IBM Global Technology Services
Services de sécurité

Créer un plan de réponse performant aux incidents de sécurité

Coup d'œil sur les 10 erreurs principales d'un plan de réponse aux incidents de sécurité informatiques (CSIRP)

Points clés :

- Les failles de sécurité sont pratiquement inévitables : elles peuvent inclure des milliers d'enregistrements de données et coûter des millions de dollars.
- La mise en place d'un plan de réponse aux incidents de sécurité informatiques, ou CSIRP, peut aider à réduire les coûts et minimiser la gravité des failles.
- Fort de sa collaboration avec des centaines d'entreprises de toutes tailles, IBM prodigue des conseils pour élaborer et maintenir un CSIRP efficace.

Comprendre les coûts élevés découlant des failles de sécurité

Les multinationales comptant des centaines de milliers d'employés, les petites sociétés exerçant dans le domaine du Web ou les organismes du secteur public de toutes tailles ont tous un point commun : leurs réseaux sont la cible constante d'attaques et leurs systèmes d'information encourent également des risques. En outre, pratiquement toutes les entreprises ont eu une faille de sécurité à un moment donné.[1]

L'impact de cette faille dépend de nombreux facteurs, notamment de votre degré de préparation face à cette situation. D'après le Ponemon Institute, pour réduire les coûts entraînés par une violation des données, l'existence d'un plan de réponse aux incidents de sécurité informatiques (CSIRP) vient en deuxième place après un dispositif de sécurité solide.[2]

Le CSIRP est la pierre angulaire de votre défense face aux pirates informatiques, aux programmes malveillants, aux erreurs humaines et autres menaces. C'est l'itinéraire à suivre pour réagir face à une attaque réussie. Ce plan doit définir les rôles et responsabilités de tous les intervenants, établir l'autorité pour la prise de décisions importantes et définir les flux de communication et les procédures de notification. Sans CSIRP, votre équipe de réponse aux incidents peut gaspiller un temps précieux et des ressources importantes à essayer de déterminer comment réagir, ce qui peut entraîner potentiellement des coûts plus élevés et des dommages plus importants pour votre entreprise et pour votre réputation.

Élaborer un plan efficace de réponse aux incidents

Même si les composants de base d'un CSIRP sont simples, il est nécessaire d'atteindre un bon équilibre entre précision et fonctionnalité pour créer un plan efficace. Étant donné que les menaces évoluent rapidement, il est impossible d'établir un plan qui répond à chaque attaque potentielle. D'ailleurs, vous ne souhaiteriez sans doute pas avoir un document aussi détaillé et aussi complexe. Vous préfèreriez plutôt élaborer des directives flexibles pouvant s'appliquer rapidement et facilement à tout type d'incident.

Le pire moment pour vous rendre compte que votre CSIRP présente des défauts est lorsque vous vous trouvez au cœur d'une urgence. En aidant les clients à réagir à des incidents déclarés, les experts IBM en sécurité qui font partie des équipes de services de réponse d'urgence ont pu observer ce qui fonctionne et ce qui ne fonctionne pas dans un CSIRP. Dans le présent document, nous allons vous indiquer les 10 défauts les plus communs que nous ayons rencontrés dans un CSIRP et vous donner des astuces pour éviter ces erreurs potentiellement coûteuses.

1 Établir un CSIRP trop complexe

Lorsque vous rédigez votre CSIRP, gardez en tête que les personnes qui liront le document seront en situation de crise. Il y aura du stress, de la confusion, et bien entendu, de l'urgence. Certaines personnes seront paniquées et se feront du souci pour leur emploi. Les cadres, qui comprendront ou non les points techniques de la situation, seront stressés si les médias leur posent des questions.

Aussi, un CSIRP doit être précis, clair et concis. Si un employé qui ne connaît pas le document ne peut pas prendre connaissance rapidement des processus décrits, comprendre la chaîne de commandes et réaliser les actions nécessaires, votre CSIRP est sans doute trop complexe. Bien entendu, il ne faut pas non plus tomber dans le piège de faire un CSIRP trop simple. Réussir à trouver le bon équilibre entre concision et directives concrètes est essentiel pour que le CSIRP soit efficace.

L'existence d'un plan de réponse aux incidents a fait économiser en moyenne 1,2 million de dollars par violation de données pour les entreprises américaines en 2013.[3]

2 Surcharger le personnel clé

Chaque organisation dispose d'un homme à tout faire. Cet homme connaît tout le monde ainsi que tous les systèmes, routeurs, câbles et machines à café du bâtiment. C'est lui que nous courons chercher lors d'un incident. C'est lui, indubitablement, qui est le plus qualifié pour s'occuper des incidents mineurs et les traiter du début à la fin. Lorsque nous préparons un CSIRP pour nos clients, nous identifions rapidement cet homme à tout faire au sein de notre organisation lorsque nous nous posons les questions standard : Qui s'occupe de l'antivirus ? C'est lui. Qui décide de la réponse technique à adopter ? C'est lui. Qui communique avec les cadres et les autorités réglementaires ? C'est lui.

Cet homme excelle dans les tâches qu'il accomplit lors d'une journée de travail normale. Néanmoins, lorsqu'un incident s'étend sur plusieurs plages horaires, voire plusieurs jours, cet homme ne peut pas être à nos côtés pendant 72 heures d'affilée. Il est donc nécessaire qu'une organisation segmente les tâches lors d'un incident et les distribue à un personnel formé identifié pour ne pas surcharger une équipe qui ne dormira plus pour répondre aux incidents et qui sera, par conséquent, moins efficace.

3 Considérer la réponse aux incidents comme un processus en série

Lorsqu'un incident de grande envergure se produit, la polyvalence est essentielle. Les responsables qui considèrent la réponse aux incidents comme un processus en série sont condamnés à l'échec lorsqu'ils doivent résoudre un incident de façon précise. Étant donné que chaque incident est unique, chaque réponse à un incident implique un certain nombre d'efforts à court terme. Publication de nouvelles signatures antivirus, application de correctifs sur les systèmes, approfondissement des analyses, indication du statut d'avancement aux employés et aux clients, approvisionnement supplémentaire en boissons caféinées et autres tâches importantes : il s'agit là de processus individuels qui doivent être traités en tant que tels. Une erreur commune consiste à ne se consacrer qu'à une seule de ces tâches à la fois et de négliger d'autres tâches importantes devant être réalisées en parallèle.

4 Échouer à mettre en place des lignes de communication appropriées

Pour répondre à un incident, différentes personnes et différents fournisseurs seront potentiellement sollicités. Le responsable de la gestion des « troupes », autrement dit le gestionnaire en cas d'incident, doit exceller en matière de communication. La communication doit être méthodique, efficace et suivre les canaux appropriés pour veiller à ce que tous les intervenants aient l'ensemble des informations utiles et soient bien coordonnés. Au sein d'une entreprise, le processus de réponse peut impliquer les équipes techniques, mais également les équipes en charge de la sécurité physique, des ressources humaines, de la conformité, des affaires réglementaires et de la gestion des risques. Les communications externes sont également essentielles : il est donc impératif qu'une personne soit clairement désignée pour fournir des mises à jour opportunes et factuelles aux relations publiques de votre entreprise, aux médias, aux équipes de services à la clientèle ainsi qu'aux points de contact marketing. En échouant à communiquer rapidement et ouvertement sur les incidents de sécurité, de nombreuses organisations ont entamé la confiance que les parties prenantes avaient placé en elles.

5 Mettre l'accent sur les tâches faciles, et pas sur celles à réaliser

Dans la plus part des cas, pour chaque incident, nous avons tendance à privilégier les tâches faciles à exécuter, au lieu de celles devant être réalisées. Pour prendre un exemple, c'est comme si nous remplissions le réservoir de liquide lave-glaces de notre voiture alors que c'est le moteur qui ne démarre pas. Lors de la résolution d'un incident, il est tentant de se consacrer en grande partie à des tâches faciles, comme la collecte de preuves statiques (ex. capture d'images du disque dur), plutôt qu'à des tâches plus complexes (ex. l'exécution d'une analyse). Toutefois, quelle que soit leur difficulté, toutes les tâches doivent être réalisées. Si vous ne parvenez pas à canaliser votre énergie sur les problèmes essentiels, qu'ils soient simples ou complexes, vous en retirerez uniquement des maux de tête plus conséquents et des incidents prolongés.

Au moins 50 pour cent des CSIRP évalués par les consultants en sécurité IBM *ne présentaient ni cycle de vie formel ni historique de révisions.*

6 Privilégier les centres d'intérêt, et non les tâches à réaliser

Lors de certains incidents, le personnel peut découvrir des informations intéressantes et se lancer par la suite à la chasse de ces informations en suivant une voie n'ayant aucun rapport avec la situation. Le personnel se laisse facilement distraire par la découverte d'une activité utilisateur inappropriée, par exemple, la navigation sur des sites « interdits d'accès ». Cette découverte peut être extrêmement captivante, mais si elle ne joue pas de rôle crucial dans l'incident sur lequel vous travaillez, elle doit être mise de côté pour de futures recherches. Vous pouvez passer un nombre d'heures incalculable sur cette piste, et de fait, prendre du temps que vous ne pouvez pas vous permettre de gaspiller. Restez concentré sur la résolution de l'incident et gardez cette piste pour plus tard.

Conseils de la part d'IBM à l'attention des premiers intervenants

Lorsqu'un incident de sécurité se déclare, gardez bien en tête ces tâches « à faire » et « à ne pas faire ».

À FAIRE :

- Consulter le CSIRP de votre entreprise et le mettre en application
- Collecter des informations sur l'incident à partir de plusieurs sources
- Veiller à ce que le personnel qualifié soit impliqué
- Commencer à prendre des notes précises
- Activer les données d'identification uniques de l'intervenant
- Recueillir des données volatiles et des fichiers logs pré-déterminés
- Conserver les systèmes et les supports pour les investigations judiciaires
- Collecter des logs réseau aux fins d'analyse ultérieure

À NE PAS FAIRE :

- Paniquer ou réagir sans avoir de plan
- Discuter de l'incident avec d'autres personnes, sauf s'il en a été convenu ainsi
- Éteindre, mettre hors tension ou sauvegarder les systèmes touchés
- Accéder à distance aux systèmes, sauf si nécessaire
- Utiliser des données d'identification communes à un domaine privilégié
- Installer ou exécuter un logiciel quel qu'il soit sur les systèmes
- Effectuer une analyse antivirus ou similaire
- Tenter de riposter contre les coupables

---

7 Abandonner le CSIRP

Vous aurez parfois envie de mettre le CSIRP au rebut s'il ne convient pas à la situation spécifique que vous rencontrez. Pourtant, il existe une raison pour laquelle le document n'aborde pas le dernier virus de messagerie ou le dernier cheval de Troie. C'est parce que le CSIRP n'a pas vocation à être un guide complet sur les méthodes permettant de traiter chaque type spécifique d'incident. Il s'agit plutôt d'un plan directeur pour établir les grandes lignes de communication, les rôles, les notifications obligatoires et les mesures à prendre pour remédier à une faille de sécurité.

Même si chaque incident a sa propre spécificité, un CSIRP flexible et bien construit permettra de formuler rapidement une réponse en identifiant le personnel clé devant intervenir, son rôle et vos protocoles de communication. En ayant cette structure en place, les mesures nécessaires pourront alors être prises pour contrer la technologie à l'origine de l'incident.

8 Rédiger une politique, et non un plan

Gardez toujours en tête que le « P » dans CSIRP signifie « Plan » et non « Politique ». Il arrive qu'IBM révise des CSIRP tenant plus de la politique que du plan. Quelle est la différence ? Un plan comprend des mesures et des rôles concrets, tandis qu'une politique énonce des directives générales à appliquer au sein de l'organisation. Lorsqu'un incident se produit, avez-vous vraiment envie de lire la politique de l'entreprise pour établir un plan ? Non, bien évidemment. Vous souhaitez vous appuyer sur un plan bien pensé vous indiquant comment procéder.

9 Ne pas affecter de propriétaire et ne pas mettre le plan à jour

Le CSIRP est à l'image d'un jardin. Tous deux demandent du temps pour se développer, nécessitent entretien et attention et requièrent la présence d'un propriétaire pour leur bien-être. Lorsque vous rédigez un CSIRP, vous devez y affecter un propriétaire, c'est-à-dire une personne désignée, et non pas un service ou une fonction, qui sera chargée de gérer le document, en veillant à ce que le personnel et les procédures qu'il contient soient toujours appropriés, et d'organiser un test annuel.

Sans propriétaire spécifique, le document ne sera pas maintenu à jour et ne connaîtra pas d'évolution. Il risque même d'augmenter le temps de réponse aux incidents. Par ailleurs, pour que le propriétaire soit efficace, il doit avoir le soutien de la direction dans l'exercice de son rôle ou avoir un poste suffisamment élevé pour allouer des ressources au test et à la mise à jour.

Un CSIRP doit être mis à jour régulièrement, au moins deux fois par an, ainsi qu'après tout événement majeur, par exemple, une fusion ou une acquisition, un changement important d'infrastructure ou de personnel, ou encore un incident de cyber-sécurité. Dans le cadre de notre collaboration avec les clients, nous avons constaté que les CSIRP étaient mis à jour en moyenne tous les 18 à 24 mois, même si, d'expérience, il est courant de voir des CSIRP n'ayant pas eu de mise à jour en cinq ans. En cas d'incident, ce document obsolète sera ressorti, époussetté, et l'équipe de réponse se rendra vite compte que le personnel clé nommé dans le plan ne fait plus partie de l'entreprise ou a changé de fonction, ce qui aboutira malheureusement sur une réponse trop tardive avec des conséquences potentiellement importantes.

10 Ignorer le processus de clôture de l'incident

Les enseignements les plus utiles que l'on puisse tirer d'un incident ressortent lors de la révision après résolution. Avant qu'un incident ne soit officiellement clôturé, une bonne pratique consiste à organiser une réunion de clôture au cours de laquelle vous pouvez évaluer l'efficacité du CSIRP (de son fonctionnement) et documenter l'origine de l'incident et autres conclusions.

Même si tout semble s'être déroulé comme prévu lors d'un incident, il apparaît qu'une révision après résolution mettra tout de même en lumière des améliorations potentielles. En identifiant des erreurs ou des problématiques à modifier, vous renforcerez votre CSIRP et sa capacité à répondre à vos besoins lors de futurs incidents. Même si votre équipe de réponse est impatiente de tourner le dos au passé et revenir à des opérations normales, cette étape finale ne doit pas être négligée. Elle représente parfois la partie la plus importante du processus de réponse aux incidents.

IBM Global Technology Services
Services de sécurité

Évaluer votre CSIRP

Votre organisation dispose-t-elle d'un plan de réponse aux incidents de sécurité informatiques officiel et documenté ? Si oui, quand votre CSIRP a-t-il été mis à jour pour la dernière fois ? Si vos réponses ne sont pas « oui » et « au cours des six derniers mois », il vous serait sans doute profitable de parler avec un expert en sécurité informatique extérieur à votre entreprise.

Chez IBM, nous aidons les clients à évaluer et à améliorer un CSIRP existant ou à en élaborer un de toutes pièces. Vous pouvez commencer par faire une évaluation de haut niveau moyennant un investissement modeste, puis, selon nos conclusions et recommandations, décider de la marche à suivre. Cette tâche est réalisée par les experts en sécurité de l'équipe de service de réponse d'urgence IBM qui travaillent main dans la main avec les clients dans le cadre d'engagements de réponse aux incidents réels. Nos meilleures pratiques de CSIRP se basent sur les normes du secteur, telles que NIST (National Institute of Standards and Technology), ISACA (Information Systems Audit and Control Association), IETF (Internet Engineering Task Force) et ISO (International Organization for Standardization).

Pour toute urgence, appelez le 1-888-241-9812.

Le service de réponse d'urgence (ERS) IBM est assuré 24h/24, 7j/7, 365j/an par des équipes de réponse aux incidents et des experts en fraudes informatiques, prêts à répondre globalement aux incidents de sécurité. Les équipes ERS sont qualifiées pour répondre aux menaces de nos clients, entre autres, les programmes malveillants type « zero day », les intrusions sur le réseau et autres menaces de sécurité avancées.

Si vous être confronté à un problème grave et que vous avez besoin d'une assistance immédiate, veuillez contacter la hotline ERS aux numéros suivants : 1-888-241-9812 ou +001-312-212-8034

Pour en savoir plus

Pour en savoir plus sur l'aide qu'IBM peut vous apporter pour protéger votre organisation des cyber-attaques et pour renforcer votre sécurité informatique, contactez votre représentant ou votre partenaire commercial IBM, ou rendez-vous sur le site Web :
ibm.com/services/security

Pour en savoir plus sur les épidémies de violations de données et les mesures à prendre pour éviter les incidents ou y répondre, rendez-vous sur le site Web suivant :
ibm.com/services/us/en/it-services/data-breach/index.html

Suivez-nous sur :

IBM France
17 avenue de l'Europe
92275 Bois Colombes Cedex

Produit en France
Juin 2015

[1] IBM, *IBM Security Services Cyber Security Intelligence Index*, Juin 2013.

[2,3] Ponemon Institute, étude 2013 sur les coûts des violations de données : analyse globale, enquête de référence sponsorisée par Symantec et conduite de façon indépendante par Ponemon Institute, Mai 2013.

Recyclable

SEE03005-FRFR-0