FACE AU RISQUE CYBER, les dirigeants et hauts cadres sont personnellement concernés

Aujourd'hui, le risque cyber est à l'intersection entre l'humain et la technologie. Les dirigeants et personnes clés au sein des organisations sont directement pris pour cible par les cybercriminels et autres adversaires. Cet enjeu ne doit plus être cantonné uniquement aux départements IT : chacun doit avoir les moyens d'assurer sa propre protection personnelle. Grâce à des solutions de protection cyber dédiées aux VIP & Key People, *ANOZR WAY* accompagne les entreprises et leurs dirigeants afin d'anticiper et de mieux prendre en compte ce risque. *Explications du CEO et cofondateur, Philippe Luc.*

Philippe Luc

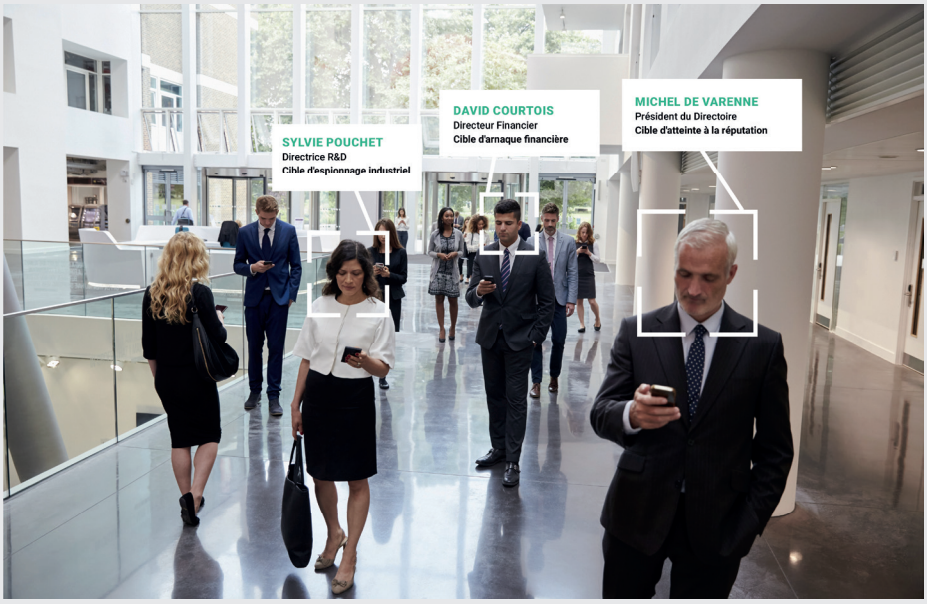
Les enjeux des menaces cyber pour les décideurs semblent encore méconnus et sous-estimés aujourd'hui, malgré l'explosion des attaques et les impacts conséquents pour les entreprises. Comment cette menace a-t-elle évoluée ?
Dans le domaine cyber, tous les attaquants ne cherchent pas forcément à franchir les défenses physiques des entreprises (firewall, VPN, anti-virus ...). Ils sont nombreux à privilégier des modes opératoires qui permettent de contourner ces dispositifs de sécurité habituels. Je pense notamment aux scénarios à base d'usurpation d'identité qui sont monnaie courante de nos jours. C'est ce qu'on appelle des attaques par ingénierie sociale qui représentent sept attaques sur dix.
D'ailleurs, une nouvelle terminologie est apparue au cours des dernières années face à la recrudescence de ces attaques. On parle dorénavant de « spear phishing » (attaque par hameçonnage ciblé contre des personnes de 1er rang) ou « whaling » (fraude au président) qui ciblent particulièrement les cadres dirigeants. Les chefs d'entreprise et hauts-cadres sont douze fois plus ciblés que les autres collaborateurs, car ont accès aux informations critiques et stratégiques, voire au capital de l'entreprise.
On voit bien qu'il ne s'agit plus uniquement de protéger le système d'information mais bien de permettre aux personnes clés des organisations de ne plus être ciblées.

Quelles sont les conséquences pour l'entreprise et ses dirigeants ?
Au-delà du vol d'argent, les conséquences financières de ces attaques peuvent prendre différentes formes : chute de la valorisation boursière pour les entreprises cotées, baisse du chiffre d'affaires due à l'impact sur l'activité, la notoriété et l'image, mais aussi à la perte de confiance des clients, des prospects et des partenaires.
Sur un plan plus personnel, les dirigeants et hauts cadres victimes peuvent voir leur ascension professionnelle bloquée et leur image portée à mal. C'est pour cette raison qu'il est essentiel de maîtriser ses données exposées, qu'elles soient d'ordre professionnel ou personnel. Les adversaires n'ont pas de tabou, ils vont rechercher et exploiter tout ce qui peut leur être utile pour compromettre, manipuler et porter atteinte à ces personnes.

Nous comptons parmi notre lectorat de nombreux chefs d'entreprise, mais aussi des hauts cadres dans des entreprises privées et publiques. Quels conseils pourriez-vous leur donner ?
Il est essentiel de prendre conscience qu'aujourd'hui le point de départ pour des individus malveillants qui préparent leurs attaques commence toujours par une phase de renseignement sur l'entreprise et son organisation. Plus l'entreprise et les personnes qui la composent exposent généreusement des informations, plus il sera facile d'élaborer des scénarios d'attaque difficiles à contrer. Ces informations sont aussi partagées et rendues disponibles sur

internet à notre insu par des tiers. Dans le passé cette phase de reconnaissance s'appuyait sur des techniques de renseignement classiques. L'avènement du web et des réseaux sociaux l'ont rendu plus prégnante et dangereuse.
Les dirigeants n'ont pas toujours conscience de toutes les informations exposées librement sur internet et de leur niveau de dangerosité une fois cumulées. Pour se prémunir efficacement contre ce risque des solutions existent, c'est ce qu'ANOZR WAY propose. Ce n'est pas une fatalité et il ne tient qu'à eux de devenir une cible moins attractive et facile à atteindre !

Comment accompagnez-vous les chefs d'entreprises et hauts cadres pour résoudre ces sujets qui les atteignent personnellement ?
Les équipes dédiées à la cybersécurité ou à la protection technique de l'entreprise ne sont pas formées pour traiter ces menaces. Ces attaques ciblent de manière directe des dirigeants sur des sujets souvent personnels qu'ils ne veulent ou ne peuvent pas forcément partager avec leur entreprise.
Dans ce cadre, nous nous positionnons comme un tiers de confiance avec qui ils vont pouvoir aborder ces sujets potentiellement problématiques de manière confidentielle et personnalisée afin de gérer leurs traces et empreinte numérique.
Notre programme premium de protection permet aux VIP & Key People d'être en maîtrise de leurs propres données et de bénéficier d'une protection continue. Nous trouvons des solutions pour réduire le niveau d'exposition personnelle face à ces menaces et mettons en place un suivi dans la durée. L'objectif est de prévenir et anticiper une exploitation malveillante de leurs données qui pourrait nuire à l'entreprise ou à leur personne.
Les dirigeants et hauts cadres bénéficient d'une solution logicielle basée sur de l'IA qui fait office de cyber bodyguard tout en étant accompagnés par des experts issus des services régaliens (services de renseignement français, cellules de lutte contre la cybercriminalité de la gendarmerie).



Quelle est la genèse d'ANOZR WAY ?
ANOZR WAY est le fruit de ma rencontre avec mon associé Alban Ondrejeck. Je suis issu d'une école de commerce et ancien dirigeant dans le secteur de l'assurance, avec une expérience dans le conseil en organisation et en management et gestion des risques. De son côté, Alban est ingénieur de formation, ancien officier dans les services de renseignement français et ancien directeur cybersécurité chez Orange Business Services.
Très tôt, dans le cadre de ses missions, il a pu se rendre compte qu'il était plus simple de faire des recherches en ligne que d'avoir recours aux méthodes traditionnelles (mise sur écoute, suivi des personnes…). Il a ainsi développé un véritable savoir-faire dans la reconstitution de l'empreinte numérique des personnes à partir des internets : le web indexé par Google, dont les réseaux sociaux, jusqu'au darkweb, espace où circulent les données piratées et volées.
Dans ce contexte, c'est la combinaison de nos expériences respectives et de nos expertises qui nous a poussé à créer la société. Nous avons développé une technologie innovante pour automatiser ce savoir-faire et permettre une analyse fine à des fins de protection. Nous accompagnons sur ces enjeux des entreprises et membres de Comex issus du monde de la finance, de l'industrie, de l'énergie…

Quelles sont les prochaines étapes pour ANOZR WAY ?
Nous connaissons une très forte croissance : nous sommes passés de cind à près de trente collaborateurs en dix-huit mois. Nous préparons aussi notre internationalisation hors des frontières européennes et des opérations de financement pour nous donner les moyens de nos ambitions.

"Il ne s'agit plus uniquement de protéger le système d'information mais bien de permettre aux personnes clés des organisations de ne plus être ciblées."