Attaques ciblées : comment gérer le risque en amont ?

Gérôme Billois

Attaques ciblées : comment gérer le risque en amont ?

(Article rédigé en collaboration avec Frédéric Chollet)

Si la gestion de crise lors d'une attaque doit suivre les 4 principes clés évoqués dans notre précédent article, elle doit surtout en intégrer l'anticipation dans ses mécanismes.

Une stratégie à moyen terme basée sur l'anticipation des attaques ciblées

Dès aujourd'hui, il est nécessaire de refondre les processus de gestion de crise. Les scénarios de cybercriminalité doivent être inclus dans les procédures opérationnelles (modalités de réponse, SI spécialisé…). Les relations avec les autorités compétentes doivent être créées ou renforcées dans le but d'accélérer la phase de mobilisation de ces acteurs et de maîtriser les circuits de communication.

Une stratégie de communication claire doit être définie en fonction des acteurs évoluant dans et autour de l'organisation. Les obligations de demain (notification aux clients des fuites de données à caractère personnel…) doivent être anticipées afin de garantir le moment venu un respect des règlementations en vigueur. De ce fait, il ne sera plus possible de garder la confidentialité sur le fait qu'une crise est en cours.

Les attaques ciblées étant souvent constituées d'une somme d'incidents unitaires, il est nécessaire de revoir en parallèle les processus de gestion des incidents pour s'inscrire dans une démarche itérative, garantissant un état de veille constant, une rapidité d'intervention et une prise de recul.

À moyen terme, évaluer son attractivité et connaître ses actifs clés permettent de déterminer les informations attirantes pour des attaquants. Le secteur d'activité et le positionnement sur le marché sont des éléments déterminants. Au-delà de données internes, les relations entretenues avec certains partenaires et / ou clients peuvent augmenter l'attractivité du SI aux yeux d'attaquants. Cette évaluation doit s'inscrire dans une revue régulière des risques avec les métiers.

Enfin, il faut mettre en place des mesures avancées pour permettre une sécurisation renforcée des cibles identifiées avec les métiers en sanctuarisant les périmètres les plus sensibles (applications métiers clés, VIP / COMEX…) mais aussi les systèmes techniques clés (serveurs et postes d'administration, infrastructure à effet d'amplification comme la télédistribution ou l'Active Directory).

Des approches plus actives (demande de fermeture des sites utilisés pour l'exfiltration, honeypot …) peuvent être envisagées.

Attaques ciblées : comment gérer le risque en amont ?

Complexifier l'attaque pour en diminuer sa rentabilité

Les attaques ciblées représentent un challenge pour les grandes organisations qui ne sont pas habituées à gérer ce type de crise silencieuse, à grande échelle, mêlant métier et SI et entraînant une perte de confiance dans ce dernier. Leur gestion nécessite de revoir les processus en place mais également de prévoir des actions pour rendre l'attaque plus difficile, faciliter leur détection et renforcer les capacités de réaction.

La mise en place de ces éléments permettra de complexifier les actions de l'attaquant et, à terme, de rendre l'attaque moins rentable ! C'est certainement une des clés de réponse face à ces nouvelles menaces.

Lire la première partie

Pour en savoir plus, lire le focus attaques ciblées, une refonte nécessaire de la gestion de crise.