Ils font la cyber en Occitanie

Entretiens avec :

Orange
Cyber'Occ
Predicta Lab…

P. 2-3

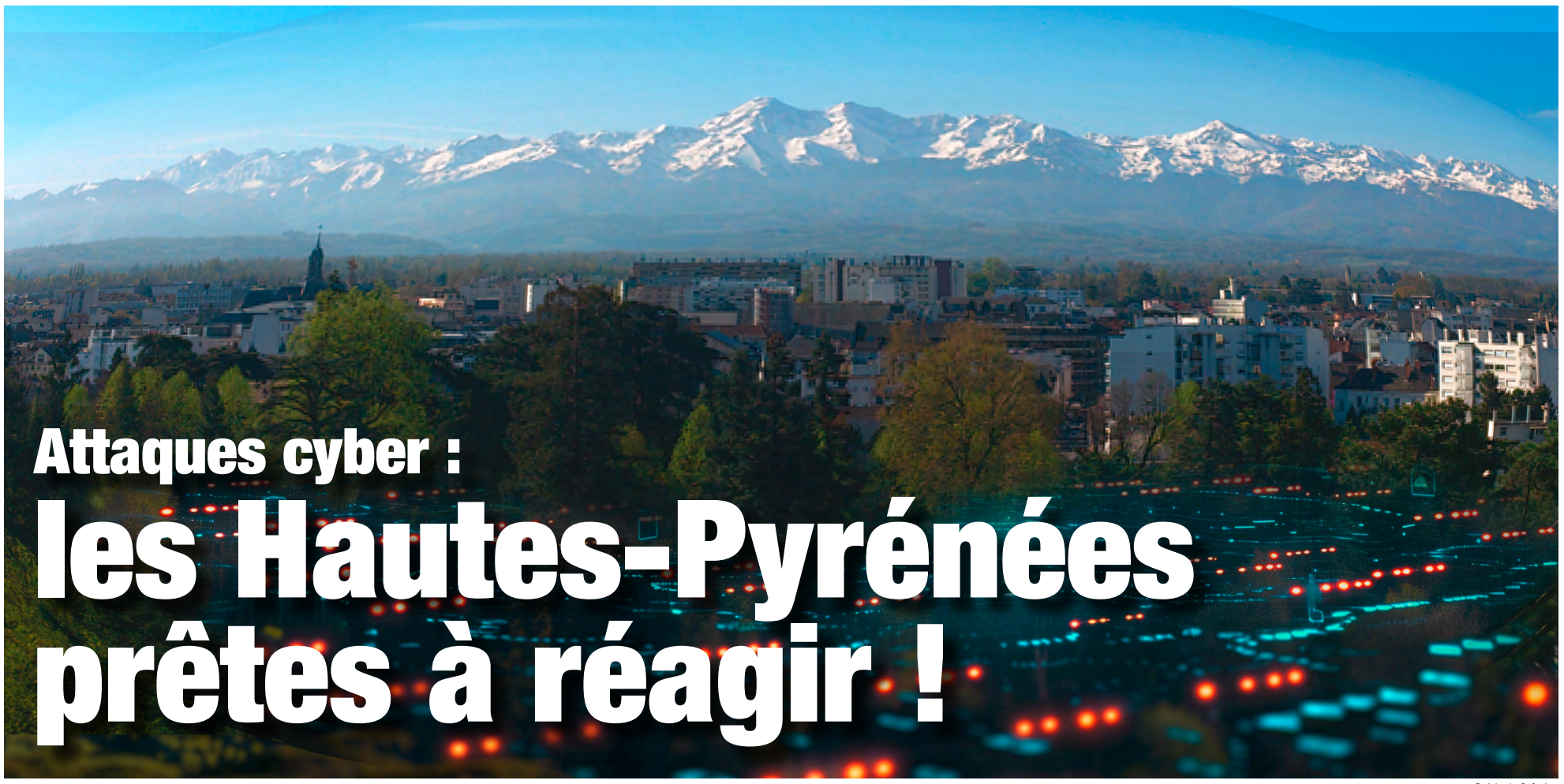
le journal de la CYBER

Parlez-vous cyber ?
Quelques définitions au fil des pages

+ Le coin juridique P. 3

Mises à jour, WPA3…
Les conseils de notre expert Ajyle
pour se protéger efficacement P. 4

#65* - Septembre 2024



Attaques cyber : les Hautes-Pyrénées prêtes à réagir !

© Adonis Créative

ÉDITO

Tous connectés, tous vigilants

© Département des Hautes-Pyrénées

D'ici la fin de l'année, les Hautes-Pyrénées seront l'un des tout premiers territoires ruraux de France à être entièrement raccordés à la fibre optique. L'aboutissement d'un chantier exceptionnel débuté en 2018 à la suite d'un accord historique entre le conseil départemental et l'opérateur Orange, qui a entièrement financé sur ses fonds propres son déploiement. Garantir d'ores et déjà à 95 % des foyers haut-pyrénéens une éligibilité au très haut débit est pour le territoire un atout considérable pour son attractivité et son développement.
Le numérique est désormais indispensable à notre quotidien. Cependant, il comporte aussi son lot d'impondérables. **Que ce soit pour les particuliers, les collectivités ou bien les entreprises, nous devons rester vigilants face aux différentes tentatives de cyberattaques et d'escroqueries. Le Département est conscient de cet enjeu.** Notre administration est la plus importante du territoire et repose sur une architecture informatique solide.
Des investissements continus sont réalisés pour assurer une protection optimale de nos systèmes. Des campagnes d'information et des mises en situation sont régulièrement organisées en interne pour sensibiliser nos agents aux bonnes pratiques à adopter. Les conseillers numériques de notre Régie Haut Débit se tiennent également à disposition des élus et agents des collectivités locales pour les accompagner et les aider à maîtriser les différents outils de cybersécurité.
Pour le Département, il est ainsi nécessaire de participer à cette prise de conscience, et d'accueillir à Tarbes pour cela un événement comme le CyberTour. Cette journée, riche en échanges, offre l'opportunité de bénéficier de l'avis d'experts et de connaître les toutes dernières avancées en matière de cybersécurité.

Michel Pélieu
Président du conseil départemental des Hautes-Pyrénées

Vous avez dit CyberTour ?

Organisé par Projet X, ce **programme de conférences locales interactives au format TED** permet aux pros, experts et novices de partager leurs expériences autour de la cybersécurité. **Keynotes**, **tables rondes** et **ateliers** rassemblent des intervenants de premier plan pour offrir aux participants une compréhension approfondie des défis de demain.

REGARDS CROISÉS

La Régie Hautes-Pyrénées Haut Débit (HPHD), créée par le conseil départemental des Hautes-Pyrénées, gère le réseau de fibre optique sur le territoire et veille aussi aux bons usages du numérique.

© Département des Hautes-Pyrénées

La Régie compte deux conseillers numériques qui accompagnent les collectivités locales, élus et services, *via* des missions de diagnostic, de conseils pour l'achat de matériel, de suivi de logiciels et d'assistance technique ponctuelle. Ils insistent particulièrement sur la sauvegarde, la sécurisation et les bonnes pratiques à adopter.
À la rentrée de septembre, dans le cadre de la feuille de route France Numérique Ensemble, la Régie a intégré un conseiller numérique coordinateur. Cette nouvelle étape permet de fixer les objectifs à atteindre dans le cadre de l'inclusion numérique pour les 3 ans à venir sur le territoire départemental. Il est prévu dans ce partenariat l'accompagnement, par l'association Coll.in et le hub régional RhinOcc, de la vingtaine de conseillers numériques déjà en place,
le Département apportant sa part par ses compétences sociales, et notamment la Régie, grâce à sa connaissance des besoins des collectivités locales. L'élaboration de cette feuille de route, avec un contenu statistique, cartographique, des données socio-économiques, se fera en relation étroite avec tous les acteurs. Elle est portée par une gouvernance tripartite alliant État, Département et Régie. Tous vont devoir s'approprier la mise en place de politiques publiques pour permettre à l'ensemble de nos concitoyens, acteurs publics et décideurs économiques d'accéder facilement et en sécurité aux données numériques. Enfin, une réflexion est actuellement en cours pour créer une entité départementale qui permettrait aux collectivités départementale et locales de mutualiser offres de services et aménagement numériques.

Nicolas Datas-Tapie
Président de la Régie Hautes-Pyrénées Haut Débit, conseiller départemental des Hautes-Pyrénées

© Jean-Marc Abbadie

C'est avec plaisir que je viens témoigner de l'excellence de la mission effectuée pour ma commune par la Régie Hautes-Pyrénées Haut Débit, qui a élaboré un diagnostic de notre système informatique en présence de la secrétaire de mairie, l'utilisatrice principale, mis en place une migration vers une nouvelle boîte mail et sécurisé l'installation d'une extension de logiciel comptable et administratif. Compte tenu de l'évolution rapide des matériels et logiciels, il est important dans l'avenir de développer cette expertise pour assister les communes ne disposant pas de services techniques spécialisés, et éviter ainsi la fracture numérique qui serait préjudiciable à nos administrés et notre territoire.
Les collègues élus ne doivent pas hésiter à demander de l'aide auprès des conseillers numériques de la Régie, compétents, bienveillants et disponibles. Le numérique est un domaine complexe et sensible qui mérite de prendre sur soi et d'accepter avec humilité de se faire accompagner. Ce n'est pas un domaine intuitif pour nombre d'élus locaux, voire d'équipes de secrétariat qui n'auraient pas reçu de formation initiale.

Jean-Marc Abbadie
Maire d'Agos-Vidalos

ORANGE CYBERDEFENSE, FORMER ET PROTÉGER À TOUS NIVEAUX

La filiale de l'opérateur télécom, acteur majeur de la cybersécurité en Europe, emploie 120 experts dans le Sud-Ouest. Entretien avec Nicolas Brochot, délégué régional Orange Occitanie.

© Orange

Quelle est la vision d'Orange concernant l'importance du CyberTour pour la communauté de la cybersécurité?

Orange est l'acteur de confiance qui donne à chacune et à chacun les clés d'un monde numérique responsable. Les défis en matière de cybersécurité sont nombreux et cet événement est une opportunité majeure pour sensibiliser les citoyens, les entreprises et les collectivités du territoire aux enjeux de la sécurité numérique. En tant qu'opérateur télécom, notre objectif est de permettre à tous de profiter des avantages du très haut débit, notamment dans les Hautes-Pyrénées où Orange déploie la fibre optique entièrement sur ses fonds propres, tout en garantissant la protection et la confidentialité des données. Notre filiale, Orange Cyberdefense, acteur majeur de la cybersécurité en France et en Europe, emploie 120 experts dans le Sud-Ouest.

> **La majorité des attaques touche des TPE, PME et collectivités. Il est donc important d'être présent localement.**

Comment Orange Cyberdefense répond-elle aux principaux défis de cybersécurité que le monde numérique affronte aujourd'hui ?

Dans un contexte de forte croissance des cyberattaques, Orange Cyberdefense a pour mission de venir au secours de nombreux clients qui sont victimes de hackers malintentionnés, avec demandes de rançons à la clé, et toujours plus expérimentés. Pour répondre localement à des besoins en forte croissance, Orange propose à ses clients un service sur mesure, avec des nouvelles offres de surveillance et de protection contre les menaces cyber, qui s'incarnent autour du Micro-SOC, une solution qui permet de protéger les postes de travail et les serveurs d'une entreprise. Son arsenal est complété par des offres innovantes en matière de gestion de crise, sécurité du cloud, environnements industriels et objets connectés, sans oublier des programmes de formation aux risques cyber. Orange a choisi de s'implanter en région car la majorité des attaques touche des TPE, PME et collectivités. Il est donc important d'être présent localement et d'analyser les besoins spécifiques de chacun. Pour le grand public, nous venons de lancer Orange Cybersecure, une solution inédite contre les fraudes sur Internet et par téléphone.

Quel rôle Orange Cyberdefense jouera-t-elle pour façonner l'avenir de la cybersécurité ?

L'évolution de la cybersécurité dans les années à venir pourrait inclure une augmentation des attaques basées sur l'intelligence artificielle. Avec la numérisation croissante des services publics, des entreprises et des infrastructures critiques, il est essentiel de garantir la protection des données sensibles et la continuité des activités. Orange Cyberdefense jouera un rôle-clé en développant des solutions de surveillance, de protection des données et de renforcement de la résilience des infrastructures critiques. La sensibilisation et la formation des acteurs des territoires seront prioritaires pour promouvoir la sécurité numérique. Orange Cyberdefense apportera des services pour aider les entreprises et les citoyens à adopter les bonnes pratiques en matière de cybersécurité.

www.orangecyberdefense.com/fr/

© Christophe Fleury

« Le CyberTour est clairement une *place to be* »

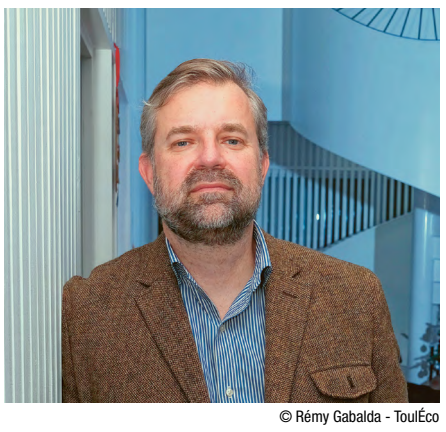
L'ANSSI, agence française de référence en matière de sécurité du numérique, est en charge de promouvoir les bonnes pratiques envers les entités publiques comme privées. **Il faut que les actions de prévention en cybersécurité ruissellent sur le territoire**, et le CyberTour des Hautes-Pyrénées fait justement partie de ces actions. Les défis actuels auxquels la France est confrontée tournent autour de la sécurisation des J.O., mais également de la **mise en œuvre de la directive européenne NIS 2**, qui permettra de mieux sécuriser certains domaines, en complément des opérateurs de services essentiels (OSE) et des opérateurs d'importance vitale (OIV). La directive NIS 2 est un changement de paradigme : on passe de quelques centaines d'opérateurs régulés à quelques milliers, ce qui nécessite un passage à l'échelle supérieure aussi bien pour les prestataires que pour le régulateur (ANSSI). Cette directive rentrera en application courant octobre 2024 et fait l'objet de consultations vis-à-vis des associations d'élus comme des fédérations métiers.

Christophe Fleury
Délégué à la sécurité numérique pour l'Occitanie – Agence nationale de la sécurité des systèmes d'information (ANSSI)

cyber.gouv.fr/decouvrir-lanssi

AJYLE, CATALYSEUR DE TRANSFORMATION NUMÉRIQUE ET SOCIÉTALE

La société Ajyle accompagne les organisations publiques et privées dans leur parcours de transition numérique. Samuel Cette, l'un de ses cofondateurs, nous dévoile son offre.



© Rémy Gabalda - ToulÉco

Quelles sont les spécificités d'Ajyle ?

Nous offrons des formations spécialisées, des conseils stratégiques et un accès à des compétences expertes *via* le modèle des salariés à temps partagé. En mettant l'accent sur l'IA, la cybersécurité et les technologies émergentes, nous dotons nos clients des outils et connaissances nécessaires pour naviguer dans un paysage numérique en constante évolution, donc instable.

> **La mesure de l'efficacité s'envisage, […] cela est unique, sur le suivi longitudinal des incidents de sécurité.**

Comment Ajyle intègre-t-elle les aspects de cybersécurité et de sécurité économique dans ses services de conseil et de formation ?

À travers des formations dédiées, des audits de sécurité et des conseils stratégiques pour renforcer la résilience des organisations face aux menaces numériques, à l'augmentation des attaques ciblées, à l'émergence de nouvelles formes de malwares.

Quelles motivations vous poussent à participer au CyberTour ?

En participant au CyberTour, Ajyle cherche à sensibiliser davantage les organisations aux enjeux de la cybersécurité, partager son expertise, raison pour laquelle nous axons nos interventions sur la transmission d'un message clair et la présentation de solutions concrètes pour y faire face.

Quelle approche adoptez-vous pour former et sensibiliser les organisations et leurs collaborateurs à la cybersécurité et à la sécurité économique ?

Notre approche repose sur des programmes obligatoirement sur mesure, des ateliers pratiques et des séminaires interactifs, conçus pour engager et acculturer les participants. La mesure de l'efficacité s'envisage, certes, à travers des évaluations avant et après formation, des retours d'expérience, mais surtout, et cela est unique, sur le suivi longitudinal des incidents de sécurité.

www.ajyle.fr

PREDICTA LAB, LA PUISSANCE DE L'OSINT

Baptiste Robert est un « hacker éthique » de renommée internationale. Il a cofondé Predicta Lab, une start-up toulousaine spécialisée dans le renseignement en sources ouvertes (OSINT).

Que propose Predicta Lab ?

Notre pôle technique développe des outils d'investigation et de protection des données, tandis que notre pôle d'analyse produit des rapports d'empreintes numériques qui permettent à notre clientèle d'évaluer son exposition en ligne et d'être accompagnée dans la réduction de cette exposition.

Pourquoi participer au CyberTour ?

Chez Predicta Lab, notre mission est de protéger les individus et les organisations contre les menaces numériques en exploitant la puissance de l'OSINT. Nous sommes engagés dans la sensibilisation et la formation à la protection des données. Par ailleurs, étant fièrement toulousains, nous sommes particulièrement enthousiastes à l'idée de participer à cette initiative dans la région Occitanie.

> **Nous sommes engagés dans la sensibilisation et la formation à la protection des données.**

© Predicta Lab

Quelles sont vos actualités ?

Je suis allé à Washington récemment, aux États-Unis, où j'ai représenté Predicta Lab aux côtés de la « CyberTaskForce ». Là-bas, j'ai pu rencontrer et échanger avec les départements de la Justice et de la Défense, ainsi qu'avec la Maison Blanche. Côté innovation, de nouvelles sources sont régulièrement ajoutées à Predicta Search, notre moteur de recherche d'empreinte numérique, et nos développeurs avancent sur Predicta Graph. Cette nouvelle solution de visualisation des données sera bientôt disponible !

www.predictalab.fr

Cyber' VOC

• Hacker éthique : Professionnel de la cybersécurité qui utilise ses compétences pour détecter et corriger les vulnérabilités des systèmes informatiques de manière légale. Son objectif ? Améliorer la sécurité en identifiant les failles avant les cyberattaques. Il agit avec l'autorisation des propriétaires des systèmes.

CYBER'OCC, LA RÉPONSE RÉGIONALE

La Région Occitanie a lancé en 2022 Cyber'Occ, son centre régional dédié à la cybersécurité. Rencontre avec Marc Sztulman, conseiller régional délégué au numérique et président de Cyber'Occ.

© Région Occitanie – DR

Quel rôle joue Cyber'Occ en Occitanie en matière de cybersécurité ?

C'est d'abord un centre de réponse aux incidents (« CSIRT ») ou service d'urgence cyber public gratuit, que les entreprises, les associations et les collectivités peuvent appeler en cas de cyberattaque pour être conseillées. C'est aussi un centre de ressources et d'information, pour aider les acteurs économiques à se prémunir au mieux contre les cyber-risques, les inscrire dans une démarche *secure by design* s'ils développent des produits numériques, et également pour animer la filière cybersécurité en Occitanie : sensibilisation auprès des TPE, PME, associations, collectivités territoriales, organisations des partenariats avec l'ensemble des corps intermédiaires, ordres professionnels, syndicats, pour diffuser la culture de la cybersécurité auprès de leurs adhérents…

Quels sont les principaux objectifs de Cyber'Occ en participant au CyberTour ?

C'est une formidable occasion de faire connaître notre action dans nos 13 départements. Il faut que les acteurs économiques de la région connaissent notre service d'assistance et, s'ils sont malheureusement attaqués, aient le réflexe de faire appel à nous pour limiter les impacts. Ce service est ouvert depuis 1 an et joignable au 0 800 71 13 13.

> **« La volonté régionale, c'est de porter la cybersécurité auprès de tous les acteurs. »**

Comment le CyberTour s'inscrit-il dans la mission globale de Cyber'Occ ?

Trop souvent, on considère que la cybersécurité, c'est une question de métropole, de grands groupes, et que finalement, les acteurs plus petits ne sont pas concernés. Or, la volonté régionale, c'est de porter la cybersécurité auprès de tous les acteurs, car ils sont potentiellement tous victimes. Ainsi, ces événements s'inscrivent naturellement dans la mission globale de notre agence.

Quelles sont les perspectives d'avenir pour Cyber'Occ ?

Tout d'abord, nous allons avoir dans les prochains mois la labellisation « Campus Cyber ». Cette reconnaissance de notre travail s'accompagnera d'un enrichissement de notre offre de services, faisant de Cyber'Occ le véritable tiers de confiance en matière de cybersécurité dans notre région. Nous allons très rapidement ouvrir des Campus Cyber, dans le Sicoval et à Montpellier. Puis d'autres viendront à brève échéance.

Quels sont les défis spécifiques à la région Occitanie en matière de cybersécurité ?

Notre région connaît 2 types de défis, les défis classiques qui s'appliquent à toutes les régions et des défis particuliers, eu égard aux spécificités de notre tissu économique et notamment industriel. L'Occitanie est un grand centre de recherche et développement, et donc particulièrement ciblée en matière d'intelligence économique.

Comment voyez-vous l'évolution de la cybersécurité en Occitanie dans les années à venir ?

Il va y avoir une multiplication des attaques et, si on n'y prend pas garde, des effets de ces attaques. Notre rôle est de limiter tant les effets que le nombre d'attaques. Mais il faut savoir rester modeste. Il s'agit d'un combat infini. Comme le disait Platon, « Seuls les morts connaissent la fin de la guerre. »

www.cyberocc.com

DÉFINITIONS

CSIRT (*computer security incident response team*)
Une équipe spécialisée dans la gestion des incidents de sécurité informatique. Il existe des CSIRT d'entreprise, sectorielles, gouvernementales, académiques, régionales, nationales…

CYBERSÉCURITÉ EN OCCITANIE : CHIFFRES-CLÉS

De 3 000 à 6 000
personnes mobilisées par la cybersécurité, un nombre qui devrait doubler dans les 2 ans.

150 millions d'euros
dédiés entre 2023 et 2027 au contrat de filière numérique, qui comprend de nombreuses actions destinées à la cybersécurité.

Près de 200 entreprises
régionales spécialisées en cybersécurité.

Une quarantaine d'universités, écoles et laboratoires
impliqués dans la région.

Source : laregion.fr

Toute structure peut subir une cyberattaque. Quid au niveau juridique ? Les conseils de **notre experte**.

#FAQ : JURIDIQUE

POURQUOI SE FAIRE ACCOMPAGNER PAR UN EXPERT EN CAS DE CYBERATTAQUE ?

Une entreprise ou toute autre structure victime d'une cyberattaque peut prendre plusieurs mesures pour faire face à la situation, en amont et en aval de la crise. Entretien avec Philippine Soucaze-Suberbielle, avocate en droit de la propriété intellectuelle et industrielle au sein du cabinet Loyve Avocats.

© Loyve Avocats

1. QUEL EST LE 1ER RÉFLEXE À ADOPTER ?

EMPÊCHER L'ATTAQUE DE SE PROPAGER

- Le premier réflexe doit être de prévenir la personne référente (en interne ou en externe) formée et sensibilisée sur cette problématique, afin de définir l'origine de l'attaque et de déterminer les dommages causés.
- Si les appareils infectés sont identifiés, il faut veiller à bien les déconnecter et ne surtout pas les éteindre, car cela effacerait d'éventuelles preuves. En revanche, il vaut mieux éteindre les appareils non infectés afin que l'attaque ne les contamine pas.

INFORMER ET DÉPOSER PLAINTE

- En cas de violation de données, l'entreprise a l'obligation de le notifier à la CNIL (Commission nationale de l'informatique et des libertés) dans les 72 heures suivant l'attaque.
- Dans ce même délai, l'entreprise doit également déposer plainte au commissariat ou à la gendarmerie la plus proche pour accès frauduleux à son système de données. C'est l'une des conditions à remplir pour que l'entreprise puisse, par la suite, être indemnisée par son assureur. Cela va également permettre de dater et circonstancier le dommage, de déclencher une enquête et de dégager la responsabilité de l'entreprise en cas de propagation de l'attaque à d'autres victimes de cette même cyberattaque.
- Les entreprises peuvent également être tenues de notifier les personnes tierces concernées par l'incident si celui-ci concerne leurs données.

2. EST-CE QUE L'ENTREPRISE PEUT ÊTRE TENUE RESPONSABLE ?

RESPONSABILITÉ DE L'ENTREPRISE
La responsabilité d'une entreprise victime d'une cyberattaque peut être engagée lorsque celle-ci entraîne des préjudices pour des tiers, tels que des clients, fournisseurs ou tout autre partenaire. L'entreprise pourra donc être tenue responsable en cas de manquement à une obligation de prudence ou de sécurité des données, ou encore en cas de défaut de notification de l'incident aux autorités compétentes et aux personnes.

CADRE RÉGLEMENTAIRE ET LÉGAL
Il revient aux entreprises d'assurer la protection des données qu'elles vont être amenées à traiter, sous-traiter ou conserver. Cela passe notamment par l'un des grands principes du règlement général sur la protection des données (RGPD) : la minimisation des données, qui implique que les entreprises ne doivent collecter et traiter que les données personnelles strictement nécessaires à des fins spécifiques, non seulement afin de protéger la vie privée et les libertés fondamentales des personnes, mais également pour qu'en cas de cyberattaque, le moins de données possibles soient en cause.

SANCTION ET ASSURANCE

- La sanction pourra être civile, pénale et/ou administrative. Les amendes, notamment, dépendront de la gravité de l'attaque et/ou de la négligence de la société.
- Afin de se protéger contre les conséquences financières, il est fortement conseillé aux entreprises de souscrire à une assurance cyber-risques.

3. QUEL ACCOMPAGNEMENT PROPOSEZ-VOUS ?

- Notre cabinet accompagne les entreprises sur toutes les questions juridiques liées à la cybersécurité. Nous recommandons à nos clients d'anticiper les risques potentiels en les accompagnant dans la mise en place, en amont, d'outils et de dispositifs permettant la mise en conformité RGPD.
- Nous préconisons également la formation des équipes afin de leur permettre d'intégrer des process en interne qui facilitent l'application de bonnes pratiques. Le panel d'actions est large et peut être adapté au cas par cas, de l'audit et de la prévention des risques à la rédaction ou l'actualisation des contrats et de la documentation juridique.
- En cas de cyberattaque, nous accompagnons également nos clients dans toutes leurs démarches ainsi que dans les phases contentieuses. Notre objectif est de sécuriser nos clients sur ces enjeux spécifiques.

www.loyve-avocats.com

Dans le vaste univers de la cybersécurité, naviguer à travers les menaces peut s'avérer un défi. Quelques conseils pratiques de notre **expert Ajyle.**

LES MISES À JOUR

COMMENT CONTRIBUENT-ELLES À MA SÉCURITÉ ?

Les mises à jour des appareils contiennent souvent des correctifs pour les vulnérabilités de sécurité récemment découvertes.

LES BONNES PRATIQUES

1. ACTIVEZ LES MISES À JOUR AUTOMATIQUES POUR VOTRE SYSTÈME D'EXPLOITATION ET VOS APPLICATIONS

POURQUOI C'EST IMPORTANT

Les mises à jour des logiciels incluent souvent des correctifs de sécurité pour les vulnérabilités récemment découvertes qui pourraient être exploitées par des cybercriminels. En activant les mises à jour automatiques, vous vous assurez que votre système d'exploitation et vos applications bénéficient des dernières protections sans délai.

COMMENT PROCÉDER

- Pour le système d'exploitation, accédez aux paramètres de mise à jour de votre système. Sur Windows, vous pouvez trouver cette option dans « Paramètres » puis « Mise à jour et sécurité ».
- Sur macOS, recherchez « Réglages Système » puis « Mise à jour logicielle ». Activez l'option pour installer automatiquement les mises à jour du système.
- Pour les applications sur PC, vérifiez les préférences ou les paramètres de chacune pour activer les mises à jour automatiques.
- Pour les applications mobiles, vous pouvez généralement configurer cela dans le magasin d'applications de votre appareil (comme l'App Store pour iOS ou Google Play pour Android), leur permettant ainsi de se mettre à jour automatiquement lorsqu'une nouvelle version est disponible.

2. REDÉMARREZ RÉGULIÈREMENT VOS APPAREILS POUR APPLIQUER LES MISES À JOUR

POURQUOI C'EST IMPORTANT

Bien que certaines mises à jour puissent être appliquées en arrière-plan sans nécessiter de redémarrage, de nombreuses mises à jour importantes, en particulier celles du système d'exploitation, requièrent de redémarrer de l'appareil pour finaliser leur installation. Cela assure qu'elles sont toutes correctement appliquées et que les correctifs de sécurité prennent effet immédiatement.

COMMENT PROCÉDER

- Planifiez des redémarrages réguliers en définissant une routine pour redémarrer vos appareils, par exemple une fois par semaine. Cela peut être particulièrement pertinent pour les ordinateurs que vous utilisez quotidiennement. Pour les appareils mobiles, profitez des redémarrages suggérés par les mises à jour du système ou redémarrez-les manuellement de temps en temps.
- N'ignorez pas les notifications ! Lorsque votre système d'exploitation indique qu'un redémarrage est nécessaire pour appliquer une mise à jour, ne le reportez pas indéfiniment. Planifiez-le à un moment qui vous convient, ou laissez-le se faire automatiquement pendant les heures où vous n'utilisez pas activement votre appareil.

5 entreprises sur 6

déclarent **ne pas disposer de moyens spécifiques** pour la sécurité de leur système d'information.

94 %

des failles de sécurité sont le fruit d'**erreurs humaines**.

Source : BusinessDIT

DÉFINITIONS

Système d'exploitation
Aussi abrégé OS en anglais et SE en français, c'est un logiciel qui assure la gestion des ressources matérielles d'un ordinateur (processeur, mémoire, interface utilisateur, fichiers, périphériques, etc.) et permet l'exécution des programmes et des applications. C'est le pilier fondamental de tout système informatique.

VPN (*virtual private network*)
Un réseau privé virtuel renforce votre confidentialité en ligne et sécurise vos connexions. Sans VPN, vos activités en ligne peuvent être facilement suivies par les fournisseurs de services Internet, les annonceurs et même les cybercriminels, car votre adresse IP réelle est exposée. Vos données personnelles et votre historique de navigation risquent d'être compromis. En bonus : un VPN vous donne l'accès à des contenus en ligne dont certains pays ou fournisseurs de services Internet limitent l'accès, en contournant les restrictions géographiques !

L'INFO EN +

Protéger votre réseau domestique

C'est crucial pour la sécurité de vos dispositifs connectés : changer le nom et le mot de passe par défaut de votre réseau Wi-Fi est nécessaire, mais ça ne suffit pas.

1. ACTIVEZ LE CHIFFREMENT WPA3 SUR VOTRE ROUTEUR

Pourquoi ? WPA3 est la dernière norme de sécurité pour les réseaux Wi-Fi, offrant une meilleure protection contre certaines attaques par rapport aux versions précédentes comme WPA2.

Comment ?

- Vérifiez si votre routeur supporte WPA3. Pour cela, consultez la documentation de votre routeur ou recherchez son modèle en ligne.
- Accédez à l'interface administrateur de votre routeur puis aux paramètres de sécurité Wi-Fi.
- Sélectionnez WPA3 comme méthode de chiffrement. Si vos appareils ne supportent pas WPA3, vous pourriez avoir besoin d'utiliser un mode mixte (WPA2/WPA3), mais visez à ce qu'à terme tous les appareils soient compatibles avec WPA3.

2. UTILISEZ UN RÉSEAU VPN POUR CHIFFRER VOTRE TRAFIC INTERNET

Pourquoi ? Un VPN crypte votre trafic Internet, empêchant ainsi les autres de voir les informations que vous envoyez ou recevez, même sur les réseaux Wi-Fi publics non sécurisés, vulnérables aux attaques de type « homme du milieu ».

Comment ?

- Choisissez un fournisseur VPN réputé qui respecte une politique stricte de non-conservation des journaux d'activités et offre un cryptage fort.
- Installez l'application VPN fournie par votre fournisseur sur tous vos appareils.
- Activez le VPN chaque fois que vous vous connectez à Internet, surtout si vous êtes sur un réseau Wi-Fi public. La plupart des fournisseurs proposent des options pour connecter automatiquement vos appareils lorsque vous accédez à de nouveaux réseaux Wi-Fi.

Le *Journal de la cyber* est édité par **Projet X** - N° 65 (* numéro bêta) – septembre 2024
Directeur de la publication : Samuel Cette
Comité éditorial : Jean-Christophe Arguillère, Samuel Cette, Célie Cousinié, Ingrid Gautier, Martin Venzal
Rédaction, création graphique et maquette : Adonis Créative – **Impression :** Techni Print imprimerie