps, Google Shopping, Instagram, LinkedIn, Pinterest, Snapchat, TikTok, X, Wikipedia, YouTube, Zalando, Bing et Google Search.

Pour INDECOSA-CGT Fiche d'information N° 84 / 28 octobre 2023