CYBERSÉCURITÉ : L'URGENCE POUR LES ENTREPRISES

COMMENT **SE PRÉMUNIR** DES CYBERATTAQUES ? COMMENT **Y RÉPONDRE** ? QUELLES PEUVENT EN ÊTRE **LES PRÉJUDICES ET LES RISQUES JURIDIQUES** ? LE **WEBINAIRE** ORGANISÉ PAR LE CABINET NANTAIS DE **CONSEIL EN ASSURANCES BESSÉ**, LE 26 NOVEMBRE, A APPORTÉ DES RÉPONSES. CAR L'URGENCE EST BIEN LÀ : LES **ATTAQUES ONT QUADRUPLÉ** LORS DU PREMIER CONFINEMENT ET TOUCHENT **TOUT TYPE** D'ENTREPRISE.

Par Julie **CATEAU**

« Entreprises, êtes-vous bien protégées contre les menaces cyber ? » C'est avec cette question que le cabinet nantais de conseil en assurance Bessé a interpellé les participants d'un webinaire organisé le 26 novembre. En partant d'un constat martelé par l'Agence nationale de sécurité des systèmes d'information (Anssi) : les réseaux sont aujourd'hui de plus en plus vulnérables, avec une multiplication par quatre des cyberattaques lors du premier confinement. En cause : une organisation éclair en télétravail avec des protocoles et du matériel souvent insuffisants pour y faire face.

Et cela concerne tous les types d'entreprises et tous les secteurs d'activité. Pas uniquement les grosses structures en vue, comme le rappelle Nicolas Guilloux, directeur grand Ouest chez Almond, opérateur de conseil et d'audit en cybermenaces. « Aujourd'hui, il y a une logique de rentabilité de l'attaque avec des systèmes automatiques qui maximisent leur portée. Donc, si l'attaque ne coûte rien, elle sera forcément rentable, même si c'est pour ne rapporter qu'une poignée de bitcoins. »

Rémi Bottin, directeur Synergies et développement chez Bessé, évoque l'imaginaire collectif autour d'un hacker surdoué s'attaquant à la Nasa ou au FBI. « Nous ne sommes plus face à ce type de profil et chaque entreprise peut potentiellement être une cible. On le constate par exemple avec les mises à jour sécurité sans cesse demandées pour nos smartphones », explique-t-il.

Le problème, c'est que les entreprises n'ont pas encore pris conscience de la valeur de leurs données immatérielles et de la nécessité de les protéger. « Traditionnellement, les organisations s'occupent de la sécurité des biens matériels. Pourtant les données des serveurs, les logiciels ou encore les informations de R&D constituent aussi une grande ressource », observe Rémi Bottin. L'avocat d'affaire, associé au cabinet Racine, Loullig Bretel, rapporte le piratage récent du secteur de la justice, notamment de certains cabinets victimes de phishing (ou hameçonnage) puis de rançonnage. Ou encore le cas de deux PME qui se pensaient inattaquables et qui ont vu leur logiciel métier bloqué car leur prestataire avait subi une cyberattaque…

Alors que faire si cela vous arrive ? Rémi Bottin détaille les étapes nécessaires : « D'abord, gérer la crise. Il faut comprendre ce qui se passe et éliminer le virus, vérifier les sauvegardes… Ensuite, soigner sa communication aussi bien interne, auprès de salariés qui ont besoin d'être rassurés, qu'externe auprès de clients, fournisseurs, partenaires qui ont besoin de transparence. Enfin, évaluer le niveau d'atteinte de l'activité, chiffrer les pertes d'exploitation, voire acheter une prestation externe pour assurer ses contrats et continuer d'alimenter la supply chain. »

« QUADRUPLE PEINE »

Car le risque peut être important aussi bien pour l'entreprise que pour le dirigeant lui-même. Pour Loullig Bretel, « c'est la double, voire triple ou quadruple peine », met-il en garde, énumérant les différentes responsabilités qui peuvent être engagées. D'abord, la responsabilité civile de l'entreprise, engagée par ses clients. « Car si on ne peut plus produire ou fournir un service, cela constitue un risque pour ses clients », rappelle l'avocat. En particulier, s'il y a une fuite de données sensibles sur ces clients ou des partenaires qui se retrouvent sur le darkweb. « C'est une source de préjudice. L'entreprise s'expose à une action de groupe et à des recours d'associations dans le cadre de la réglementation RGPD de 2018. » Il y a par ailleurs des sanctions pénales possibles s'il est établi que l'entreprise n'a pas suffisamment sécurisé ces données. Et des sanctions administratives, au regard de la Cnil, sur la sécurisation des données également. Dans l'Union européenne, depuis l'entrée en vigueur de la RGPD (mai 2018), 93 sanctions ont été prononcées avec des peines allant de moins de 10 000 € à plus d'un million. En France, le groupe immobilier Sergic a été condamné à 400 000 € d'amendes par la Cnil après une attaque via un site web insuffisamment sûr. Les hackers avaient réussi à accéder aux dossiers de location…

Rémi **BOTTIN**, directeur Synergies et développement chez Bessé

Loullig **BRETEL**, avocat associé du cabinet Racine

Nicolas **GUILLOUX**, directeur grand Ouest chez Almond

Outre l'entreprise, la responsabilité, tant civile que pénale, du dirigeant peut elle aussi être engagée. Au civil, il faut démontrer qu'il n'y a pas eu de faute de gestion. « Mais cela est vite arrivé car ce peut être une simple imprudence ou une négligence », prévient encore Loullig Bretel. L'engagement de la responsabilité civile du dirigeant peut être menée par les associés. Seul réconfort ? « Au pénal, les sanctions sont évitables, via une délégation de pouvoir auprès du DSI ou du RSI qui eux-mêmes peuvent subdéléguer leur responsabilité. »

PRÉSERVER LA VALEUR DE L'ENTREPRISE

Rémi Bottin met en garde : « Tout ceci a un impact sur la valeur même de l'entreprise. » Il évoque une enquête réalisée auprès de sociétés cotées : celles qui s'étaient préparées aux risques cyber avaient certes connu une légère baisse de leur cotation mais avait connu une augmentation de 5% à horizon de douze mois. Quand celles qui étaient les moins préparées ont vu leur cotation chuter de 20%.

Alors comment éviter ces menaces cyber ? L'Anssi a produit une documentation détaillée sur les éléments incontournables à ne pas négliger : configuration des autorisations, droits d'accès, organisation de la sécurité interne, sensibilisation des acteurs pour éviter les erreurs… « Il y a une revue transverse à opérer, soit en interne si on en a les compétences et la bande passante, soit en externe via un prestataire », explique Nicolas Guilloux. « Un hackeur est une sorte de cambrioleur, rappelle Rémi Bottin. Il veut voir comment entrer. Il faut donc prévenir pour qu'il n'y arrive pas et s'en protéger. L'entreprise doit faire le tour de sa maison numérique : même si le système d'information est hébergé par un fournisseur, il faut vérifier qu'il est bien protégé. Car nous échangeons de plus en plus de flux qui fragilisent l'ensemble » *(voir à ce sujet p. 22)*.

Loullig Bretel insiste d'ailleurs sur ces relations contractuelles. « La sécurité est souvent mal prise en compte dans les contrats avec un prestataire informatique. Or, il faut la traiter à part entière. » Avec un point très important : le niveau de responsabilité du prestataire. « Les contrats excluent la plupart du temps leur responsabilité, notamment sur les dommages indirects tels que l'atteinte aux données, et prévoient quasi systématiquement un plafond de responsabilité. C'est alors l'entreprise qui supporte un risque qui réside pourtant chez le prestataire… Il faut donc négocier, de manière équilibrée, mais en déterminant un plafond qui comprenne bien l'ensemble des risques encourus par l'entreprise. »

Au final, quid du prix de cette sécurisation ? Pour Nicolas Guilloux, « ce qui coûte cher, c'est de se faire attaquer. Avec un coût médian de l'attaque à 50 000 € mais qui peut aller jusqu'à 800 000 € pour du rançonnage… Quand, pour 5 000 €, vous pouvez avoir un audit, des tests d'intrusion… »