Les petites entreprises aussi victimes de cybercriminalité | Denis JACOPINI

Vols de données clients, piratage de propriété intellectuelle… les cyberattaques sont légion, mais les petites entreprises se croient souvent peu concernées. A tort. Pour se protéger de ces actes malveillants, une bonne « hygiène numérique » simple à mettre en place s'avère nécessaire.

« Dirigeant d'une petite entreprise, vous pensez n'avoir jamais été victime d'une cyberattaque ? Soit vous ne l'avez pas détectée, soit vous n'intéressez plus personne et il faudrait penser à changer de métier ! « .
Cette boutade, destinée à faire prendre conscience aux patrons de PME des risques qu'ils encourent face aux hackers en tout genre, émane du contre-amiral Dominique Riban, directeur général adjoint de l'Anssi, l'Agence nationale de la sécurité des systèmes d'information.
Il faut dire que pour une PME, détecter ne serait-ce que les incidents de sécurité, autrement dit le fait qu'un pirate essaie de s'introduire dans le système sans y parvenir, s'avère bien compliqué. Idem pour les attaques. Certes, des comportements bizarres de l'ordinateur peuvent attirer l'attention, comme son ralentissement, des connexions qui s'effectuent toutes seules, la flèche de la souris qui se ballade… Mais les » méchants » savent surtout se faire discrets. Et il s'agit d'un sujet très – trop – technique, lorsqu'on ne possède pas un collaborateur spécialisé à plein temps pour s'en préoccuper…

Peu de PME portent plainte
Difficile d'avoir des chiffres fiables sur la réalité de la cybercriminalité subie par les PME. Pour une raison simple: peu portent plainte, lorsqu'elles en sont victimes. Pourquoi risquer la mauvaise publicité ? Retrouver l'auteur de l'infraction s'avère de toute façon souvent mission impossible, admet Jean-Louis Di Giovanni, associé PwC du département Litiges et Investigations auteur d'une enquête sur les fraudes en entreprises* : » On peut remonter sa trace, mais quand l'adresse IP provient d'un cybercafé aux alentours de la gare de l'Est, comment voulez-vous mettre la main dessus ? « . Devenir cybercriminel est en tout cas à la portée de tous. » Aujourd'hui, pour une centaine d'euros, vous disposez d'une solution pour attaquer le système d'information de votre concurrent, ou, pour trois fois moins cher, son smartphone « , indique Dominique Riban.

Une menace à plusieurs visages
Fomentée par de malveillants collaborateurs, actuels ou anciens, ou bien perpétrée par des hackers externes, la cybercriminalité s'avère multi-formes. Les attaques ciblées, qui visent à voler un savoir-faire particulier ou des données sensibles (secrets de fabrication, brevets, plans industriels, fichiers clients…), côtoient des attaques que Philippe Humeau, directeur général de NBS System, spécialisée dans l'hébergement de haute sécurité et les tests d'intrusion, nomme d' » opportunistes » : » Il suffit que l'entreprise ait un bout de son système connecté sur le net, qu'elle laisse traîner un mot de passe par défaut, et ça y est, elle est vulnérable. Il faut savoir qu'une adresse IP est scannée vingt fois par jour, explique-t-il. Une vraie industrie, que ces scanners qui recherchent des données relatives à des cartes bleues ou à des » identités « , autrement dit à des informations sur les personnes (celles que l'entreprise doit signaler détenir à la Cnil, ndlr). Aux commandes, des pirates qui effectuent de la récupération massive de données de ce type, puis les revendent au détail à d'autres pirates. » Car elles ont de la valeur. Des données bancaires se revendent dix dollars. Une « identité », entre 5 et 15 dollars. » Une filière aussi organisée que le recel de bijoux « , confirme Dominique Riban.

Des piégeurs pros
Parfois, les cybercriminels entrent carrément en contact avec l'entreprise. Leur inventivité sans faille leur permet de s'engouffrer dans toute nouvelle brèche. Dernier coup à la mode, la » fraude Sepa « . Les entreprises ont, rappelons-le, jusqu'au 31 juillet 2014 maximum, pour opérer leur migration afin d'être conforme à ces nouvelles normes de paiement européennes. Une aubaine, pour les fraudeurs.

Jean-Louis Di Giovanni détaille le processus : » Quelques jours auparavant, ils envoient un mail à la société, pour l'avertir qu'ils vont la contacter par téléphone afin de procéder à des essais. Le mail semble officiel évidemment. On y trouve le numéro du fraudeur, et, comble du raffinement, si l'on appelle, on tombera sur la petite musique d'attente officielle de la banque. Le jour J, ils téléphonent donc à l'entreprise, et demandent à leur interlocuteur de télécharger un programme… qui sert en réalité à prendre la main sur son ordinateur. Le fraudeur voit sur l'écran toutes les informations qu'aurait normalement la banque, et cela le rend ainsi crédible pour passer un ordre, du type : allez sur le compte x sur lequel vous disposez de 2,5 millions d'euros et faites un virement vers ce numéro de compte étranger. » Nombreuses ont été les entreprises à s'exécuter. 48 h plus tard – le délai maximum pour faire bloquer in extremis le virement – c'est trop tard !

80 % de risques évités avec des mesures simples
Des mesures de protection sont aujourd'hui nécessaires. Contrairement aux idées reçues, le recours à des solutions » technologiques » ne constituerait pas forcément la meilleure arme de défense contre les hackers. » Il est surtout important de sensibiliser ses collaborateurs aux bonnes pratiques « , assure Philippe Trouchaud, associé PwC, spécialiste de la cybersécurité.

L'Anssi publie sur son site un mode d'emploi pour éviter les incidents. Il s'agit d'une quarantaine de » règles d'hygiène « , concernant la sécurité des messageries, du poste de travail, des imprimantes etc. Une quinzaine sont applicables par les petites entreprises. » 80 % des attaques n'auraient pas lieu si ces recommandations étaient respectées « , assure Dominique Riban. Parmi elles, des gestes simples… mais trop souvent négligés. Une évidence, par exemple, de toujours utiliser des mots de passe solides? » 70 % d'entre eux sont faibles, se désole Philippe Humeau. Cette négligence généralisée cause énormément de désastres. Sans compter que les gens utilisent les mêmes partout. »

En plus du choix de mot de passe costauds, les experts font trois recommandations essentielles :

1. Des mises à jour régulières
Se doter d'au moins deux anti-virus et les remettre à jour. » Même si un antivirus n'a jamais été la panacée « , concède le contre-amiral Riban. Même nécessité de remise à jour pour tous ses logiciels. » Si les éditeurs font évoluer leurs versions, c'est parce qu'ils ont constaté des failles de sécurité, pointe Philippe Humeau. Mieux vaut éviter de reporter sans cesse le » rebootage » de sa machine quand elle le demande. »

2. Attention au cloud
Toute nouvelle pratique engendre de nouvelles menaces. C'est le cas du cloud. « N'y stockez pas de données cruciales, exhorte Dominique Riban. Privilégiez des opérateurs français dont vous trouverez la liste sur le site de l'Anssi. Je ne dis pas qu'il n'y aura pas d'accident, mais au moins, notre structure a analysé leur façon de travailler, les a audité, leur a fait corriger leurs failles. Ce n'est pas le cas, par exemple, avec Google ou Microsoft. »

3.Haro sur le BYOD
Philippe Humeau n'hésite pas également à pointer du doigt ce qu'il appelle le » problème des jeunes générations » : » Elles débarquent dans l'entreprise avec des notions de sécurité et de vie privée assez light. Elles ont encore moins de réflexes que leurs aînées. Lorsqu'un jeune n'hésite pas à dévoiler sa cuite du week-end sur Facebook, il ne faut pas s'attendre à ce qu'il sache mettre des barrières là où il devrait les mettre. » Souvent associé à la génération Y – mais pas que – , le phénomène BYOD (» bring your own device «) tient du fléau en matière de cybersécurité. La pratique nécessite d'être encadrée.

» Il devient difficile de l'interdire, mieux vaut donc accompagner l'usage « , préconise Philippe Humeau. Mettre en place par exemple un réseau internet privé et un autre public, pour que les collaborateurs s'y connectent avec leur machine. Dominique Riban se montre, lui, beaucoup plus radical : » Même si l'appareil appartient à l'employé, seul l'employeur doit pouvoir administrer la machine, afin que l'utilisateur, ou ses enfants, ne puisse pas télécharger tout et n'importe quoi le week-end ou désactiver l'anti-virus. » Pas sûr que les collaborateurs acceptent…

Procéder ou pas à un test d'intrusion
Pour évaluer la capacité de résistance de son système informatique, on peut évidemment faire effectuer un test d'intrusion. A une petite entreprise, il en coûtera aux alentours de 7000 euros. Une facture qui peut paraître prohibitive. » Evidemment cela ne s'adresse pas à tout petit entrepreneur , se défend Philippe Humeau, dont la société propose de tels tests. Mais si l'on a des secrets de fabrication, la dépense est justifiée. Nos interventions se déroulent encore malheureusement trop souvent en post-mortem, nous faisons peu de prévention. »

* Selon cette récente étude, la cybercriminalité est la 2ème fraude la plus signalée en France. Son évolution inquiète particulièrement les dirigeants qui la classent comme la fraude la plus redoutée dans les 24 mois à venir.

Nous organisons régulièrement des **actions de sensibilisation ou de formation** au risque informatique, à l'hygiène informatique, à la cybercriminalité et à la mise en conformité auprès de la CNIL. Nos actions peuvent aussi être personnalisées et organisées dans votre établissement.
Besoin d'informations complémentaires ?
Contactez-nous
Denis JACOPINI
Tel : 06 19 71 79 12
formateur n°93 84 03041 84

Expert Informatique assermenté et formateur spécialisé en sécurité Informatique, en **cybercriminalité** et en **déclarations à la CNIL**, Denis JACOPINI et Le Net Expert sont en mesure de prendre en charge, en tant qu'intervenant de confiance, la sensibilisation ou la **formation de vos salariés** afin de leur enseigner les bonnes pratiques pour assurer une meilleure sécurité des systèmes informatiques et améliorer la protection juridique du chef d'entreprise.
Contactez-nous

Cet article vous plait ? Partagez !
Un avis ? Laissez-nous un commentaire !

Source : http://lentreprise.lexpress.fr/high-tech-innovation/cybercriminalite-les-petites-entreprises-ne-sont-pas-a-l-abri_1518760.html