Cybersécurité : comment sortir des radars des pirates

Chaque jour apporte son lot de cyberattaques. De la TPE à la multinationale, du particulier à la collectivité, personne n’est épargné. Mais que l’on se rassure (un peu) ! Il existe, aujourd’hui, un véritable arsenal pour tenir la menace éloignée.

Lundi, 8 h 45. Thibault, CEO dans une startup lyonnaise, a juste le temps de jeter un œil à ses mails avant un rendez-vous. Parmi les courriels reçus, l’un de ses prestataires lui envoie le lien vers un rapport sur lequel ils ont brièvement échangé au détour d’un post LinkedIn. L’adresse mail, le ton de l’interlocuteur : tout y est. Rien de suspect à première vue. Il télécharge le rapport. Un clic qui revient à confier les clés d’un coffre-fort à un pirate. A peine quelques heures suffiront pour que l’ensemble du réseau de l’entreprise soit chiffré et qu’une rançon soit demandée.

Désormais, ce type d’histoire ne relève plus de l’anecdote. En 2021, 1.082 cyberattaques ont été signalées en France, soit 37 % de plus qu’en 2020. Un chiffre qui serait loin de refléter la réalité, selon Brice Augras, hacker éthique et CEO de BZHunt *: « Même si le RGPD impose de notifier la violation de données, 75 % des entreprises victimes préfèrent encore taire une cyberattaques et ne pas porter plainte. »*

Pourtant, *« ça cogne fort, tout le temps et sur n’importe qui »*, rapporte Ingrid Söllner, directrice marketing de Tehtris, société spécialisée dans la

cybersécurité fondée par des anciens membres du renseignement français.

Vulnérabilités : prendre le pouls de l'entreprise

« Une entreprise n'est jamais trop petite pour être ciblée, insiste Philippe Luc, cofondateur et CEO d'Anozr Way. TPE, PME et ETI sont même des cibles de choix. *Elles n'ont pas encore la culture cyber et se pensent parfois en dehors des radars estimant qu'elles ne représentent pas une manne financière intéressante. Propriété intellectuelle, données… tout cela intéresse les pirates* » Ils optimisent leurs gains en attaquant les plus vulnérables, ceux qui n'ont pas la maturité ou la ressource financière pour engager une politique cyber.

Si le *phishing* (hameçonnage) reste une offensive très prisée, de nouvelles méthodes comme le *ransomware* arrivent en force. *« La question n'est plus de savoir si on risque la cyberattaque mais comment elle va se produire »*, résume Brice Augras. La réponse : anticiper. L'audit de sécurité est l'une des premières pierres du rempart. Du site web vitrine aux interfaces de connexion, en passant par les environnements de messagerie, quelle est ma surface d'exposition sur Internet ? *« La mauvaise configuration des outils déployés sur Internet est un problème fréquent,* observe le chercheur en cybersécurité. *Le marché propose de plus en plus de solutions sophistiquées mais si l'entreprise utilise en parallèle des identifiants aussi originaux que « admin », c'est un peu comme donner une Ferrari à quelqu'un qui ne sait pas conduire. »*

Une bonne hygiène informatique : la base

Avant même la vulnérabilité technique, il y a la faille humaine ! Elle est à l'origine de la majorité des attaques. Cliquer sur une pièce jointe, choisir un mot de passe commun à l'ensemble de ses applications, connecter sa e-cigarette à son poste de travail… *« Les pirates se saisissent de notre paresse,* souligne Luc Philippe. *Par exemple, il faut proscrire l'enregistrement automatique des mots de passe sur son poste et opter pour un coffre-fort de mot de passe. L'idéal est également d'avoir plusieurs adresses, une pour les contacts commerciaux, l'autre pour les fournisseurs, etc. »* Ne jamais remettre au lendemain les mises à jour !

62 % des salariés français disent ne jamais avoir bénéficié de formation à la cybersécurité (Baromètre de la cybersécurité en entreprise CESIN 2022). Une charte informatique qui consigne toutes les bonnes pratiques peut s'avérer très utile. L'Agence nationale de sécurité des systèmes d'information (Anssi)

propose un guide d'hygiène informatique *qui donne les clés pour sensibiliser les salariés, sécuriser le réseau, les postes et l'administration, authentifier et contrôler les accès… « Il n'en faut parfois pas plus pour qu'un pirate aille choisir une proie plus facile,* souligne Brice Auras. *Evidemment, ça ne suffit pas toujours. »*

À lire aussi

5 bonnes raisons de se former à la cybersécurité

Eviter l'empreinte numérique qui « parle » trop

Une date de naissance visible sur Facebook, des photos de vacances sur Instagram, une annonce de levée de fonds sur LinkedIn… *« Les pirates font avant tout du renseignement,* rappelle Philippe Luc, CEO d'Anozr Way dont la solution vise notamment à réduire l'exposition numérique face à la menace cyber. *Toutes les données issues de notre empreinte numérique représentent une matière première de choix. Il ne s'agit pas de bannir les réseaux sociaux. Mais plutôt de maîtriser ce qu'on y met pour ne pas devenir une cible. »*

Et tout cela, c'est sans compter sur ce qui circule sur le dark web. « Aujourd'hui, *72 % des données volées et diffusées sur le darkweb sont des données personnelles des salariés »,* souligne le CEO d'Anozr Way qui prône, en matière de cybersécurité, le préventif plus que le curatif. En moyenne depuis le début de l'année 2022, chaque attaque par ransomware engendre la violation de données de plus de 3.300 personnes.

Attaque moi si tu peux

« Plus il y a de couches de sécurité, plus ça peut décourager un pirate », indique Brice Augras évoquant une sorte de stratégie de l'oignon.

« L'humain ne peut pas tout, estime Ingrid Söllner, directrice marketing de Tehtris dont la solution de remédiation permet de bloquer les intrusions en peu de temps. *Certains assauts se déploient en moins d'une minute. Parfois, l'entreprise ne se rend même pas compte qu'elle a été attaquée. Les pirates s'installent dans les systèmes d'information et attendent sagement le week-*

end ou les vacances pour lancer l'attaque. »

L'anticipation, c'est aussi le bon sens qui veut que l'on réalise des sauvegardes très régulières et déconnectées du système. Cela permet une reprise des activités opérationnelles plus rapide en cas de problème.

Autre possibilité : organiser sa propre attaque via des *pen tests*. « *Ce sont des opérations d'intrusion informatique et parfois physique qui permettent de mettre les outils et les systèmes d'information d'une entreprise à l'épreuve d'une attaque dans les conditions du réel* », expose Brice Augras. Une technique efficace pour détecter ces failles avant un pirate. Ne dit-on pas que la meilleure défense… c'est l'attaque.

Article écrit par MADDYNESS AVEC SALESFORCE