Startups, comment vous prémunir des cyber attaques ?

Même si les cyberattaques font peur aux entreprises, la tendance est de penser que cela n'arrive qu'aux autres... Pourtant, il s'agit d'un phénomène bien moins rare que ce que l'on pense, c'est pourquoi s'armer contre ce fléau pourrait leur éviter de véritables catastrophes

Temps de lecture : minute

18 avril 2019

Vol des données, demande de rançon, installation de virus... les pirates ont plus d'un tour dans leur sac, et dans des cas extrêmes, cela peut coûter la vie à certaines entreprises. Or, il est aujourd'hui possible de lutter contre ces attaques. Maddyness et Hiscox vous donnent quelques conseils pour votre entreprise.

1/ Sécuriser les accès

Afin de sécuriser les accès, il faut tout d'abord mettre en place une politique de mot de passe. De fait, en plus de rendre obligatoire son changement de temps en temps, il faut travailler sur sa complexité. Des caractères spéciaux, des chiffres, et des successions de mots sont à privilégier car cela rendra leur décryptage beaucoup plus difficile. Ensuite, il est bien sûr recommandé d'éviter tout trace écrite visible du code.

D'ailleurs, lorsqu'une personne extérieure à l'entreprise entre dans les locaux, il faut rester vigilant quant à sa raison d'être là. Il s'agit effectivement d'un point auquel peu de monde pense, mais si une personne mal intentionnée pénètre dans les locaux, accède à un

ordinateur non verrouillé, ou tout simplement à la photocopieuse où de nombreuses informations sont enregistrées, les conséquences peuvent être lourdes. C'est d'ailleurs une des raisons pour laquelle les collaborateurs doivent avoir un mot de passe et penser à verrouiller leur ordinateur lorsqu'ils quittent leur poste de travail.

De plus, Astrid-Marie Pirson, Directrice technique de la souscription et experte marché cyber chez Hiscox France, assureur spécialiste, conseille aux entreprises de mettre en place une politique de gestion des accès. "*Tout le monde n'a pas besoin d'avoir accès à tout dans l'entreprise*" explique-t-elle. "*Chez Hiscox, il y a des données très sensibles, auxquelles je n'ai pas accès, puisque je n'en ai pas besoin dans mon travail au quotidien*". Ce n'est pas du tout dans une démarche restrictive, mais plutôt pour prévenir du risque. En effet, si une personne réussit à se connecter à son ordinateur et accède à ses fichiers, elle n'y trouvera pas l'intégralité de la vie de l'entreprise, ce qui limite les répercussions.

2/ Prévenir l'accès à distance des données

Depuis qu'il est possible de travailler de partout et à tout moment, le système d'information des entreprises est exposé à beaucoup plus de risques. L'accès à distance des données rend ces dernières plus susceptibles d'être interceptées par des personnes malveillantes. Pour anticiper cela, Astrid-Marie Pirson conseille de mettre en place un système de double authentification. Cette solution demandera au collaborateur qui se connecte à distance depuis son ordinateur, d'entrer, en plus de son mot de passe, un code reçu sur son téléphone par exemple, pour assurer qu'il s'agit bien de lui. Cela augmente la sécurité puisque qu'une connexion frauduleuse peut davantage être évitée. Par ailleurs, elle revient sur la mise en place d'une politique de gestion des mots de passe. Il faut effectivement s'assurer que le changement de mot de passe soit obligatoire sur les ordinateurs, mais aussi sur les smartphones et les tablettes, afin de se protéger en cas de vol de

l’appareil. Astrid-Marie Pirson explique que “*beaucoup d’entreprises ont une politique de mots de passe pour les ordinateurs de leur entreprise, mais pensent moins à l’appliquer aux téléphones*” alors que c’est tout aussi important. Enfin, elle prévient que la connexion à un Wifi public, par exemple celui d’un train, d’un aéroport, ou encore d’un hôtel, peut permettre à des pirates d’avoir directement accès à l’activité sur l’appareil. Ainsi elle recommande de privilégier un partage de connexion depuis son propre téléphone plutôt que d’utiliser ce type de wifi.

2/ Ne pas négliger les mises à jour

Le cas de la cyberattaque WannaCry, qui a eu lieu en mai 2017, est une bonne illustration de l’importance des mises à jour. Lors de cette cyberattaque mondiale massive, le ransomware WannaCrypt - un logiciel informatique malveillant prenant en otage les données - a utilisé une faille informatique de Windows pour chiffrer des millions de données, et ainsi exiger de grandes sommes d’argent des victimes, en échange de la clé de déchiffrement à appliquer à leurs documents, rendus inutilisables. Or, peu de temps avant l’attaque, Microsoft avait déployé une mise à jour pour Windows afin de corriger la faille. Le problème, c'est que de nombreux entreprises et individus ne l’ont pas effectuée, ce qui a permis au ransomware de se répandre.

Avec cet exemple, Astrid-Marie Pirson cherche à montrer que lorsqu’on ne met pas à jour un logiciel, on a plus de risque d’être exposé à des logiciels malveillants. “*Il faut penser à le faire régulièrement, par exemple une nuit par mois, pour ne pas trop déranger l’activité des collaborateurs*”.

Pour plus de prudence, elle conseille par ailleurs aux entreprises de créer une sauvegarde externe de leurs données essentielles, et ce à occurrence régulière. Cela permettra au moins de récupérer la dernière sauvegarde, plutôt que de tout perdre. En France, encore peu d’entreprises ont une sauvegarde séparée de leur système d’information alors que cela leur

apporterait une véritable sécurité. Astrid-Marie Pirson explique que cela peut effectivement faire la différence pour l'entreprise, car par exemple "*quand une attaque a lieu, qu'elle entraîne une confiscation des données contre une demande de rançon, l'entreprise qui n'a pas de sauvegarde peut être tentée de payer, pour ne pas tout perdre. Sauf qu'en payant, elle encourage le pirate à revenir pour recommencer. Or si elle avait eu une sauvegarde, elle n'aurait pas perdu toutes ses données et n'aurait donc pas eu à céder au chantage*" .

Il faut également veiller à ce que le système d'exploitation de l'entreprise ne soit pas obsolète, et ne propose donc plus de mises à jour. Sans pour autant devoir systématiquement se procurer la toute dernière version d'un système d'exploitation, il faut être attentif à ce que l'éditeur de celui qu'on utilise continue de proposer des mises à jour régulières pour la version du système concernée.

4/ Faire des sauvegardes

Faire une sauvegarde peut être important en cas de confiscation des données. Mais cela peut également l'être pour d'autres raisons. Par exemple, beaucoup de startups externalisent leurs informations auprès d'un hébergeur. Or, même si c'est relativement rare, il se peut qu'un problème survienne chez cet hébergeur. Avoir une sauvegarde peut donc éviter à la jeune pousse d'être totalement bloquée si quoique ce soit arrive chez son prestataire et être ainsi moins dépendante de ce dernier.

Astrid-Marie Pirson conseille de faire une sauvegarde au moins une fois par semaine, et de la tester de temps en temps pour s'assurer qu'elle fonctionne correctement. Lors de ces manipulations, il est important qu'elle soit complètement séparée du système d'information de l'entreprise. De fait, si un logiciel malveillant arrive à accéder au système et que le disque dur où est la sauvegarde est branché, ce disque risque aussi d'être attaqué. Par ailleurs, elle avertit qu'"*effectuer des*

sauvegardes ne doit pas faire baisser votre vigilance. En cas de cyberattaque il faudra être ultra réactif, et ne pas attendre le lendemain pour faire quelque chose, car entre-temps les dégâts pourront s'être étendus même à la sauvegarde, et dans ce cas pires seront les conséquences" . Si un tel problème survient, il n'est pas forcément nécessaire d'éteindre l'ordinateur, mais plutôt de le couper du réseau pour éviter que le logiciel malveillant se propage. Il faut ensuite nettoyer l'ordinateur infecté, puis le relier avec le réseau, et enfin remonter la sauvegarde. Il faut surtout s'assurer, dans une telle situation, d'être bien accompagné par des experts.

5/ Veiller à la sécurité des paiements

En France, les risques cyber liés aux paiements physiques sont relativement rares, puisque nous utilisons encore beaucoup les codes de nos cartes de crédit. En revanche, pour ce qui est des paiements en ligne, les fraudes sont plus fréquentes. La plupart des startups font le choix de sous-traiter leur processing de paiement auprès d'acteurs reconnus, qui seront eux en mesure de bien sécuriser les données bancaires des clients de l'entreprise. Astrid-Marie Pirson encourage le recours à ce type de prestataire car ce sont des experts, et en cas de problème, l'entreprise est un minimum protégée. En effet, processer des paiements est une chose qui ne s'improvise pas, "*c'est très à risque puisque, potentiellement, l'entreprise en cas d'attaque se fera voler directement les informations de paiement de ses clients.*"

Le seul danger pour le client, c'est d'être redirigé vers une "fausse" page dédiée au paiement. Lorsque l'entreprise fait appel à un prestataire de paiement, cela impose effectivement de prévoir un passage du site marchand vers le site pour payer, or un pirate pourrait intercepter le client à ce moment-là, et le diriger vers une page frauduleuse ou tout simplement voler les données relatives à sa carte bancaire.

Pour que l'entreprise puisse mieux se protéger d’une éventuelle fraude sur ses propres transactions financières, Astrid-Marie Pirson encourage l’utilisation d’une double autorisation. Elle explique en effet que dans certains cas, des personnes malveillantes pourraient usurper l’identité d’une personne de l’entreprise (par mail, téléphone, etc.), celle du CEO par exemple, pour demander au comptable, par exemple, de faire un virement à son profit. C’est pourquoi mettre en place une double autorisation, automatique à partir d’un certain montant, pourrait réduire ce risque. Plus concrètement deux personnes doivent donner un accord écrit pour que le paiement soit validé, ce qui complique la tâche au pirate qui devrait alors se faire passer pour deux personnes au lieu d’une – mais souvent il verra sa tentative échouer dans ce cas.

Pour conclure, l’experte d’Hiscox explique que lorsque les collaborateurs sont bien formés à l’ensemble de ces risques, le danger est beaucoup moins présent. En effet, selon elle, “*les entreprises doivent être conscientes que ce type de problème n’est pas majoritairement dû à des cyberattaques, mais plutôt à des erreurs humaines*” . Il est donc important de les former, par exemple via des programmes d'entreprise de plus en plus courant, comme celui mis en place par Hiscox, le programme Hiscox CyberClear academy, pour leur donner accès aux bonnes pratiques et aux choses à éviter.

Maddyness, partenaire média d’Hiscox

Article écrit par Maddyness, avec Hiscox