Cybersécurité : quel hacké·e êtes-vous ?

Si les grandes entreprises ont bien conscience des risques liés à leurs données, les startups font souvent l'erreur de penser qu'ils sont trop "petits" pour intéresser les hackers. Pourtant, toutes les entreprises, ont, par leur valeur ajoutée, de quoi attirer les voleurs.

Temps de lecture : minute

---

28 janvier 2020

A mesure que le monde et l'économie se digitalisent, la protection des données et les enjeux de sécurité liés au numérique prennent chaque jour plus d'ampleur. Les pirates du web l'ont bien compris et raflent ainsi leur mise au cœur de l'espace virtuel. Leurs méfaits cryptés les rendent de fait plus durs à repérer, mais aussi à sanctionner.

C'est pourquoi Hiscox, partenaire de la Maddy Keynote 2020, a décidé de mettre en place une "Hacking Room" sur l'événement : un espace expérientiel pour découvrir des cas d'usages de cyber attaques, et écouter des conférences d'experts à ce sujet. Et pour vous en dévoiler un peu plus avant l'événement, Maddyness a interrogé Astrid-Marie Pirson, directrice technique souscription et experte en cyber sécurité, pour évoquer les différents cas de cyber attaques pouvant toucher les entrepreneurs.

Alors, comment avoir une vision lucide de son niveau de sensibilisation au hacking, lors que l'on est une PME ou une startup ? Découvrez ici que type de hacké·e êtes-vous !

“La cible parfaite” : *Celui qui n’a rien fait pour se protéger*

La cible parfaite est en général celle qui n’a même pas conscience d’être exposée à des risques : si jamais elle fait l’objet d’une attaque, il est même possible qu’elle ne s’en aperçoive tout simplement pas ! Cette personne sera généralement surexposée aux attaques de grande ampleur comme les *ransomwares* (ou rançongiciels, logiciels de rançon qui prennent en otage des données personnelles contre une contrepartie financière) ou les *phishings* (ou hameçonnages, techniques utilisées pour obtenir des informations personnelles dans le but d’une usurpation d’identité en ligne).

Dans le cadre d’une entreprise, cela risque d’ailleurs de lui coûter des clients, car ces derniers sont de plus en plus nombreux à se préoccuper des risques et à exiger de leurs prestataires un niveau minimum de protection, notamment depuis qu’est intervenu le règlement européen sur la protection des données personnelles.. “*Préoccupation parfaitement légitime, car le prestataire est en général un bon point d’entrée chez son client (parfois il a même des accès direct au système de ce dernier). Si ce point d’entrée est mal protégé, les conséquences peuvent être vertigineuses car le hacker parfois aura accès à l’ensemble des données du client du fait des mauvaises pratiques du prestataire* !” explique Astrid-Marie Pirson.

“Une bonne défense, mais encore quelques failles dans le système” : *Celui qui pense qu’il a mis une protection IT donc croit être à l’abri*

L’IT (la protection du système d’information d’une entreprise via la

technologie) est un des atouts clés de la bonne gestion des risques cyber, et c'est donc par là qu'il faut commencer pour se protéger. Le deuxième type de hacké·e aura généralement mis en place les premières défenses IT pour protéger ses données. Pour autant, "*ce n'est pas parce que ce sont des risques numériques que les protections à mettre en place ne peuvent être, elles aussi, que numériques*" souligne Astrid-Marie Pirson. "*Quand vous cherchez à vous prémunir contre le risque d'incendie, vous allez installer des détecteurs et des extincteurs, mais vous allez aussi expliquer à vos salariés pourquoi il ne faut pas fumer à côté de la chaudière et, au cas où, prendre une assurance."* Dans le cas d'une cyber attaque, c'est la même chose : avant de s'assurer, il faut avoir mis en place les défenses nécessaires pour limiter les dégâts (antivirus, pare-feu, logiciels mis à jour, patchs de sécurité, etc.) pour avoir ensuite accès à de bonnes conditions d'assurance. Mettre en place des solutions techniques sans assurance, ce n'est pas suffisant, car un accident peut toujours arriver, qu'il soit d'origine criminelle ou le fait d'une erreur humaine. En effet, plus plus des ¾ des incidents cyber dont des faits de négligence, et non de malveillance !

"La forteresse inattaquable" *Celui qui croit avoir le dispositif complet pour se prémunir*

Détrompez-vous, la forteresse inattaquable n'existe pas. Toutes les entreprises ont leurs failles, une porte d'entrée pour un Cheval de Troie.

Si l'on peut se prémunir de manière efficace contre les cyber attaques - mettre en place des outils de protection IT, avoir sensibilisé ses salariés aux bonnes pratiques à avoir (mots de passe, réaction au phishing, gestion des accès, utilisation de logiciels sécurisés, etc.), et prendre une assurance - cela ne veut malheureusement pas dire qu'un incident n'arrivera pas. Le groupe M6 avait par exemple été hacké par randsomeware en octobre 2019, ciblant la diffusion de ses programmes

TV et radio. On peut également se souvenir de l'attaque de TV5 Monde il y a 5 ans, qui avait coût 4,6 millions d'euros à la chaîne."*On peut tous, même en ayant été sensibilisé à ces risques, laisser passer par inadvertance un mail de ransomware, perdre un fichier ou donner ses infos confidentielles à la mauvaise personne : un salarié qui vient d'arriver, un stagiaire, son enfant… C'est humain et ce n'est pas fatal si on a pris les bonnes précautions en amont*" souligne l'experte.

Il faut garder en tête que même si de bonnes pratiques permettent d'éviter en partie les attaques de grande ampleur, elles ne stopperont pas un hacker qui a décidé de s'introduire spécifiquement chez vous, pour y chercher quelque chose en particulier (un procédé nouveau, une base de données, un point d'entrée chez un client, etc). Mais rassurez-vous ! Avec une gestion des risques qui repose sur trois solides piliers (outils technologiques, bonne sensibilisation des salariés, assurance souscrite), votre entreprise pourra survivre à une crise de ce type, et peut-être même faire de sa résilience un atout supplémentaire.

Pour en savoir plus sur les cyber attaques et tous les moyens de s'en prémunir, rendez-vous sur la Hacking Room d'Hiscox lors de Maddy Keynote 2020, les 30 et 31 janvier prochains au 104 !

Maddyness, partenaire média de Hiscox

Prendre son billet pour la Maddy Keynote 2020

Article écrit par Maddyness, avec Hiscox