

L'empreinte numérique du dirigeant : rien à cacher, tout à perdre

par

Yoan BLANC

Analyste OSINT

"Je m'en fous, je n'ai rien à cacher."
"Personne ne s'intéresse à nous, on est trop petits."
"Mais tout le monde s'en fout d'où je pars en vacances."

Ces phrases, vous les avez probablement déjà entendues. Peut-être les avez-vous même prononcées. Pourtant, elles révèlent une dangereuse méconnaissance des enjeux liés à l'empreinte numérique.

Dans notre monde hyperconnecté, chaque information publiée, chaque donnée partagée, chaque trace laissée en ligne constitue une brique dans l'édifice de votre identité numérique. Et cet édifice, qu'on le veuille ou non, peut devenir une cible de choix pour qui sait l'exploiter.

Une exposition croissante et souvent involontaire

L'empreinte numérique d'un dirigeant se construit jour après jour, et parfois à son insu.

Elle commence par les données publiques légales, ces informations que la loi nous oblige à rendre accessibles :

- Les registres du commerce livrent vos mandats sociaux.
- Le cadastre révèle vos investissements immobiliers et vos SCI familiales.
- Les publications légales racontent l'histoire de vos nominations, de vos révocations, de vos créations d'entreprises.
- Chaque réponse à un marché public, chaque dépôt de brevet devient une pièce du puzzle.

Mais l'exposition ne s'arrête pas là.

Les réseaux sociaux professionnels dessinent votre parcours, révèlent vos centres d'intérêt, cartographient votre réseau. Vos interventions publiques, qu'elles

soient filmées ou retranscrites, figent dans le temps vos opinions, vos positions, vos ambitions. Chaque conférence, chaque interview, chaque article de blog contribue à façonner votre image numérique.

Et il y a aussi les traces que les autres laissent pour vous. Une photo partagée par un proche, une mention dans un article de presse locale, un commentaire d'un collaborateur sur LinkedIn. Votre empreinte numérique échappe en partie à votre contrôle, alimentée par un entourage qui ne mesure pas toujours les conséquences de ses partages.

Des risques bien réels pour l'entreprise

Cette accumulation d'informations représente une véritable mine d'or pour les cybercriminels.

Le spear-phishing¹ devient redoutablement efficace quand l'attaquant connaît vos habitudes, vos déplacements, vos centres d'intérêt. L'usurpation d'identité se fait plus crédible quand elle s'appuie sur des détails authentiques de votre vie. Le social engineering exploite les failles humaines révélées par votre présence en ligne.

Les conséquences peuvent être dévastatrices.

Un ransomware bien ciblé paralyse votre entreprise. Un chantage aux données personnelles met en péril votre réputation. Une campagne de désinformation orchestrée fragilise votre position. L'image de votre entreprise devient otage de votre exposition numérique.

Au-delà des risques directs, cette transparence forcée peut compromettre vos projets stratégiques. Vos déplacements trahissent vos ambitions d'expansion. Vos recrutements racontent vos orientations futures. Vos likes et partages révèlent vos affinités commerciales.

Dans un monde où l'information est pouvoir, votre empreinte numérique devient une vulnérabilité stratégique.

¹ Ou hameçonnage ciblé : méthode de piratage qui consiste à usurper l'identité d'un de vos contacts pour vous piéger.

Et à l'heure des deepfakes, où il est possible de cloner la voix de quelqu'un grâce à un échantillon de voix d'une minute à peine, ces risques sont décuplés.

Une protection nécessaire et possible

Vous allez penser que je conseille aux dirigeants d'aller vivre dans une grotte, mais ce serait oublier bien vite que dans nos secteurs d'activité, le dirigeant doit incarner son entreprise pour asseoir sa réputation et trouver des clients.

Le conseil à apporter n'est donc pas de disparaître d'internet mais de contrôler activement son image numérique et de connaître les informations disponibles sur internet.

Cette notion s'appelle l'hygiène numérique : il faut cartographier votre exposition, identifier les sources d'information, comprendre les vulnérabilités. Cette démarche, similaire à un audit de sécurité informatique, révèle souvent des surprises. Des informations qu'on croyait privées s'avèrent publiques. Des données qu'on pensait effacées resurgissent dans des archives.

Et bien entendu, le dirigeant ne doit pas être le seul à mener ces actions : cette vigilance doit s'étendre à votre entourage. Vos collaborateurs, votre famille, vos proches doivent comprendre les enjeux liés à la sécurité de leur vie privée, mais aussi à la sécurité de leur entreprise.

Conclusion

La maîtrise de l'empreinte numérique n'est pas un concept abstrait mais une réalité stratégique dont doivent se saisir les chefs d'entreprises, quels que soient leur secteur d'activité ou leur taille.

Face aux "je n'ai rien à cacher", il faut désormais répondre "j'ai tout à perdre".

Sans tomber dans un alarmisme commercial, il faut envisager la sécurité de l'information de la même manière que la sécurité physique d'un site. Si un dirigeant sait qu'une porte de l'entrepôt ferme mal, il la fera réparer, ou mettra un vigile à cet endroit... Pourquoi ne pas faire pareil sur internet ? Il ne faut pas voir cette hygiène numérique comme une contrainte mais comme un investissement dans la résilience de votre entreprise.

Dans un monde où la désinformation et la tromperie sont des armes, il serait dommage de ne pas se protéger.