# "Nos données méritent une meilleure protection"

*Pourquoi votre entreprise pourrait-elle être la prochaine cible des hackers ? Mettez-vous vos données en danger ? Comment vous protéger efficacement contre de potentielles attaques ? Maddyness a fait le point avec Joël Thiery, Directeur Général de la société Corefiim et élu de la CCI Paris Île-de-France en charge de la cybersécurité.*

Temps de lecture : minute

*6 juin 2018*

La cybersécurité n'a jamais autant été au coeur de l'actualité. Des violations colossales de données ont fait la Une des journaux dans le monde entier en 2017, de WannaCry à NotPetya en passant par Spectre et Meltdown. Pire encore : les entreprises financières et les gouvernements ne sont plus les principales cibles des cyberattaques, la menace est désormais universelle et aucune entreprise n'est à l'abri. Joël Thiery, Directeur Général de la société Corefiim et élu de la CCI Paris Île-de-France en charge de la cybersécurité, revient pour Maddyness sur les enjeux de la cybersécurité.

## Quels peuvent-être les risques encourus par les entreprises, aujourd'hui, si elles ne se protègent pas ?

Il ne se passe pas un jour sans que l'on apprenne qu'il y a une faille dans un système et que des hackers ont volé les données de millions de comptes. On a vu, dernièrement dans l'actualité, Uber et ses 57 millions d'utilisateurs concernés, mais aussi des logiciels pirates détourner des

centaines de millions de comptes. Pas seulement aux Etats-Unis, mais dans le monde entier. Et ce n'est que la partie la plus visible de l'iceberg, la plus médiatisée.

À côté de cela, tous les jours, des centaines voire des milliers de TPE et PME (qui représentent l'essentiel des emplois en France) sont frappées par des pirates, voient leurs systèmes d'information bloqués et arriver des demandes de rançons pour les débloquer. Certaines sont même acculées à la faillite car leurs données sont définitivement perdues si elles n'ont pas pris certaines précautions pour les sauvegarder. Selon une étude SystemX réalisée en 2017, 50 000 PME françaises ont été victimes de cyberattaques et près d'un tiers d'entre elles ont subi un dommage financier.

## Est-ce que ces attaques dépendent de la taille des entreprises ? Les grandes entreprises sont-elles plus visées ?

Cela touche tout type d'entreprise, quels qu'en soit la taille et le secteur. Aujourd'hui, les pirates ont à disposition des systèmes qui leur permettent d'attaquer les entreprises les plus importantes avec des moyens extrêmement sophistiqués, mais aussi d'attaquer des PME et TPE avec des moyens relativement modestes grâce aux failles de leurs réseaux et systèmes informatiques.

Il ne faut pas croire que parce que l'on est petit, avec un chiffre d'affaires de " seulement " quelques centaines de milliers d'euros, on ne sera pas attaqué. Les pirates visaient, il y a encore quelques années, en priorité les grands groupes, du secteur bancaire ou de la distribution par exemple. Aujourd'hui, ces derniers ont mis en place des services de cybersécurité très performants qui travaillent chaque jour à protéger leurs données. Même s'ils ne les délaissent pas, car personne n'est infaillible, les hackers

visent aujourd’hui aussi d’autres secteurs.

Il ne faut pas se leurrer : tout le monde est une cible potentielle pour les pirates informatiques. L'activité malveillante étant maintenant plus facilement monétisable, ce n'est pas une question de " si ", mais bien une question de " quand " : quand une violation de données se produira-t-elle?

## Comment expliquer que les attaques se soient multipliées ces dernières années ?

D’une part, il y a de plus en plus de pirates et de plus en plus de matériels qui permettent des attaques massives et extrêmement percutantes. D’un autre côté, on est malheureusement un peu trop confiant sur la manière dont nos données sont protégées. On ne prend pas suffisamment le temps de concevoir une protection efficace de nos systèmes d’information, ni de former les collaborateurs aux risques et aux bonnes pratiques.

Combien de fois voit-on encore des mots de passe écrits sur un post-it, ou des clés USB se promener sans connaître leur origine ? Cette clé, justement, a-t-elle été véritablement contrôlée sans danger ou va-t-elle affecter notre système ? Aujourd’hui, le maillon faible, c’est l’Homme. Plus d’un tiers des accidents de cybersécurité sont dus aux collaborateurs, qui ont tendance à oublier les principes élémentaires de protection, ou parfois qui n’en n’ont même pas conscience !

## Y a-t-il eu, néanmoins, une prise de conscience ces dernières années ?

Beaucoup d’entreprises ne sont pas encore assez informées des enjeux de la cybersécurité et des méthodes qui existent sur le marché, et ainsi négligent leurs systèmes de protection. D’autres, à l’inverse, sont bien

conscientes du problème mais estiment n'avoir ni le temps ni les ressources humaines, technologiques, financières pour se doter d'un dispositif efficace de cybersécurité.

En somme, il y a globalement une prise de conscience mais celle-ci ne se traduit pour le moment pas par des efforts de formation et d'équipement. Il faut prendre le temps de se former, et ce n'est pas toujours évident, en particulier dans les petites entreprises qui n'ont pas toujours les moyens de financer la formation de leurs collaborateurs.

## Quels seraient vos conseils pour aider les entreprises à se protéger ?

Il faut avant tout former et accompagner les hommes dans cette réflexion sur la cybersécurité, en se réunissant par exemple en équipe pour réfléchir aux règles de confidentialité des informations de l'entreprise. Ensuite, il faut respecter un minimum de règles de confidentialité : vérifier les clés USB que l'on vous donne ainsi que la provenance des mails que vous recevez, déconnecter votre bluetooth quand vous n'en avez pas besoin, ou encore emporter le moins de données possible sur votre ordinateur quand vous voyagez à l'étranger.

Il est également nécessaire de se poser les bonnes questions : le Cloud est-il vraiment sécurisé ? Vos données sont-elles conservées dans l'Union Européenne ou ailleurs dans le monde ? Vos données vous appartiennent-elles ou sont-elles la propriété d'un tiers établi outre-Atlantique, car vous avez sûrement coché une petite case pour les conditions générales d'utilisation (souvent près d'une centaine de pages) des GAFA, sans avoir vu que vous acceptez ainsi l'utilisation intégrale de vos données !

Beaucoup d'entre nous n'ont pas encore la notion de la valeur de la donnée. Le RGPD, entré en vigueur le 25 mai, est intéressant car il va permettre à tous de prendre conscience que leurs données valent

quelque chose. Il faut demain que cette prise de conscience se transforme en actions.

Il faut donc se protéger et savoir exploiter nos ressources. Cela demande un effort de tous les collaborateurs de l'entreprise et un minimum d'investissement financier. Il n'est pas normal aujourd'hui, dans les petites entreprises, que l'on ait des systèmes de sécurité contre les intrusions physiques, avec des portes blindées et de la vidéo-surveillance, sans avoir des systèmes de sécurité informatiques vraiment efficaces. Les experts s'entendent pour dire que seulement 2 à 3 % des budgets informatiques sont dédiés à la cybersécurité, alors qu'il faudrait y consacrer plus de 10 %.

Pour aider les entreprises à faire face à un tel enjeu, la CCI Paris Île-de-France consacre le Mois du numérique by Les Digiteurs à la protection des données. Du 7 au 29 juin 2018, les experts, porteurs de solutions et conseillers numériques les informeront et répondront à toutes leurs questions.

*Maddyness, partenaire média de la CCI IdF.*

---

Article écrit par Maddyness, avec la CCI IdF