Comment mieux accompagner les TPE et PME dans la gestion des risques cyber ?
Par Stanislas de Goriainoff, CTO de Sewan

Bien que les hackeurs n'aient pas attendu le conflit entre la Russie et l'Ukraine pour sévir, la mise en lumière des différentes menaces venues d'Orient, avérées ou supposées, a semé comme un vent de lucidité au sein de notre économie française. En outre, si les niveaux de sécurité sont déjà à leur maximum dans bon nombre de grandes entreprises - dans un contexte de recrudescence des attaques observée depuis la pandémie en réalité - certaines d'entre elles demeurent bien moins armées. C'est le cas notamment des TPE et PME, encore peu matures sur le sujet.[1] En effet, si leurs dirigeants semblent bien au fait des risques cyber qui pèsent sur leur activité, beaucoup ont dans le même temps tendance à surestimer leur niveau de protection actuel… Une réputation qui les précède et une erreur qui les expose : 33% des TPE/PME de moins de 250 salariés ont été touchés au cours de l'année 2021.[2]

Bien informer, sans alarmer.

Pour espérer les impliquer sur ce sujet anxiogène, et les convaincre des investissements et sacrifices nécessaires, la priorité est assez logiquement de les informer, avec pédagogie, et pragmatisme. Tandis que la majorité des TPE et PME attend malheureusement d'être victime d'une cyberattaque pour agir, l'enjeu est de déployer des efforts de prévention, tout en évitant de tomber dans des discours trop alarmistes. Ces dernières, disons-le, ne seront en effet pas davantage ciblées à la suite du conflit européen. Lorsqu'elles le sont, les attaques sont le plus souvent automatisées, et le motif plus volontiers crapuleux que politique : extorsion de fonds, ou de données. De fait, et logiquement, les montants des rançons réclamées restent toujours à la hauteur de leur capacité, l'intérêt des hackeurs étant avant tout de s'assurer de la solvabilité de ces rançons. L'instauration d'un climat exagérément angoissant contribue de mon point de vue à une perception erronée des enjeux cyber, et nuit de fait aux bons comportements, comme aux bons investissements.

Prioriser les données à protéger.

Car, en effet, de quelles données parlons-nous ? En premier lieu, nos TPE et PME, une fois convaincues de l'intérêt de mettre en place une cybersécurité, doivent être guidées dans l'identification, le choix, et la priorisation des données à défendre. Cette action requiert des audits spécifiques et un travail souvent (très) long de récupération de ces données, entre ordinateurs individuels et cloud, entre salariés présents ou passés,…L'essor du télétravail au lendemain de la crise COVID a par ailleurs mis ce sujet sur le devant de la scène. Les discours et prises de parole se multiplient depuis deux ans pour évangéliser sur les protections minimales à mettre en place : chiffrage des flux de données (firewall/VPN), chiffrement des disques, sauvegardes des données redondantes, limitations des accès et contrôles de chaque poste de travail… La protection de cette typologie d'entreprise est d'autant plus importante que les évolutions numériques à venir sont colossales et impacteront fortement le bureau de demain.

Améliorer l’expérience de la sécurité.

Une chose est certaine : compliquer la vie du hackeur, c’est aussi compliquer la vie de l’utilisateur, et de fait entacher - légèrement - son expérience en ligne. Tandis que la précieuse « UX » est devenue un maillon central de la compétitivité sur le web, l’on peut aisément entendre que la complexification des passwords, la multiplication des identifiants ou autres codes reçus SMS par exemple, pour ne citer qu’eux, apparaissent comme des freins non envisageables pour les administrateurs. Au-delà de la pédagogie que nous nous devons de parfaire sur ce point, à nous également d’imaginer et d’inventer une cybersécurité qui sache préserver une expérience de navigation ou d’achat de qualité.

---

[1] Ifop

[2] Forrester