Livre blanc

Réponse aux incidents : dix erreurs courantes commises par les équipes

intel Security

Ce livre blanc a été rédigé par :
Michael G. Spohn
Expert-conseil
McAfee® Foundstone®
Professional Services
Réponse aux incidents et
investigations numériques

Sommaire

Introduction

Ma fonction d'enquêteur principal au sein de l'équipe d'investigation et de réponse aux incidents McAfee® Foundstone®, qui fait partie de l'offre de produits et services Intel® Security, m'a amené à traiter ma part d'incidents de sécurité. Ces derniers années, je me suis rendu dans plus de 100 entreprises pour les aider à remédier à de graves compromissions. Divers problèmes peuvent être à l'origine de ces missions : infestations par des logiciels malveillants courants, incidents dus à des fautes commises par des employés, et même compromissions de grande envergure par des groupes tels qu'Anonymous et LulzSec. La plupart des incidents entraînent une interruption totale ou partielle des activités, de même que le vol d'éléments de propriété intellectuelle, de secrets commerciaux, de données financières et/ou d'informations personnelles sensibles.

Chacune de ces missions a été riche d'enseignements. C'est l'aspect qui me passionne le plus dans les enquêtes liées à des compromissions de la sécurité. Avec le temps, j'ai commencé à distinguer certains types de comportement au sein des équipes de réponse aux incidents aux côtés desquelles je travaillais. Dans la plupart des cas, elles étaient incapables de faire face aux menaces de manière efficace et reproductible. Cela semble par ailleurs assez évident : sinon, elles n'auraient pas eu besoin de faire appel aux services d'une société comme la nôtre.

Dans ce livre blanc, je reviens brièvement sur les dix principales erreurs commises par les équipes de réponse aux incidents telles que je les ai constatées sur le terrain. En mettant en lumière ces problèmes, mon but est de vous permettre d'examiner vos pratiques de réponse aux incidents afin de déterminer si vous présentez les mêmes lacunes.

Scénario d'une mission

Lors d'une mission classique, un client nous demande d'intervenir sans délai afin d'endiguer une compromission de sécurité ; dans la plupart des cas, nous dépêchons un enquêteur sur place dans les 24 heures.

L'examen des pratiques efficaces de réponse aux incidents m'a permis de dresser une série de constats :

- La taille de l'entreprise n'est pas pertinente. Les grandes entreprises ont parfois besoin de plus de temps pour contenir un incident, mais le processus reste le même.
- Le secteur d'activité n'est pas pertinent. La manière dont est prise en charge une compromission de sécurité ne dépend pas de l'activité exercée par le client. Bien sûr, certains problèmes réglementaires et de confidentialité sont propres à certains secteurs, mais nous traitons tous les incidents en appliquant les critères les plus stricts. Et vous devriez faire de même.
- Les compétences des clients en matière de gestion des crises varient. Ainsi, les organismes publics nationaux disposent généralement de capacités de gestion des crises plus développées que des cabinets d'avocats de moyenne envergure. Néanmoins, je me suis rendu compte que la différence n'était pas suffisamment importante pour peser réellement dans la balance.
- Les compétences techniques des clients varient. Ce point fait une énorme différence. Les clients qui possèdent des compétences techniques pointues, en particulier en gestion du réseau, contiennent généralement les incidents de sécurité de manière plus efficace.
- Mises sous pression, toutes les entreprises affichent un type de comportement similaire.

Cette liste vise à vous convaincre de l'intérêt d'adopter une approche évoluée et disciplinée de la réponse aux incidents au sein de votre entreprise.

Les dix principales erreurs

1. Absence de responsable
Je ne soulignerai jamais assez l'importance de désigner un responsable de la gestion des opérations de réponse aux incidents. Ces dix dernières années, les entreprises ont choisi de décentraliser davantage les structures de gestion. Les structures hiérarchiques sont souples. Les frontières géographiques se sont évanouies.

Le gestionnaire des incidents désigné assume la responsabilité ultime de l'endiguement d'un incident. Je suis parfois invité à endosser cette fonction, mais je préfère qu'elle soit confiée à un membre du personnel interne, idéalement un cadre ou un directeur. Il est rare que les cadres dirigeants assument cette fonction. La personne désignée ne doit pas faire montre de compétences techniques pointues ; le sens de la communication, de l'organisation et de la délégation sont des qualités bien plus importantes.

2. Incapacité à mettre en place un centre de commandement
Les entreprises essaient souvent de résoudre de graves incidents par le biais de téléconférences, d'appels téléphoniques ou d'e-mails. Croyez-moi, ce type d'approche ne donne pas de résultats. Il est primordial de mettre en place un centre de commandement dans une salle de conférence ou un bureau unique.

L'endroit choisi doit être suffisamment spacieux pour accueillir une dizaine de personnes. Il doit par ailleurs disposer de grands tableaux blancs ou de chevalets à feuilles mobiles et d'un téléphone de conférence/mains libres et être sécurisable. L'accès au centre de commandement doit être limité aux seules personnes responsables de la gestion de l'incident. Le centre servira de plate-forme centrale pour toutes les communications, la planification de l'endiguement de l'incident, la délégation des tâches et les rapports sur l'état d'avancement.

3. Incapacité à repérer et à identifier l'ennemi
À la question de savoir quels aspects de nos services de réponse d'urgence aux incidents ils apprécient le plus, les clients citent généralement les compétences en gestion des crises et la gestion des menaces. Cette dernière nécessite de pouvoir identifier la source d'une menace et de comprendre son mode opératoire, autrement dit d'« identifier l'ennemi ». Bien que cette tâche ne soit pas particulièrement complexe, la plupart des clients éprouvent des difficultés à cet égard.

L'« ennemi » varie selon le type d'incident. L'important est d'identifier la menace et de bien comprendre son fonctionnement. Par exemple, dans le cas d'une attaque de logiciel malveillant sérieuse, notre processus de localisation et d'identification de l'ennemi comprend les étapes suivantes :

- Identification du vecteur d'attaque
- Investigation numérique en direct
- Isolement des hôtes et collecte d'échantillons
- Profilage du logiciel malveillant et identification du mode de communication utilisé
- Soumission d'échantillons du logiciel malveillant au fournisseur de solutions antivirus
- Exploitation des outils antivirus de l'entreprise

Croyez-moi : une parfaite connaissance de l'ennemi est indispensable pour mettre en place une stratégie d'endiguement efficace.

4. Incapacité à élaborer un plan d'endiguement
Lorsque j'arrive sur site à la suite d'un incident majeur, je suis toujours surpris par le chaos ambiant. La plupart des entreprises ne disposent d'aucun plan de gestion des crises éprouvé et documenté. Nous devons donc en élaborer un à leur place. Dans les quatre heures suivant le début de mon intervention pour une compromission de sécurité, je produis généralement un document concis (une à deux pages) pour l'endiguement de l'incident. Ce plan d'endiguement constitue un élément essentiel de la méthodologie de réponse aux incidents de McAfee Foundstone. Nous n'y dérogeons pas.

En bref, cette méthodologie repose sur les étapes suivantes :

- Détermination du vecteur d'attaque et de l'ampleur de l'incident
- Identification de l'ennemi, de ses outils et de ses tactiques
- Élaboration et documentation d'une stratégie d'endiguement en collaboration avec l'entreprise
- Création d'une liste de tâches sur la base du plan d'endiguement
- Délégation et surveillance des tâches jusqu'à la mise sous contrôle

5. Incapacité à documenter l'incident
Je dois l'admettre : je suis de la vieille école et je continue d'utiliser des calepins lors de mes enquêtes. Les temps ont changé. Les jeunes générations n'ont jamais connu un monde dépourvu d'électronique. Les SMS et les e-mails ont donné un nouveau sens à la documentation. Par conséquent, bon nombre de responsables de la réponse aux incidents ont perdu de vue l'importance d'une bonne documentation.

Vous ne pouvez pas compter sur le système de gestion des tickets de votre service d'assistance pour documenter les incidents. Nous encourageons tous les membres des équipes de réponse aux incidents à avoir en permanence un carnet de notes sur eux afin d'y consigner leurs actions. Il convient de documenter l'ensemble des événements et des tâches déléguées, et d'en conserver la trace dans un emplacement centralisé et sécurisé.

6. Incapacité à établir la chronologie de l'incident
L'établissement de la chronologie de l'incident constitue à mes yeux une des tâches les plus importantes de la mise sous contrôle d'un incident. Cela signifie essentiellement que vous devez documenter les événements et les trier par ordre chronologique, du plus ancien au plus récent. Votre liste ne doit pas être sophistiquées : juste complète et précise.

Une chronologie détaillée de l'incident vous guidera tout au long de votre enquête, ainsi que lors de l'élaboration de votre stratégie d'endiguement. Elle apporte en outre un éclairage supplémentaire aux enquêtes complexes et vous permet d'envisager le problème dans son ensemble. Enfin, elle constitue un formidable outil de briefing pour les dirigeants.

7. Confusion entre endiguement et correction
Lors de la réponse à un incident, les entreprises commettent très souvent l'erreur de confondre endiguement et correction. Pour réussir, vous devez commencer par vous concentrer sur l'endiguement. Les efforts de correction viendront plus tard. Pourquoi ? Parce que l'endiguement a simplement pour but de bloquer la menace, tandis que la correction vise à remédier aux vulnérabilités. Si l'on établit un parallèle entre la réponse aux incidents et un bâtiment en feu, il est clair que, dans un premier temps, vous concentrerez tous vos efforts sur l'extinction de l'incendie. La réparation du toit viendra plus tard.

La réponse aux incidents consiste en un processus d'endiguement, de mise sous contrôle. Il est essentiel que tous les membres de l'équipe de réponse aux incidents comprennent l'importance de d'abord se concentrer sur l'endiguement. Toute tâche non essentielle à cette fin doit être remise à plus tard.

8. Incapacité à surveiller et à sécuriser le périmètre réseau
Je suis stupéfait par le nombre d'entreprises qui n'utilisent pas de technologies de surveillance du réseau. Si vous ignorez quel type de trafic circule sur vos réseaux, vous serez dans l'impossibilité de vous protéger contre les menaces réseau. Je ne soulignerai jamais assez l'importance de sécuriser le périmètre réseau et de surveiller le trafic réseau sortant.

Pourquoi le trafic sortant ? Parce que vos ennemis doivent faire sortir vos données sensibles de votre réseau pour le transférer vers le leur. Lors d'un incident avec compromission de la sécurité, nous commençons toujours par sécuriser le périmètre réseau avant d'examiner les éléments internes. La protection du périmètre permet d'empêcher l'ennemi de communiquer. Une fois le périmètre sécurisé, vous pouvez vous déplacer vers l'intérieur afin d'identifier et de détruire les outils utilisés par les pirates.

9. Journalisation inadéquate
En bref, la grande majorité des entreprises qui font appel à nos services n'ont pas mis en place de mécanismes de journalisation adéquats. Pour une raison qui m'échappe, cette opposition à la mise en place d'une journalisation efficace demeure très vive. Les mentalités doivent changer. Les journaux constituent la source d'informations la plus efficace dans la plupart des incidents. D'après mon expérience, les journaux les plus précieux sont ceux du périmètre réseau.

Pour pouvoir intervenir de manière efficace, les équipes de réponse aux incidents doivent avoir rapidement accès aux fichiers journaux, notamment :

- Journaux syslog et autres journaux centralisés
- Journaux des pare-feux et des systèmes IDS/IPS
- Journaux des proxys web
- Journaux d'événements Microsoft Windows
- Journaux VPN
- Journaux DHCP
- Journaux DNS
- Journaux Microsoft Active Directory
- Journaux AD d'entreprise

10. Systèmes antivirus d'entreprise orphelins
Une telle erreur a de quoi étonner. Nombreux sont ceux qui pensent au sein des experts en sécurité que les systèmes antivirus d'entreprise modernes sont devenus inefficaces face aux menaces sophistiquées et polymorphes d'aujourd'hui. Force est d'admettre que nous sommes en train de perdre la bataille sur ce front. Il n'empêche que le système antivirus de votre entreprise demeure un outil essentiel de votre arsenal de défense. En fait, dans la plupart des incidents dus à des logiciels malveillants ou à des menaces APT auxquels j'ai été confronté ces quatre dernières années, un système antivirus d'entreprise a été utilisé pour contrer la menace.

Les entreprises qui n'exploitent pas leurs outils antivirus se mettent en danger. Plusieurs erreurs sont couramment commises dans ce domaine :

- Incapacité à surveiller et/ou à garantir la conformité des antivirus
- Agents obsolètes
- Fichiers de signatures (.DAT) obsolètes
- Incapacité à assurer la supervision au quotidien des systèmes antivirus
- Incapacité à créer des alertes d'événement automatisées
- Incapacité à surveiller les alertes des fournisseurs de solutions antivirus

Résumé

Nous voici arrivé au terme de notre tour d'horizon des dix principales erreurs commises par les équipes de réponse aux incidents. Comme vous pouvez le constater, aucune de ces erreurs n'est réellement difficile à corriger. En fait, votre entreprise pourrait utiliser cette liste pour évaluer l'efficacité de vos pratiques actuelles en matière de réponse aux incidents. Chez McAfee Foundstone, la sécurité informatique est une vraie religion. Nous nous efforçons d'aider les entreprises à améliorer leur niveau de protection. La meilleure approche consiste à adopter une attitude proactive. Assurez-vous donc que vos plans de réponse aux incidents sont à jour et efficaces.

L'auteur

Expert-conseil en sécurité chez McAfee Foundstone, Michael Spohn propose aux clients des services de réponse aux incidents et d'investigation numérique. Ses tâches comprennent notamment la création de programmes de gestion de la réponse aux incidents, les analyses et tests des plans de réponse aux incidents existants et l'exécution d'investigations numériques. Il assure également des formations en investigation numérique et en réponse aux incidents. Il est par ailleurs membre de l'équipe Emergency Incident Response de McAfee Foundstone, qui intervient en urgence chez les clients en cas de compromission grave de la sécurité.

À propos de McAfee Foundstone Professional Services

McAfee Foundstone Professional Services est une division de McAfee, qui fait partie d'Intel Security. Elle propose des services et des formations assurés par des experts dans le but d'aider les entreprises à protéger, de façon continue et mesurable, leurs actifs les plus importants contre les menaces les plus critiques. Par une approche stratégique de la sécurité, McAfee Foundstone identifie et implémente, suivant un équilibre optimal, les technologies, le personnel et les processus requis pour gérer les risques numériques et optimiser les investissements en sécurité. L'équipe Professional Services se compose d'auteurs et d'experts reconnus en matière de sécurité informatique, qui bénéficient d'une vaste expérience glanée tant auprès de grandes entreprises multinationales que dans le secteur public ou les forcées armées. **http://www.mcafee.com/fr/services/mcafee-foundstone-practice.aspx**

À propos d'Intel Security

McAfee fait désormais partie d'Intel Security. Avec sa stratégie Security Connected, son approche innovante de la sécurité optimisée par le matériel et son réseau mondial de renseignements sur les menaces Global Threat Intelligence, Intel Security consacre tous ses efforts à développer des solutions et des services de sécurité proactifs et éprouvés, qui assurent la protection des systèmes, des réseaux et des équipements mobiles des entreprises et des particuliers du monde entier. Intel Security allie l'expérience et les compétences de McAfee avec les innovations et les performances reconnues d'Intel pour faire de la sécurité un élément essentiel de toute architecture et de toute plate-forme informatique. La mission d'Intel Security est de permettre à chacun de vivre et de travailler en toute confiance et en toute sécurité dans le monde numérique. **www.intelsecurity.com**.

McAfee. Part of Intel Security.
Tour Franklin, La Défense 8
92042 Paris La Défense Cedex
France
+33 1 47 62 56 00 (standard)
www.intelsecurity.com