Le dirigeant d'entreprise privée ou publique se doit de préparer son plan de réponse à incident cybersécurité : quel est le chemin de l'attaque ?

Lorsqu'une entreprise privée ou publique n'est pas préparée à gérer un incident cyber, les conséquences peuvent être lourdes, s'enchaîner et s'accumuler : voici quelques éléments clés.

L'irrationnel
• La première étape d'une attaque cyber : le dirigeant de l'entreprise ne comprend pas ce qu'il lui arrive.
• La deuxième étape, il se demande pourquoi lui ?
• La troisième étape, aurait-on pu l'éviter ?
• Et si les tensions sont fortes en interne, le dirigeant veut trouver le coupable parce qu'il y a forcément une cause interne à cet incident cyber.

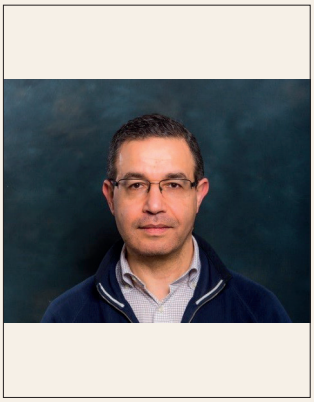
Le rationnel
• Il commence à réaliser les conséquences d'une dégradation du service/métier.
• Il demande aux équipes IT une solution.
• Il évalue les pertes commerciales.
• Il cherche des solutions pour continuer à opérer.
• Il communique plus au moins bien ou pas avec ses clients, ses actionnaires, ses parties prenantes.

La raison
• Il cherche désespérément un prestataire pour aider à résoudre le problème mais cela n'était pas prévu au budget !
• Il commence à comprendre le problème.
• Les équipes commencent à s'organiser pour rendre le service/métier en mode dégradé.
• Il identifie le problème.
• Il cherche à tout prix à rétablir le système d'information.
• Sans trop savoir si l'attaquant pourra revenir dans le système d'information.

« Les emmerdes volent en escadrilles »
• Il découvre que les données captées sont exposées sur le darknet et à la vente.
• Il réalise qu'il faudra plusieurs semaines voire des mois pour rétablir une situation normale.
• Il peut se voir exposer dans les médias et les réseaux sociaux.
• Il reçoit un ou plusieurs recommandés de clients mécontents.
• Il commence à comprendre qu'il va falloir demander au service juridique de travailler le sujet (CNIL/RGPD, DORA, NIS 2, IA, etc.).
• Il observe une érosion de l'activité commerciale les semaines ou mois qui suivent l'attaque.

« Circulez y'a rien à voir»
• La crise finie, on veut oublier tout cela.
• On n'a pas le temps de comprendre.
• Et puis l'IT, c'est ennuyeux.
• Alors on ne prend pas le temps de se corriger.
• De toute manière, l'activité commerciale reprend.

Un an, deux ans plus tard : l'histoire se répète



• Le dirigeant avait identifié le problème mais pas son origine.
• Il avait tout de suite cherché à rétablir la situation à la normale.
• Mais il n'avait pas compris que l'attaquant avait mis en place un chemin d'attaque.
• Et l'attaquant a revendu ses accès dans le système d'information à un autre groupe d'attaquant.
• Et là je vous laisse imaginer le scénario…

Que retenir de ce constat ?

Les militaires s'entraînent tout au long de l'année car ils doivent être capables de réagir face à des situations extrêmes parfois imprévisibles. Les pompiers s'entraînent à éteindre le feu. Il doit en être de même pour les sociétés/organisations. Les organisations doivent intégrer dans leur gestion du risque la capacité de se préparer à répondre à un incident de sécurité et de s'exercer pour y remédier. Préparer son plan de réponse à incident, c'est :
• Cartographier ses données sensibles (ce qui a de la valeur).
• Préparer les équipes à intervenir (qui fait quoi ?).
• Identifier qui fera la réponse à incident (maîtriser les coûts).
• Être accompagner pour bien communiquer.
• Impliquer le juridique pour maîtriser les conséquences en amont et en aval de l'incident.
• S'adosser à un assureur/courtier pour disposer de services idoines et performants.
• Faire travailler les métiers avec les équipes IT.
• Simuler régulièrement des incidents dans des exercices de *war room*.

En se préparant à définir une stratégie de réponse à incident, en la simulant et en se faisant accompagner par des experts (ingénieurs cyber, juristes spécialisés cyber, etc.), le dirigeant d'entreprise privée ou publique évitera l'impensable, contrôlera ses coûts, sa communication rassurera son environnement (clients, actionnaires, parties prenantes) et finalement se construira une posture cyber qui est la capacité de démontrer que l'entreprise est résiliente. La cyberattaque est certaine un jour ou l'autre, sa date de survenance ne l'est pas. Il faut donc se préparer à l'affronter avec détermination et professionnalisme.

Mohamed BEGHDADI
Directeur Cybersécurité
Ingénieur réseaux & télécom
Membre d'EUROLAW FRANCE CYBER