Les effectifs réduits l'été oblige t les e treprises à re forcer leur résilie ce, explique **Neil Levi** , expert e cybersécurité

« Les hackeurs aime t surtout les vaca ces des décideurs »

Ecra total

lors que la Direction générale des finances publiques a révélé, jeudi 13 août, que les données fiscales de près de 680 000 personnes avaient été piratées, le sujet de la cybercriminalité est plus actuel que jamais. Les attaques, menées par des pirates de plus en plus néophytes, ont souvent lieu l'été, saison de tous les dangers en la matière.

Interview lice Clavier

JULIO LOPEZ/PEXELS

Les **attaques cyber** sont toujours plus sophistiquées et vont augmenter dans les années à venir.

C'EST UN CONST T établi par les professionnels de la sécurité : l'été, les cyberpirates profitent des équipes réduites et de leur vigilance relâchée pour passer à l'action. Neil Levin, expert cyber et senior manager dans les équipes de MC2I, un cabinet de conseil français spécialisé en transformation numérique, explique à l'Opinion comment s'en prémunir.

Pourquoi la saison estivale est-elle la période idéale pour les cybercriminels ?

Les cybercriminels aiment surtout les vacances des décideurs. Pendant l'été, les vulnérabilités technologiques des entreprises n'augmentent pas, mais la diminution des capacités humaines affaiblit la défense. Les effectifs réduits diminuent le temps de réactivité face à une attaque. Les remplacements pendant l'été, aussi bien au sein de l'entreprise, sur des fonctions critiques, que l'arrivée de personnes ou de prestataires externes, peuvent affaiblir les systèmes si les processus de gestion de crise ne sont pas bien maîtrisés par les nouveaux venus. Enfin, la vigilance décroît aussi pendant cette période, les règles de sensibilisation sont parfois appliquées moins scrupuleusement.

C.G. JERUS LMI

Neil Levi , expert en cybersécurité et senior manager au sein du cabinet MC2I.

Toutes les entreprises peuvent être visées, quels que soient le secteur ou leur taille. Les attaques cyber se démocratisent de plus en plus et elles vont augmenter dans les années à venir. Elles sont aussi bien menées par des groupes et des spécialistes que par des personnes inexpérimentées qui dénichent des conseils et techniques sur le dark web.

Quelles sont les failles les plus exploitées ?

L'humain, quelle que soit la saison, est le facteur clé de la compromission. Les pirates visent souvent des postes de décideurs. Ils cartographient précisément l'écosystème de l'entreprise pour cibler les différents décideurs et essayent d'usurper leur identité. Le graal, c'est le mail de phishing : si une personne n'est pas suffisamment sensibilisée à ce sujet, elle donne ses identifiants et, pour peu qu'elle ait des accès informatiques et administrateurs, l'attaquant peut se faire passer pour elle. C'est difficile de se défendre, dans ce cas de figure, car on a en face de nous un utilisateur qui semble légitime du point de vue informatique.

« Le erf de la guerre, c'est la se sibilisatio . Il faut que chaque acteur au sei de l'e treprise adopte les bo s réflexes : e pas utiliser deux fois le même mot de passe, avoir des processus d'authe tificatio complexes… »

D'autres techniques existent : les deepfakes, l'authentification à un seul facteur, des applications mal sécurisées, des défaillances au niveau des développeurs ou via le réseau… La liste est très longue et c'est une difficulté : le hackeur va trouver une porte d'entrée et s'y faufiler mais l'entreprise qui se protège doit prendre en compte toutes les possibilités.

Comment faire pour limiter le risque ?

Le nerf de la guerre, c'est la sensibilisation. Il faut que chaque acteur au sein de l'entreprise adopte les bons réflexes : ne pas utiliser deux fois le même mot de passe, utiliser des identifiants multifacteurs, avoir des processus d'authentification complexes… Plus précisément, pour préparer la période estivale, il faut mettre en garde ceux qui feront du télétravail : le wifi public, dans les transports, les salles d'attente ou les hôtels peut être vicié. Quant aux équipes réduites sur place, elles doivent, si c'est possible, diminuer le seuil d'alerte habituel pour réagir à la moindre situation suspecte.

La préparation de la période estivale concerne aussi la résilience : si on est attaqué, que fait-on ? Si les serveurs sont attaqués, comment reconstruire le service informatique ? Il est important d'avoir une maîtrise complète de la chaîne et de ses sauvegardes pour que l'activité se poursuive en cas de cyberattaque. La protection et la résilience vont de pair.

Comment réagir si c'est trop tard ?

Si l'entreprise est bien préparée, on applique le plan de continuité d'activité pour maintenir les fonctions vitales de l'entreprise. Ensuite, on applique le plan de reprise de l'activité pour retrouver la stabilité qui précédait la crise ou adopter un nouvel équilibre. Si ces plans sont prêts et mis à jour, il suffit d'activer la cellule de crise en temps voulu et d'avancer.

En revanche, si l'entreprise n'a pas anticipé, les dégâts seront mesurés en fonction du niveau de protection et de ses failles : à quel niveau les pirates sont-ils entrés, est-ce que seul le service informatique est touché ou est-ce toute l'entreprise, a-t-on réussi à les freiner, à cloisonner les services, est-ce que les hackeurs viennent d'entrer ou sont-ils là depuis deux mois, ont-ils eu le temps d'exfiltrer et de chiffrer les données…

Dans ce cas-là, il faut contacter une entreprise pour rechercher des preuves de cette intrusion, comprendre le comportement des intrus et remédier à la situation, si c'est possible. Mais attention, les employés ne doivent toucher à rien et laisser faire les professionnels : c'est comme une scène de crime.

Et l'I , dans tout ça ? Est-ce un outil pour les pirates ou un bouclier pour les entreprises ?

Les deux. L'I ne crée pas elle-même de nouvelles vulnérabilités mais elle permet d'augmenter l'ampleur des attaques, leur volumétrie et leur étendue, et de supprimer les signaux faibles qu'on utilisait avant pour détecter une attaque. Par exemple, quand on recevait un mail suspect, on faisait attention aux fautes d'orthographe, à l'adresse de l'expéditeur, au manque de cohérence et de clarté du mail… L'I lisse tout ça. Pire : elle peut construire le persona d'un individu en fonction de tout ce qui existe à son sujet sur Internet et sur les réseaux sociaux. Le mail de phishing sera bien plus ciblé et précis.

Pour autant, l'I peut aussi être employée pour lutter contre des intrusions en détectant plus rapidement les incohérences de requêtes ou mouvements au sein du système, mais aussi pour optimiser les processus de gouvernance. C'est aussi un très bon outil pour rendre la sensibilisation à la cybersécurité et la formation plus immersives et adaptées aux utilisateurs.

Thi kagai Ciotti, les attaques russes et le Co seil co stitutio el : la liberté de pe ser e péril

La chro ique de Eric Le Boucher

JE N-FR NÇOIS P G

La capacité de penser librement sera la grande question du XXIe siècle. llons-nous pouvoir encore faire naître un esprit critique chez les enfants, celui qu'on leur enseigne depuis Socrate ? llons-nous pouvoir conserver un espace public de débat libre, avec une presse pluraliste et des partis politiques de qualité, comme s'en inquiétait Jürgen Habermas ? La semaine qui vient de s'écouler illustre, par trois événements, combien la question de la liberté de penser devient centrale.

Un : « Le macronisme menace nos libertés », s'émeut Eric Ciotti dans *Le Jour al du Dima che*. Il dénonce une « dérive illibérale ». « Quand on parle d'interdire X ou de fermer CNews, je dis que notre démocratie est en danger ».

Deux : chez nos voisins allemands, le projet du gouvernement d'étendre le pouvoir de l'agence de surveillance du territoire pour créer des « réels services secrets » a fait resurgir le spectre de la Stasi d'avant la chute du mur de Berlin.

Trois : le Conseil constitutionnel a rejeté la loi sur l'interdiction de l'accès des moins de 15 ans aux réseaux sociaux au motif d'un texte « non adapté et non proportionné ».

Le cœur de la menace soulevée par chacun de ces trois événements est la technologie. D'abord parce que sa puissance démultipliée permet à une dictature (chinoise, russe…) une surveillance de plus en plus parfaite de ses propres citoyens et une déstabilisation « cyber » de ses ennemis réels ou supposés.

Ensuite parce que la technologie numérique utilise la connaissance et l'intelligence, autrement dit elle entre dans les têtes, les façonne, les asservit. La menace technologique est, de la sorte, double : collective et individuelle.

Lig e de crête. Si Berlin veut renforcer ses services, c'est en clair pour lutter contre les attaques informatiques russes. La difficulté est que le parti d'extrême droite fD a été classé « suspect d'extrémisme » et qu'il va en tirer argument pour se plaindre d'être « surveillé ».

« Etablir la vérité des faits, e premier celle des attaques russes, est la première étape de la préservatio de la démocratie, mais les i stitutio s do t c'est le rôle, la presse et les partis politiques, e le fo t pas »

On assiste à une inversion de la charge : l'extrémisme de droite, favorable au dictateur Vladimir Poutine, accuse le pouvoir démocratique allemand d'être liberticide.

Eric Ciotti fait la pure démonstration pour la France de cette inversion des charges. Le rallié au Rassemblement national nie la véracité des attaques russes contre les candidats Edouard Philippe, Gabriel ttal et Raphaël Glucksmann, en parlant « de pseudo-attaques » et de « stratégie de communication », mais il s'en prend au président de la République.

Que celui-ci, sous influence de la gauche, se soit fourvoyé dans l'impasse d'une charte pour les journaux est une chose (les états généraux de l'information). Mais qu'il veuille contrôler et censurer la presse, la liberté d'écrire et de penser, est une grossière absurdité.

La bataille des idées utilise, comme toutes les guerres, des ruses et des leurres. Tout gouvernement démocratique est sur une ligne de crête : pour défendre la liberté, il lui faut en effet « surveiller » les intrusions des agents russes mais sans dépasser une frontière, forcément délicate à tracer, de la liberté de ses citoyens.

Le juge de paix est « la confiance » que ces citoyens doivent porter à leurs élus de rester démocratiques. L'extrême droite est, a contrario, « suspecte » de ne pas faire de la liberté son mantra mais, passant à l'attaque, elle veut faire croire tout l'inverse. Si le débat public s'est détraqué au point que la confiance dans les autorités est devenue défiance, la manœuvre peut marcher.

Or, nous y sommes. Etablir la vérité des faits, en premier celle des attaques russes, est la première étape de la préservation de la démocratie, mais les institutions dont c'est le rôle, la presse et les partis politiques, ne le font pas. ucune ne s'est attardée sur les mensonges pro-russes d'Eric Ciotti. Lorsque ceux qui sont en devoir de défendre les faits s'égarent dans la course à la polémique et la démagogie, n'ayant d'yeux que pour leur « audience », ils perdent toute référence et toute ligne.

Médiocrité i tellectuelle. Cette défaite au niveau « collectif » du débat public s'explique-t-elle parce que le numérique aurait déjà gagné la bataille au niveau « individuel », des militants politiques, des intellectuels, des journalistes ? La capacité de penser librement est-elle déjà réduite, laminée par l'effet destructeur des réseaux sociaux ? Le Conseil constitutionnel ne le pense pas. Il croit qu'il y a de bons sites et des mauvais sites pour les enfants et qu'il faut une loi plus précise. -t-il raison ? Je ne le pense pas.

« Il est paradoxal de voir que c'est l'extrême gauche qui est à l'origi e du recours au Co seil co stitutio el. Sa s doute estime-t-elle avoir gag é la bataille des idées sur les réseaux sociaux et que pour cette raiso , il e faut pas les fermer »

Pour se convaincre de la transformation inouïe des cervelles à laquelle on assiste, il suffit de lire, parmi des centaines d'autres scientifiques, Ioan Roxin, professeur émérite à l'université Marie et Louis Pasteur (Polytechnique Insights du 3 juillet).

« L'utilisation massive d'Internet et des réseaux sociaux a déjà fragilisé notre rapport au savoir (…). Je ne crois pas exagéré de dire qu'ils poussent globalement à une médiocrité intellectuelle, émotionnelle et morale. Intellectuelle parce qu'ils favorisent une surconsommation de contenus sans véritable analyse critique, émotionnelle parce qu'ils occasionnent une dépendance toujours plus profonde aux stimulations et au divertissement, et morale, parce que nous sommes tombés dans une acceptation passive des décisions algorithmiques ».

L'arrivée de l'I va amplifier cette atrophie cognitive en réduisant encore « l'effort intellectuel nécessaire pour transformer une information en connaissance ». Conclusion : « nous risquons une uniformisation de la pensée, c'est déjà le cas dans les jeunes générations ».

Le péril sur la liberté de penser est plus grave que ne le pense le Conseil constitutionnel puisque le mal est dans les algorithmes eux-mêmes. Une interdiction totale pour les moins de quinze ans est une précaution indispensable pour se donner le temps de leur construire un esprit critique.

Il est paradoxal de voir que c'est l'extrême gauche qui est à l'origine du recours au Conseil constitutionnel. Sans doute estime-t-elle avoir gagné la bataille des idées sur les réseaux sociaux, chez les jeunes en particulier, et que pour cette raison, il ne faut pas les fermer. Ce n'est pas faux sur le constat. Mais c'est désolant de voir un parti content de gagner la guerre des idées lorsqu'il n'y a plus d'idées.

@EricLeBoucher

Retrouvez **toutes os chro iques** sur lopi io .fr