Attaques ciblées : une refonte nécessaire de la gestion de crise

Gérôme Billois | Manager

Attaques ciblées : une refonte nécessaire de la gestion de crise

(Article rédigé en collaboration avec Frédéric Chollet)

La cybercriminalité ne cesse de croître. Les cas concrets se multiplient.

Les retours d'expérience montrent la difficulté à gérer des crises d'un nouveau type. Ces attaques ciblées sont souvent des crises silencieuses qui atteignent directement la confidentialité des données sans remettre en cause le fonctionnement visible du SI. Ces crises sont difficiles à matérialiser, à traiter et finalement à clore de manière définitive.

Comment réagir à ces attaques ? Quelles démarches et organisations doit-on mettre en place pour se préparer au mieux ? Quelles actions de traitements doivent être mises en œuvre ?

Refondre les piliers de la gestion de crise

Une attaque ciblée n'est pas une crise SI mais bien une crise métier

En effet, si cette attaque a lieu c'est pour voler ou altérer des données métiers. Il est donc primordial d'impliquer les métiers et d'identifier les enjeux métiers actuels (contrats importants, fusion / acquisition, R&D…) afin d'anticiper les cibles de l'attaque et d'agir pro-activement. Dans le même esprit, et suivant les contextes, un support auprès d'entités étatiques peut également être recherché. Les équipes SI, malgré leur vigilance, ont un périmètre d'observation trop large pour être attentives sur tous les fronts. Identifier les cibles métiers majeures permettra de focaliser l'attention sur les périmètres sensibles.

Augmenter sa visibilité sur le système d'information

Pour analyser l'attaque et proposer des contre-mesures efficaces, il est nécessaire de détecter et de rapprocher les successions d'incidents unitaires et d'événements suspicieux. Pour cela la mobilisation des équipes d'experts « forensics » est essentielle. Ils seront à même de comprendre le fonctionnement des codes malicieux utilisés pour l'attaque et de pouvoir proposer des plans d'actions techniques pertinents. Ces ressources, encore trop rares aujourd'hui, devront être rapidement mobilisées.

L'utilisation d'outils pour capter les « signaux faibles » (analyses de journaux, sondes réseaux et détec-

Attaques ciblées : une refonte nécessaire de la gestion de crise

tion d'intrusion) est également un vrai plus malheureusement encore peu généralisé. Notre retour d'expérience montre qu'il est possible de déployer rapidement ce type d'outil pendant une crise mais il nécessite un degré d'expertise fort pour être efficace.

S'astreindre à prendre du recul face à une multitude d'attaques silencieuses et trompeuses

Il est important de prendre régulièrement du recul, malgré la multitude d'évènements, pour comprendre la finalité de l'attaque, son évolution et définir le mode de réponse. La cellule de pilotage devra donc être séparée des opérations les plus « terrains » pour garder ce recul nécessaire.

Attention également à la logique de diversion, souvent mise en oeuvre par les attaquants (attaque en déni de services, sur d'autres serveurs peu critiques…). Il est conseillé dans ce genre de situation de rester focalisé sur les cibles potentielles définies avec les métiers et vigilants pendant les périodes d'inactivité de l'organisation (HNO, week-end, jours fériés).

Une limite souvent rencontrée dans une telle crise est la mobilisation de trop nombreux acteurs décisionnels au regard d'un faible nombre d'acteurs opérationnels en capacité à réaliser les actions. La longue durée d'une attaque (pouvant s'étaler sur plusieurs mois) nécessite la mise en place d'un rythme de gestion différent d'une crise classique. Une organisation adaptée doit être mise en place dans la durée, en prévoyant des rotations des acteurs impliqués.

Disposer d'un SI de crise parallèle et indépendant

L'expérience montre que les attaquants réussissent souvent à prendre le contrôle de l'Active Directory ou encore de la messagerie. Ils sont alors en mesure « d'écouter » les décisions prises par la cellule de crise et de les anticiper. Pour réagir efficacement durant la crise, il est donc crucial de disposer de postes de travail durcis hors des domaines d'administration classique et d'un service de messagerie spécifique. L'utilisation de services Cloud est possible. Attention cependant, les attaquants ayant pu également compromettre les messageries personnelles de tout ou partie des collaborateurs…

Admettre la perte de confiance dans le SI et la regagner

La découverte d'une intrusion majeure a souvent pour conséquence une perte de confiance en son SI vu le nombre et la criticité des serveurs compromis. Pour reprendre le contrôle de ceux-ci, il est souvent nécessaire de reconstruire des socles sains, et en particulier de réinstaller complètement l'Active Directory. À partir de ces socles sains, il sera alors possible de recréer progressivement des zones de confiance en privilégiant les fonctions les plus sensibles de l'organisation.

Les investissements liés à ces plans de reconstruction peuvent être très lourds (nos retours d'expérience montrent qu'ils dépassent fréquemment la dizaine de millions d'euros) et l'attention ne doit en aucun cas être relâchée dans ces zones assainies pour éviter une nouvelle attaque. Il faudra alors mettre en place tous les processus nécessaires pour garantir leur sécurité (administration sécurisée, analyse des journées, filtrage réseaux, gestion des accès fins…).

À suivre …