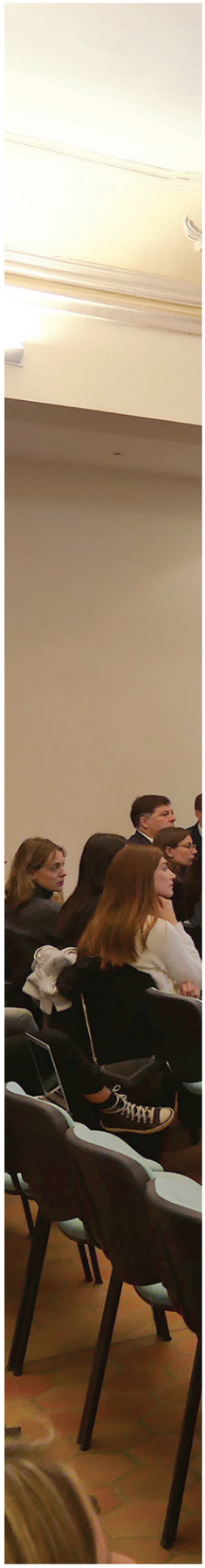
Cyberdélinquance : le droit en rempart des entreprises



Le colloque de l'Afdit Sud-Est (Association française de droit de l'informatique et de la télécommunication) organisé à Aix-en-Provence le 7 décembre par Me Nicolas Courtier, avec les bareaux de Marseille et Aix-en-Provence, a rappelé que le droit est en première ligne dans la lutte contre la cyberdélinquance, notamment celle qui vise les entreprises.

Dossier réalisé par Frédéric Delmonte
@DelmonteFred


2 milliards
de coût de préjudice
indirect
200 000
entreprises victimes
par an
800 millions
de nouveaux internautes
dans les prochaines
années.

© F.D.

Attaques informatiques : deux milliards de préjudice par an en France

Philippe Laurier, économiste et chercheur à l'Institut de recherche technologique (IRT) SystemX, a réalisé une étude sur la nature des PME soumises aux attaques informatiques.

© F.D

Philippe Laurier, économiste et chercheur à l'IRT SystemX.

« Les entreprises du second œuvre dans le bâtiment, les cabinets d'avocats figurent parmi les professions les plus touchées, parce qu'elles sont au contact avec de nombreux intervenants et échangent beaucoup de mails », a constaté Philippe Laurier.

Economiste et surtout chercheur à l'Institut de recherche technologique (IRT) SystemX, Philippe Laurier a réalisé une étude sur le coût des cyberattaques sur les petites entreprises. Un constat : « il est difficile d'identifier les attaques et leur nature, car les PME font rarement remonter leurs cyberattaques ». Toutes les entreprises peuvent faire l'objet d'attaques, d'intru-

sions dans le système informatique ou d'actes malveillants. « Les entreprises du second œuvre dans le bâtiment, les cabinets d'avocats figurent parmi les professions les plus touchées, parce qu'elles sont au contact avec de nombreux intervenants et échangent beaucoup de mails », a constaté Philippe Laurier.

NATURE DES ATTAQUES

Ces attaques ont un coût élevé sur notre économie. Philippe Laurier parle de 2 milliards d'euros de coût de préjudice indirect pour l'économie, « en perte de production, arrêt du travail, etc. ». Pourtant, les sommes volées sont faibles : 200 millions d'euros par an. C'est le nombre d'entreprises victimes d'un chiffrement de données qui est élevé : 200 000 par an. Même si elle est rare, la fraude au président concerne souvent de gros montants. « Mais la plupart du temps, on arrive à retracer les attaques. »
La majorité des attaques ne coûte pas cher, mais elles sont nombreuses. « Quand vous avez 3000 euros de préjudice, vous allez ajouter une demi-journée à aller porter plainte ? Si vous avez un préjudice de quelques milliers d'euros, vous n'irez pas forcément porter plainte », a constaté Philippe Laurier.

UNE PROBABILITÉ D'ATTAQUE ÉLEVÉE

La probabilité d'avoir une attaque reste importante : « sur trente entreprises, une sera victime d'une attaque, a minima ». « On est sur une démocratisation des attaques. Des petites attaques, qui polluent les victimes, font perdre du temps et arrivent à détruire des entreprises. Des attaques peuvent créer des nuisances sur plusieurs mois et l'entreprise va s'affaiblir et ne s'en sortira pas », analyse ce spécialiste.
« La trajectoire actuelle de développer le zéro papier, d'accélérer la transition numérique va engendrer une augmentation des attaques », prédit Philippe Laurier.

L'Anssi, bras armé de la France

Moïse Moyal, délégué régional Paca-Corse à la sécurité numérique de l'Agence nationale de sécurité des systèmes d'information, a expliqué comment l'Anssi peut aider le monde économique.

L'Agence nationale de sécurité des systèmes d'information (Anssi) est une agence d'Etat « pas très connue, pourtant, nous avons énormément de missions », reconnaît Moïse Moyal, son délégué régional Paca-Corse à la sécurité numérique. Elle est rattachée au service du Premier ministre, via le secrétariat général à la défense. « On met en place des visas de sécurité pour certifier des prestataires de confiance que l'on va recommander après évaluation. On assiste les entreprises qui sont des OIV, Opérateurs d'importance vitale, essentiels pour le fonctionnement de la nation », explique ce dernier.

L'ARMÉE EN EXEMPLE

« En fait, elle ne concerne pas forcément l'ensemble des entreprises, même si notre souhait est que cette liste soit élargie. » L'expérience de l'armée est importante en France en matière de lutte contre les cyberattaques. « La loi de programmation militaire de 2013, qui consiste à améliorer la sécurité informatique des entreprises essentielles à l'Etat, nous a permis de développer un certain nombre de compétences en la matière. »

NIS. « On n'en a pas beaucoup parlé à l'époque et pourtant… », regrette le représentant de l'Anssi. La directive Network and Information System Security (NIS) poursuit un objectif majeur : assurer un niveau de sécurité élevé et commun pour les réseaux et les systèmes d'information de l'Union européenne. Elle a été adoptée par les institutions européennes le 6 juillet 2016.

> « On nous appelle les cyber-pompiers de l'Etat. On intervient auprès des entreprises victimes d'attaques. On fait une vingtaine d'interventions par an dans de grandes d'entreprises qui, bien entendu, ne veulent pas forcément communiquer », souligne Moïse Moyal, délégué régional Paca-Corse à la sécurité numérique de l'Anssi.

« On nous appelle les cyber-pompiers de l'Etat. On intervient auprès des entreprises victimes d'attaques. On fait une vingtaine d'interventions par an dans de grandes d'entreprises qui, bien entendu, ne veulent pas forcément communiquer. »
Ce dernier est revenu sur la directive


© F.D

Moïse Moyal, délégué régional Paca-Corse à la sécurité numérique de l'Anssi.

L'Anssi a aussi un regard sur les services essentiels de la France, qui sont liés aux transports, à l'énergie, aux banques, les infrastructures de marché comme les banques, la santé, l'eau potable, etc. Pour ces dernières, la démarche de l'Anssi « n'est pas d'appliquer une loi mais de faire de la pédagogie auprès des entreprises afin de les amener de manière coopérative à appliquer des mesures de sécurité performantes ».

UN RESPONSABLE SÉCURITÉ PAR ENTREPRISE

Pour faire face aux attaques, dans les entreprises, il faut un management des systèmes d'information, un système de défense et un processus de résilience pour rebondir et relancer le système. Plus on a prévu en amont, plus vite on récupèrera ses données.

L'intelligence artificielle face au droit

Jean-Paul Pinte, docteur en sciences de l'information et de la communication, ancien lieutenant-colonel de gendarmerie, est revenu sur le développement de l'intelligence artificielle face au droit.

Tous les secteurs de la société sont impactés par le développement de l'Intelligence artificielle (IA) : « 20 % des entreprises en France ont investi dans l'IA », souligne Jean-Paul Pinte, docteur en sciences de l'information et de la communication. Par rapport au monde du droit, il n'y a pas un sujet qui échappe à l'IA. « On va vers une humanité augmentée, avec des outils de plus en plus professionnels. Dans le droit, quand on a une masse de données, il est intéressant de la traiter avec l'IA. En 26 secondes, on peut étudier 26 contrats quand les professionnels y passaient 92 minutes... Ce gain de temps est énorme. Il faut y aller maintenant », conseille ce spécialiste, également lieutenant-colonel de gendarmerie.

© F.D

Pour Jean-Paul Pinte, docteur en sciences de l'information et de la communication, « il n'est plus possible d'ignorer l'IA ».

JURISTE HUMAIN CONTRE IA ?

La question de l'automatisation d'une partie de l'activité des avocats est posée avec de plus en plus d'insistance. « Les outils de l'IA s'appliquent à des tâches quotidiennes ou basiques, comme la relecture de contrats. L'IA s'applique aussi à la recherche des avocats et à leur capacité de gagner des procès », explique l'intervenant. « Même si le savoir-être restera essentiel, ainsi que la capacité de jugement et d'empathie, il n'est plus possible d'ignorer l'IA », conseille Jean-Paul Printe. Ce dernier se veut rassurant : « il n'y a pas de disparition prévue des avocats et des juges à court terme. Certaines professions vont intégrer progressivement l'IA. Le rapport humain va rester essentiel. »

L'Afnor certifie les entreprises engagées dans une démarche de sécurité

Bruno Hamon est gérant de Mirca SARL et représentant de l'Afnor, pour Association française de normalisation. Il revient sur les services que peut apporter cette association aux entreprises.

Bruno Hamon prévient, en introduction de son intervention : « 800 millions d'internautes vont arriver dans les prochaines années. On peut imaginer différents scénarios parce qu'il y aura des méchants et des gentils. » Et ce dernier d'avancer différents scenarii à la James Bond... Des histoires qui pourraient arriver : « imaginez qu'il y ait des hackers qui arrivent à exploiter le logiciel d'un barrage et qu'ils ouvrent les vannes, ou alors qu'ils prennent le contrôle à distance d'une usine nucléaire, ou dévient un porte-containers et le lancent dans un port ».
Loin de ces risques extrêmes, les patrons d'entreprise peuvent faire face à des attaques moins spectaculaires, mais tout aussi problématiques : « imaginez que vous êtes patron d'une entreprise possiblement victime de hackers. Ces derniers veulent dévoiler des données confidentielles de vos clients. Comment réagir ? Les clients concernés vous annoncent qu'ils veulent quitter votre établissement et vous attaquer en justice [...] Que faites-vous à ce moment-là ? Et surtout que faites-vous pour empêcher une telle catastrophe ? », demande Bruno Hamon.
Une des solutions consiste à se renseigner, former son personnel, s'organiser et élever son niveau de sécurité dans l'entreprise. Pour cela, l'Afnor édite des guides pour accompagner les patrons dans des problématiques liées à la sécurité informatique.
« La cybersécurité, ce n'est plus une option. Il faut y aller maintenant », conseille Bruno Hamon.

© F.D

Bruno Hamon est gérant de Mirca SARL et représentant de l'Afnor (Association française de normalisation).

QUATRE GUIDES PRATIQUES

L'Afnor édite quatre guides pratiques sur le sujet, à destination des chefs d'entreprise et salariés concernés. Ils sont à télécharger (payant) sur le site de l'Afnor : www.afnor.org/dossiers-thematiques/numerique.