WAVESTONE

ATTAQUES CIBLÉES
UNE REFONTE NÉCESSAIRE DE LA GESTION DE CRISE

La cybercriminalité ne cesse de croître. Les attaques se multiplient. Des entités gouvernementales, des géants du numérique, des leaders industriels… Tous les types d'entreprises et d'organisations sont susceptibles d'être victimes d'attaques informatiques ciblant directement les données et les sytèmes qui constituent le coeur de métier de l'organisation.

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 oeuvre ?

DE LA CYBERCRIMINALITÉ D'ESTIME AUX ATTAQUES CIBLÉES

Les motivations des attaquants ont fortement évolué ces dernières années. Les premières attaques étaient conduites par des personnes isolées dont l'objectif était de dépasser les défis techniques pour se faire une réputation. Désormais, les moteurs idéologiques et lucratifs sont à l'origine de la plupart des attaques observées : fuite ciblée d'informations sensibles (AshleyMadison…) ou dénis de services (attaques des groupes Anomymous ou Lulzsec comme celles qui ont impacté Sony et la plaforme de jeux de Microsoft…), vols de données personnelles et financières (JPMorgan Chase, Target…), attaque d'infrastructures et de données étatiques (Ministères des Finances, Office of Personal Management aux États-Unis…), attaques virales, *ransomwares*, etc.

AUTEURS


GÉRÔME BILLOIS
gerome.billois@wavestone.com

FRÉDÉRIC CHOLLET
frederic.chollet@wavestone.com

Trois grandes catégories d'attaques peuvent être distinguées.

La première concerne les **attaques diffuses**, elles sont sans cible précise ou visent le grand public (virus, *phishing*, *ransomware*...). Elles sont facilement contrées par les mécanismes de sécurité classique.

La deuxième représente les **attaques opportunistes**. D'un niveau technique plus avancé, elles vont viser les organismes les moins sécurisés dans un objectif de gain immédiat (vol de données personnelles, vols de données carte de crédit...). La mise en place et le maintien de dispositif de sécurité classique permet d'éviter une grande partie de ces attaques. Les personnes malveillantes cherchant un gain immédiat, elles changeront de cible en cas de difficultés à réussir l'attaque.

Une troisième catégorie, les **attaques ciblées**, connaît aujourd'hui un regain d'activité. La spécificité des attaques ciblées est de viser des informations ou les systèmes sensibles dans une organisation donnée. Ses auteurs sont mandatés pour viser une cible en particulier avec un objectif clair. Il s'agit en général de voler des données confidentielles, scénario sur lequel nous basons notre analyse. Des cas d'attaques destructrices ont également eu lieu mais en plus faible nombre.

Ils disposent de temps pour analyser l'organisation, préparent des scénarios d'attaques et utilisent tous les moyens à leur disposition, techniques comme humains, simples comme complexes, pour atteindre leur but.

Le niveau de technicité et les moyens disponibles peuvent s'élever drastiquement. La communauté sécurité évoque ainsi le terme « APT » ou « *Advanced Persistent Threat* » pour décrire ces menaces potentiellement avancées et persistantes. Ce sont ces attaques qui représentent aujourd'hui un réel défi, en particulier pour la gestion de la crise.

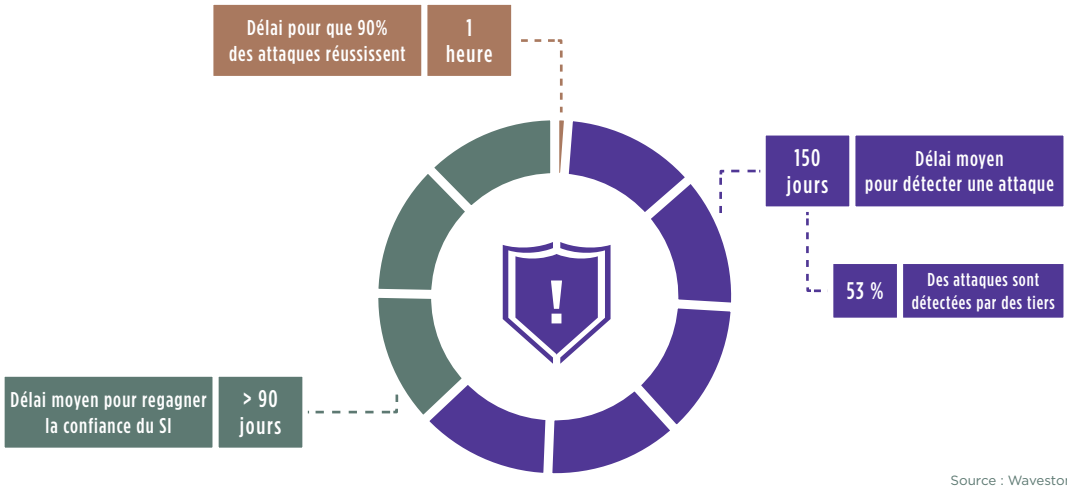
ATTAQUES CIBLÉES : UNE MENACE SILENCIEUSE AUX IMPACTS À RETARDEMENTS

Ces attaques ciblées mettent à mal les processus habituels de gestion de crise ou de gestion des incidents de sécurité pour plusieurs raisons :

- **Ces attaque sont silencieuses :** les attaquants utilisent des mécanismes d'attaques les plus discrets possibles afin de ne pas révéler leurs présence. Les données peuvent être exfiltrées avec des tunnels chiffrés ou les attaques avoir lieu en dehors des heures ouvrées. Les chiffres sont frappants : le délai moyen de détection d'une attaque est de 150 jours (Rapport M-trends 2016 de Mandiant).
- **Les attaquants sont efficaces et rapides :** ils sont organisés en équipes structurées avec des experts chargés d'accéder au SI et d'en garder le contrôle, des explorateurs pour rechercher les informations visées et de la « main d'oeuvre » pour exfiltrer des données. Cette organisation permet des attaques souvent bien plus rapides que les temps de réaction des grandes organisations. Le rapport Verizon de 2016 le montre clairement : 90 % des attaques réussissent en moins d'une heure, 67 % des exfiltrations ont lieu en moins d'une journée.
- **Les effets de ces attaques ne sont pas visibles :** le vol et l'exfiltration de données ne remet pas en cause le fonctionnement de l'entreprise au quotidien. Le SI continue à fonctionner correctement. En l'absence d'outils de surveillance avancée, la découverte d'une attaque est souvent fortuite – un coup de chance - ou alors liée au fait que les conséquences externes sont déjà perceptibles. Les chiffres vont dans ce sens : dans 53 % des cas, l'attaque ciblée est détectée par un tiers (rapport M-trends 2016 de Mandiant).
- **Ces attaques visent à conserver une position à long terme dans le SI :** au-delà de cette percée initiale au sein du SI, l'expérience montre qu'il existe chez l'attaquant une volonté de garder la main sur le SI à travers une compromission large des différents composants du SI à l'échelle de l'organisation. La prise de contrôle des systèmes centraux (en particulier l'*Active Directory*) est également très courante. Les éléments attaqués sont souvent compromis de multiples fois pour complexifier la remédiation.

Aujourd'hui, les grandes organisations disposent de processus de gestion des incidents

Le paradoxe des attaques ciblées : une échelle de temps différente entre la réalisation et la détection



Source : Wavestone, Mandiant, Verizon - 2016

à même de traiter des situations classiques (virus, *ransomware*, *phishing*, voir déni de service…). Souvent ces processus fonctionnent de manière unitaire : un incident entraîne une analyse et une résolution, sans forcément chercher à comprendre si l'incident ne fait pas partie d'une attaque plus large. La gestion de crise, quant à elle, est un dispositif avant tout managérial. Ces dispositifs sont conçus et mis en place pour adresser des événements « disruptifs » majeurs qui interrompent ou modifient le fonctionnement au quotidien de l'organisation. Ce qui n'est pas le cas pour les attaques ciblées !

Comment alors faire face à un sinistre discret, évolutif, n'impactant pas directement l'activité de l'entreprise mais compromettant la confidentialité des données et des systèmes d'information ?

REFONDRE LES PILIERS DE LA GESTION DE CRISE

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

En effet, si cette attaque a lieu c'est pour voler ou altérer des données et les systèmes 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 est essentiel

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 détection 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.

En complément, la sensibilisation des équipes SI à capter ces comportements suspects (dysfonctionnements partiels, augmentation de volume de stockage, de flux réseau…) et le développement de la capacité à automatiser l'analyse et la remédiation pour la plupart des incidents sont deux approches intéressantes. Ces relais peuvent être alimentés par les équipes d'investigation numériquettsur les éléments significatifs d'une attaque pour réaliser des analyses sur leur périmètre et détecter de potentielles compromissions.

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

> « Une attaque ciblée n'est pas une crise IT mais bien une crise métier : elle a pour objectif de voler des données métier »

à réaliser les actions. La longue durée d'une attaque (pouvant s'étaler sur plusieurs semaines, voire 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 d'une 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, 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 de sécurité nécessaires pour garantir leur sécurité (administration sécurisée, analyse des journées, filtrage réseaux, gestion des accès fins…).

Une stratégie à moyen terme basée sur l'anticipation

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, etc.) 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.

> « Il est nécessaire de refondre les processus de gestion de crise en intégrant les scénarios de cybercriminalité dans les procédures opérationnelles»

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.

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.

WAVESTONE

www.wavestone.com

Wavestone est un cabinet de conseil, issu du rapprochement de Solucom et des activités européennes de Kurt Salmon (hors consulting dans les secteurs retail & consumer goods). Il figure parmi les leaders indépendants du conseil en Europe.

La mission de Wavestone est d'éclairer et guider ses clients dans leurs décisions les plus stratégiques en s'appuyant sur une triple expertise fonctionnelle, sectorielle et technologique.