kaspersky

Votre guide de mise en place d'un plan de réponse aux incidents de cybersécurité

kaspersky

Sommaire

1. **Qu'est-ce qu'un plan de réponse aux incidents de cybersécurité ?**
2. **Le coût d'une violation de données**
3. **Pourquoi avez-vous besoin d'un plan de réponse aux incidents de cybersécurité ?**
4. **6 phases d'un plan de réponse aux incidents de cybersécurité**
5. **Création d'une équipe de réponse aux incidents**
6. **Exercices de formation à la cybersécurité**
7. **Pratiques exemplaires relatives au plan de réponse aux incidents de cybersécurité**
8. **Exemples et modèles**
9. **Comment Kaspersky peut vous aider**

Chiffres importants

Selon un sondage réalisé en 2021 par VMware en partenariat avec Kroll, Red Canary et Wakefield Research, la grande majorité (93 %) des entreprises ont été confrontées à un incident de cybersécurité au cours des 12 derniers mois, tandis que 49 % seulement ont déclaré se sentir équipées (sur le plan des outils, du personnel et de l'expertise) pour détecter les cybermenaces ou y répondre[1].

Qu'est-ce qu'un plan de réponse aux incidents de cybersécurité ?

Un plan de réponse aux incidents de cybersécurité est un document qui vous indique, ainsi qu'à votre personnel, les mesures à prendre en cas d'incident de sécurité, comme une violation des données, une attaque par ransomwares, une interruption de service ou la perte d'informations confidentielles. Le plan de réponse aux incidents comporte plusieurs étapes, dont l'identification des incidents, la reconnaissance de leur priorité, leur maîtrise et leur élimination, le rétablissement ainsi que la prise de mesures pour prévenir de futurs incidents. Le plan comprend également les rôles et les responsabilités (c'est-à-dire qui, dans votre entreprise, fait quoi en cas d'incident de sécurité) et les plans de communication. Nous aborderons chacun de ces éléments dans ce guide.

Le National Institute of Standards and Technology (NIST) propose un guide complet pour mettre en place un plan de réponse aux incidents de cybersécurité, que vous pouvez trouver ici. Il est assez long et détaillé, c'est pourquoi nous en avons extrait les points essentiels pour vous ici !

[1] https://www.vmware.com/content/dam/digitalmarketing/vmware/en/pdf/docs/vmwcb-report-the-state-of-incident-response-2021.pdf

Le coût d'une violation de la sécurité

Aucune entreprise qui stocke ou traite des données confidentielles n'est trop petite ou assez sécurisée pour éviter une violation de la sécurité, quelle que soit l'industrie.

- Selon l'étude 2020 Cost of Cyber Crime du Ponemon Institute, une organisation typique est confrontée à 130 incidents de sécurité par an[2]
- Selon la dernière version de l'Almanach de la cybersécurité 2022 de Cisco/Cybersecurity Ventures[3], le coût de la cybercriminalité devrait atteindre 10 500 milliards de dollars d'ici 2025.
- Selon le rapport annuel Cost of Data Breach Report 2021 d'IBM, le coût moyen d'une violation des données a atteint un record depuis la création du rapport il y a 17 ans, avec 4,37 millions de dollars[4].
- Le même rapport indique que le coût moyen des violations dans lesquelles le travail à distance a joué un rôle était de 1,07 million de dollars plus élevé (par rapport aux violations n'impliquant pas de travail à distance), ce qui signifie que la tendance à adopter des modes de télétravail à la suite de la pandémie de COVID-19 a largement contribué à l'augmentation du coût des violations de données.
- Un autre sondage réalisé par le Ponemon Institute a révélé que 77 % des entreprises en 2019 ne disposaient d'aucun plan de réponse aux incidents de sécurité[5], ce qui les laissait largement exposées à une coûteuse violation de la sécurité.

Des actes, pas que des paroles

En 2015, l'entreprise de télécommunications TalkTalk a été condamnée à une amende record de 400 000 £ par l'Information Commissioner's Office (ICO) à la suite d'une violation importante des données de ses clients. Cette amende aurait pu atteindre 60 millions de livres si la sanction maximale avait été appliquée. L'enquête de l'ICO[6] a révélé que la violation aurait pu être évitée si certaines mesures simples avaient été prises, comme la mise à jour régulière des systèmes et la surveillance proactive des menaces – autant d'éléments de base d'un bon plan de réponse aux incidents. Si l'entreprise avait mis en place un plan de réponse efficace aux incidents de cybersécurité et si son personnel y avait été formé, des coûts énormes et des atteintes à la réputation auraient pu être évités.

Le facteur humain

Les cyberattaques entraînent également un coût humain. Par exemple, le sondage Kaspersky Global Corporate IT Security Risks Survey (ITSRS) 2019 a révélé que 33 % des employés se sentaient beaucoup plus stressés au travail à la suite d'une violation des données, tandis que 30 % ont dû manquer un événement familial important ou un rendez-vous personnel parce qu'ils travaillaient tard à la suite d'une violation des données. Lisez l'intégralité du sondage ici.

Un problème dans le pipeline

La cyberattaque de mai 2021 contre l'oléoduc Colonial Pipeline, qui transporte du pétrole à travers les États-Unis, est un autre exemple du type de dangers auxquels les entreprises sont confrontées de nos jours. L'entreprise a payé une rançon de 4,4 millions de dollars pour remettre ses systèmes en service, tout simplement parce que les identifiants de connexion des utilisateurs n'avaient pas été mis à jour ni renforcés[7] (ce qui fait partie intégrante d'un plan de réponse aux incidents de cybersécurité). À la suite de cette attaque, le président des États-Unis, Joe Biden, a signé un décret visant à améliorer la cybersécurité au sein de l'administration fédérale, soulignant que les agences doivent « montrer l'exemple ». Voilà un autre signe du monde dans lequel nous évoluons tous. La cybersécurité doit être une priorité absolue pour toutes les organisations.

Pour en savoir plus à propos de l'environnement actuel des ransomwares, découvrez ce webinar.

[2] https://www.accenture.com/us-en/insights/security/eighth-annual-cost-cybercrime-study

[3] https://cybersecurityventures.com/cybersecurity-almanac-2022/

[4] https://www.ibm.com/security/data-breach

[5] https://newsroom.ibm.com/2019-04-11-IBM-Study-More-Than-Half-of-Organizations-with-Cybersecurity-Incident-Response-Plans-Fail-to-Test-Them

[6] https://ico.org.uk/about-the-ico/media-centre/talktalk-cyber-attack-how-the-ico-investigation-unfolded/

[7] https://www.bloomberg.com/news/articles/2021-06-04/hackers-breached-colonial-pipeline-using-compromised-password

Pourquoi avez-vous besoin d'un plan de réponse aux incidents de cybersécurité ?

Gardez votre calme en cas d'urgence

Si vous n'avez pas déjà mis en place un plan de réponse aux incidents, vos équipes de sécurité et de gestion tenteront, à la dernière minute, de gérer un incident d'urgence. Elles risquent de mal communiquer entre elles et d'agir de façon inefficace, ce qui rendra la violation des données beaucoup plus coûteuse qu'elle ne doit l'être.

Réduisez vos coûts

Les violations sont potentiellement très coûteuses en raison des amendes réglementaires, des dédommagements à verser aux clients, des enquêtes à mener ainsi que des mesures à prendre à la suite d'un incident. Un plan de réponse efficace aux incidents de cybersécurité réduira tous ces coûts, ce qui en fait un investissement judicieux.

Restez dans les bonnes grâces

Certains organismes de réglementation spécialisés dans la protection des données (comme la loi californienne sur la protection des consommateurs) exigent légalement que les organisations opérant dans leur juridiction mettent en place un plan de réponse aux incidents. De plus, pour certains cadres de sécurité propres à un secteur, comme la certification ISO 27001, sans plan de réponse aux incidents, vous ne passerez pas l'audit permettant d'obtenir la certification.

Ne manquez rien

En cas de violation des données, il se peut que vous soyez légalement tenu de prendre certaines mesures et d'informer les autorités compétentes, comme les agences gouvernementales ainsi que les parties concernées. Sans plan de réponse aux incidents de cybersécurité, vous risquez de passer à côté d'étapes cruciales ou de négliger certains détails, ce qui vous expose à des amendes supplémentaires et à des poursuites judiciaires.

Protégez vos arrières

À la suite d'une violation importante, vous devrez passer par une enquête ou un audit externe. Si vous ne pouvez pas fournir la preuve de l'existence d'un plan de réponse aux incidents de cybersécurité, les auditeurs considéreront que vous ne prenez pas suffisamment au sérieux votre responsabilité à l'égard de vos données confidentielles et pourront vous imposer des sanctions plus sévères. En outre, sans plan de réponse aux incidents de cybersécurité, vos primes d'assurance risquent d'être considérablement plus élevées, ou votre assurance pourrait même être annulée ! Aïe !

Réponse rapide et protection des données

Un plan de réponse efficace aux incidents de cybersécurité comprend des procédures détaillées pour protéger les sauvegardes, assurer une gestion sécurisée des identités et des accès, et répondre rapidement aux vulnérabilités ainsi qu'aux menaces. La mise en place de ces procédures vous permet de résoudre rapidement tout incident, et de protéger vos données et vos systèmes.

Protégez votre réputation

Vos clients sont susceptibles de réagir très négativement si leurs données sont compromises. De même, les actionnaires et les investisseurs risquent de retirer leur soutien à une entreprise qui subit une violation. En contrepartie, le fait de répondre efficacement aux incidents démontre votre engagement en faveur de la sécurité et de la confidentialité, ce qui permet de renforcer la loyauté et la confiance des clients ainsi que des actionnaires. Dans le monde des affaires, la réputation est primordiale.

6 phases d'un plan de réponse efficace aux incidents de cybersécurité

1. Préparation

La phase de préparation est à bien des égards la partie la plus importante, car elle constitue la base du reste du plan. Techniquement, vous devriez toujours être en phase de préparation : être prêt à faire face à tout incident naissant, et maintenir votre plan constamment à jour et opérationnel. Voici les éléments clés qui doivent être inclus dans la phase de préparation :

- Veillez à ce que tous vos employés soient correctement formés à la sécurité des données ainsi qu'à la réponse aux cybermenaces et aux urgences.
- Procédez à une évaluation des risques pour hiérarchiser les problèmes de sécurité, identifier les éléments les plus confidentiels et les incidents de sécurité les plus critiques sur lesquels votre équipe doit se concentrer.
- Organisez régulièrement des formations et des exercices afin que chacun soit prêt à agir de manière appropriée en cas d'incident. Consultez la page 10 pour en savoir plus à propos des exercices du plan de réponse aux incidents courants.
- Attribuez les responsabilités et rôles pertinents aux membres de votre équipe responsable de la réponse aux incidents de cybersécurité, et veillez à ce qu'ils aient accès aux systèmes et aux outils nécessaires. Pour en savoir plus à propos des responsabilités de l'équipe, consultez la page 9.
- Clarifiez les processus et les stratégies de communication en cas d'incident. Qui doit être contacté, et à quel moment ? L'absence de communications claires et structurées en cas d'urgence peut être source de désordre et d'inefficacité.
- Assurez-vous que chaque aspect de votre plan (formation, exécution, ressources, etc.) est approuvé, financé et disponible à l'avance. En résumé, votre plan est-il opérationnel ?

La phase de préparation de votre plan est-elle terminée ? Pour vous en assurer, posez-vous les questions suivantes :

1. Tous les salariés ont-ils été formés aux stratégies et procédures de sécurité nécessaires ?
2. Votre plan de sécurité a-t-il été approuvé par la direction ? Est-il à jour et complété par des ressources ?
3. Tous les membres de l'équipe de réponse aux incidents connaissent-ils leur rôle et leur plan d'action ?
4. L'ensemble du personnel a-t-il participé à des exercices de simulation ? Est-il prêt à intervenir ?

2. Identification

Cette phase du plan est déclenchée lorsqu'un incident vient de se produire, et que vous devez le diagnostiquer et déterminer les mesures à prendre. Vous ne pouvez pas vous préparer spécifiquement à toutes les sources d'incidents possibles, car elles sont trop nombreuses, mais votre équipe doit être en mesure de détecter efficacement le type de menace ainsi que son niveau de gravité et de déterminer la réponse à apporter.

Il existe deux types de signes indiquant que vos systèmes de sécurité sont attaqués : **les précurseurs** (détectés avant qu'une attaque ne se produise) ou **les indicateurs** (détectés pendant ou après une attaque).

- Un exemple de précurseur serait un nombre élevé de tentatives d'identification échouées, suggérant qu'un pirate informatique tente de pénétrer votre réseau en devinant un nom d'utilisateur et un mot de passe.
- Un exemple d'indicateur serait un logiciel antivirus vous alertant qu'une personne de votre réseau a cliqué sur un lien malveillant et que son ordinateur est infecté.

Cette phase comprend également la **documentation** : votre équipe doit enregistrer tout ce qui se passe, y compris la nature de l'attaque, les preuves et les mesures prises pour y répondre. Ces informations seront utiles dans la phase d'actions post-incident, au tribunal et face aux auditeurs.

Enfin, cette phase doit également inclure la **notification** : il s'agit de s'assurer que toutes les parties concernées (forces de l'ordre, organismes fédéraux, clients, actionnaires et entreprises touchées) sont informées qu'une attaque a eu lieu. Une notification en temps utile vous permet de rester du bon côté de la loi, de protéger votre réputation et de réduire votre responsabilité à long terme. Votre plan doit inclure des instructions claires indiquant qui doit être informé et quelles sont les étapes de la procédure de notification.

Questions à poser lors de la phase d'identification :

1. Quand et où l'incident a-t-il commencé ?
2. Qui l'a découvert, et comment ?
3. Quelle est l'étendue des dégâts ?
   Quelles sont les zones touchées ?
4. Les opérations commerciales sont-elles touchées ? Comment ?

3. Confinement

Lorsque vous découvrez une violation, vous pourriez être tenté de supprimer toutes les données contaminées dès que possible pour éliminer la menace. Cependant, cette mesure aurait pour effet de supprimer toutes les preuves précieuses que vous pouvez utiliser dans le cadre d'audits post-incident, et pour vous aider à déterminer comment la violation a commencé et comment empêcher qu'elle ne se reproduise.

Au lieu de cela, il est préférable de contenir la violation en déconnectant les appareils concernés d'Internet, afin de prévenir tout dommage supplémentaire pour votre entreprise. Il est également judicieux de disposer d'une sauvegarde redondante du système pour faciliter la restauration des opérations et ne pas perdre définitivement les données compromises.

Le confinement peut se présenter sous deux formes :

- **Confinement à court terme :** solutions temporaires, comme l'isolement du segment de réseau affecté, la mise hors service de tout serveur compromis et la redirection du trafic vers des serveurs de secours.
- **Confinement à long terme :** poursuite des opérations en utilisant des solutions temporaires tout en reconstruisant des systèmes propres, en se préparant à les remettre en ligne lors de la phase de rétablissement.

Au cours de cette phase, vous pouvez également mettre à jour et corriger vos systèmes, vérifier vos protocoles d'accès à distance, modifier tous les identifiants d'accès au système et renforcer vos mots de passe.

Il vaut mieux prévenir que guérir

Selon le rapport Cost of a Data Breach 2021 d'IBM, il faut en moyenne 287 jours à une équipe de sécurité pour identifier et contenir une violation de données[9]. C'est pourquoi la phase de préparation est si importante – pour éviter tout incident dès le départ.

Vous devez tenir compte d'un certain nombre de facteurs avant de décider d'une procédure de confinement. Le NIST les énumère comme suit :

- Dommages potentiels et vol de ressources
- Nécessité de préserver les preuves
- Disponibilité des services (par exemple, connectivité du réseau, services fournis à des parties externes)
- Temps et ressources nécessaires à la mise en œuvre de la stratégie
- Efficacité de la stratégie (par exemple, confinement partiel, confinement total)
- Durée de la solution (par exemple, une solution de contournement d'urgence à retirer au bout de quatre heures, une solution de contournement temporaire à retirer au bout de deux semaines ou encore une solution permanente).

Questions à poser lors de la phase de confinement :

1. Que faites-vous pour contenir les violations à court et à long terme ?
2. Avez-vous mis en quarantaine toutes les zones touchées ?
3. Quelles sont les sauvegardes que vous avez mises en place ?
4. Toutes les autorisations d'accès ont-elles été modifiées et renforcées ?
5. Avez-vous appliqué tous les derniers correctifs et mises à jour de sécurité ?

4. Élimination

Les étapes exactes de la phase d'élimination dépendent du type d'attaque auquel vous êtes confronté. Par exemple, il s'agit de supprimer les programmes malveillants, de désactiver tout compte compromis, de combler les vulnérabilités du réseau, etc. Fondamentalement, l'élimination signifie trouver la cause profonde de l'attaque et s'en débarrasser !

Votre équipe peut éliminer la menace par elle-même ou confier cette tâche à un tiers. Dans tous les cas, il y a un point important à retenir : l'élimination doit être complète. S'il reste ne serait-ce qu'une trace de programme malveillant ou de zones touchées dans vos systèmes, vous risquez de vous retrouver avec des données compromises et une responsabilité aggravée.

La Commission fédérale du commerce des États-Unis dresse une liste des mesures que vous pouvez prendre pour sécuriser vos systèmes pendant et après une violation, y compris la consultation d'une équipe tierce d'analyse des données, la sécurisation des systèmes physiques qui ont été compromis, le tri de tout contenu inapproprié qui a été publié sur vos réseaux et la communication avec les personnes qui ont découvert la violation.

La mise en place d'un plan de réponse efficace aux incidents de cybersécurité est cruciale pour cette phase, car en suivant les instructions qu'il prévoit, vous vous assurez que vos mesures d'élimination et de sécurité sont approfondies et méticuleuses, et qu'elles ne laissent rien au hasard.

Questions à poser lors de la phase d'élimination :

1. Tous les programmes malveillants et les zones affectées ont-ils été éliminés ?
2. Avez-vous vérifié toutes les zones qui auraient pu être touchées ?
3. Avez-vous nettoyé tout autre dommage résultant de l'attaque, comme du contenu publié sur votre site Internet ou sur des canaux de communication ?

[9] https://www.ibm.com/security/data-breach

5. Rétablissement

La phase de rétablissement consiste à restaurer les systèmes touchés et à les remettre en service. Cette démarche doit être effectuée avec soin afin d'éviter qu'un autre incident ne se produise.

Ce processus peut prendre des jours, des semaines ou des mois, selon la gravité de la violation. Le NIST recommande de commencer par renforcer immédiatement votre sécurité dans son ensemble, puis de se concentrer sur des changements permanents à long terme pour que vos systèmes soient le plus sécurisés possible.

Les points importants à prendre en compte pendant cette phase sont le moment où vous rétablirez complètement les opérations, la manière dont vous vérifierez que tout fonctionne correctement et la durée pendant laquelle vous continuerez à surveiller la situation jusqu'à ce que vous soyez vraiment sûr que les choses sont rentrées dans l'ordre.

Questions à poser lors de la phase de rétablissement :

1. Quand les systèmes seront-ils de nouveau opérationnels ?
2. Quels outils et procédures continus utiliserez-vous pour vérifier que les systèmes restaurés fonctionnent correctement ?
3. Le système peut-il être restauré à partir d'une sauvegarde fiable ?
4. Combien de temps allez-vous surveiller la situation jusqu'à ce que vous puissiez être certain que tout est rentré dans l'ordre ?

6. Actions post-incident

Cette phase consiste essentiellement à organiser une réunion de compte-rendu post-incident en présence de toutes les parties concernées. Il est préférable d'organiser la réunion quelques jours après la résolution de l'incident, mais pas plus de deux semaines après, afin que tous les participants aient encore la mémoire fraîche. C'est une façon de tourner la page après l'incident.

Voici les éléments clés de cette phase :

- Un examen complet de l'incident, de la découverte au rétablissement. L'examen doit se concentrer sur des questions de ce type : tout le monde a-t-il suivi les procédures du plan de réponse aux incidents de cybersécurité ? Étaient-elles efficaces ? Avez-vous relevé des points faibles ou des éléments à améliorer ? Que pourrait-on faire différemment la prochaine fois ? Comment pourrait-on prévenir des incidents similaires à l'avenir ?
- Une évaluation et une mise à jour de votre plan de réponse aux incidents en fonction des conclusions tirées de l'examen.
- La création d'un rapport de suivi qui servira de référence lors de la gestion d'incidents similaires. Il est également utile de disposer d'une chronologie formelle des événements (avec des informations horodatées, comme les journaux de données) en cas de procédures juridiques telles que les audits.
- Une évaluation du dommage total causé par la violation, y compris une estimation monétaire. Cette information est également utile pour des raisons juridiques, comme les activités de poursuites judiciaires.
- Résoudre tous les problèmes que vous n'avez pas eu le temps de régler pendant l'incident, comme remplir les documents nécessaires et s'assurer que toutes les parties concernées sont informées.

Questions à poser lors de la phase d'actions post-incident :

1. Quels changements doivent être apportés à la sécurité ?
2. Quelles sont les faiblesses que la violation a exploitées et comment peut-on les éviter à l'avenir ?
3. Avez-vous examiné en détail l'incident et créé un rapport de suivi ?
4. Avez-vous prévenu toutes les personnes qui doivent l'être ?
5. Avez-vous tout préparé pour faire face au processus d'audit post-incident ?

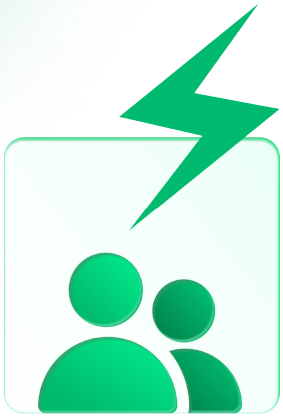
Mise en place d'une équipe de réponse aux incidents

Vous avez donc créé le plan de réponse aux incidents parfait, mais qui va l'exécuter ? C'est là que vous avez besoin d'une équipe dédiée spécialisée dans la réponse aux incidents.

Le NIST propose trois modèles différents d'équipes de réponse aux incidents :

- Central – un organisme central qui gère tous les incidents pour l'ensemble de l'organisation.
- Distribué – plusieurs équipes d'intervention, chacune responsable d'un lieu physique différent, d'un département ou d'une partie de l'infrastructure informatique.
- Coordonné – une équipe centrale servant de centre de connaissances pour diverses équipes distribuées, et les assistant dans les incidents complexes, critiques ou à l'échelle de l'organisation.

En fonction de la taille de votre organisation ainsi que de la gravité et de la complexité des incidents possibles, vous pouvez disposer d'une équipe de réponse aux incidents dédiée et à plein temps, ou former des employés ordinaires pour qu'ils deviennent une équipe de réponse aux situations d'urgence. Certaines organisations confient même leurs besoins en matière de sécurité à une équipe tierce de réponse aux incidents.



Questions à poser lors de la création d'une équipe :

Lorsque vous créez votre équipe de réponse aux incidents, vous pouvez vous poser les questions suivantes pour orienter le processus :

1. Avez-vous besoin d'une équipe dédiée à temps plein ou d'une équipe de « bénévoles » à temps partiel ?
2. De quelles formations l'équipe aura-t-elle besoin ? Les membres de l'équipe doivent-ils être des experts en sécurité ?
3. Quel sera le coût de la formation et du suivi de l'équipe de réponse ? Le coût peut être élevé, mais une violation majeure de la sécurité résultant d'un mauvais plan et d'une équipe non préparée peut s'avérer beaucoup plus coûteuse. L'investissement en vaut donc la peine.

Formez-vous pour garder une longueur d'avance

Le sondage « ISACA State of Cybersecurity 2021 Part 1 » a révélé que 61% des organisations se sentent en sous-effectif pour ce qui est des professionnels de la cybersécurité[10]. 50% des répondants se sentent insuffisamment qualifiés pour les postes de sécurité, et 31% du personnel des ressources humaines ne se rend pas compte du caractère critique des problèmes de cybersécurité. C'est probablement le cas de votre personnel aussi, n'est-ce pas ? La mise en place d'un plan efficace est donc essentielle pour sensibiliser le personnel et améliorer ses compétences.

Rôles clés dans une équipe de réponse aux incidents :

Voici quelques-uns des acteurs clés qui composent une équipe solide de réponse aux incidents. Si vous êtes une petite entreprise, ne vous inquiétez pas ! Il s'agit de rôles, et non de salaires supplémentaires – ce qui signifie que les membres de l'équipe peuvent jouer plusieurs rôles. Dans certains cas, votre équipe peut se composer d'une seule personne !

- **Responsables de la réponse aux incidents :** chargés d'approuver le plan de réponse aux incidents de cybersécurité et de coordonner l'activité lorsqu'un incident se produit.
- **Analystes de sécurité :** passent en revue les alertes, détectent les incidents possibles et lancent des enquêtes lorsqu'un incident est détecté.
- **Chercheurs de menaces :** fournissent des informations contextuelles sur une menace en effectuant des recherches sur le Web, en consultant les flux de Threat Intelligence, les données des outils de sécurité, etc.
- **Autres parties prenantes :** cadres supérieurs, membres du conseil d'administration, RH, RP et personnel de sécurité de haut niveau comme le responsable de la sécurité des systèmes d'information (CISO).
- **Tiers :** avocats, services de sécurité externalisés, forces de l'ordre, etc.

Exercices de formation à la cybersécurité

Comme nous l'avons mentionné dans la phase de préparation, l'une des principales mesures de tout plan de réponse aux incidents de cybersécurité consiste à organiser régulièrement des exercices d'entraînement et de simulation afin de maintenir votre équipe sur le qui-vive et prête à faire face à toute urgence. L'objectif de ces exercices est de sensibiliser le personnel à la sécurité, de tester l'efficacité de votre plan et de votre formation, et de susciter des discussions entre les employés.

Votre plan de formation doit comprendre au moins un exercice annuel coordonné à grande échelle, qui peut durer un ou deux jours. Des exercices de table ronde peuvent être réalisés plus fréquemment, en fonction des besoins de votre organisation.

Types d'exercices d'entraînement

Exercices de discussion

Il s'agit d'un exercice de table ronde au cours duquel votre équipe examine une menace hypothétique à la sécurité et explore verbalement les voies de réponse possibles.

- **Avantages :** requiert un minimum de préparation et de ressources, tout en mettant à l'épreuve les connaissances de votre équipe en matière de sécurité et la compréhension de leur rôle en matière de réponse aux incidents dans un scénario réel potentiel.
- **Inconvénients :** ne permet pas de tester pleinement votre plan de réponse ni les actions de réponse de votre équipe en temps réel.

Exercices de simulation

Il s'agit d'une démonstration en direct qui a été soigneusement chorégraphiée et planifiée.

- **Avantages :** permet de tester les réponses aux incidents de votre équipe en temps semi-réel, leur donnant une meilleure compréhension de leurs rôles et de la gravité d'une urgence réelle.
- **Inconvénients :** la planification et la coordination demandent plus de temps, mais ne permettent pas de tester complètement votre plan ni les rôles des équipes de la façon la plus réaliste.

[10] https://www.isaca.org/why-isaca/about-us/newsroom/press-releases/2021/new-isaca-study-finds-cybersecurity-workforce-minimally-impacted-by-pandemic-but-still-grappling

Tests en parallèle

Un test en parallèle est réalisé dans un environnement de test sûr, ce qui en fait le type d'exercice le plus réaliste possible, sans pour autant mettre votre organisation en danger.

- **Avantages :** fournit à votre équipe la simulation la plus réaliste et le meilleur compte-rendu en temps réel de ses actions et de son rôle. Ce type d'exercices devrait permettre d'identifier les points faibles ou les lacunes de votre plan et de la compréhension du rôle de l'équipe.

- **Inconvénients :** requiert plus de planification que tout autre type de formation, et est également la plus coûteuse, car un environnement de test réel doit être simulé (y compris les systèmes séparés, les réseaux, etc.).

Pratiques exemplaires relatives au plan de réponse aux incidents de cybersécurité

Résumons en examinant ces quatre pratiques exemplaires qui devraient être mises en place pour vous assurer que votre plan de réponse aux incidents de cybersécurité est parfaitement au point !

1. Impliquez toutes les parties prenantes

Une violation de la sécurité peut avoir des répercussions sur tous les secteurs de l'organisation. Vous devez donc vous assurer que tout le monde est impliqué et se sent concerné. Toutes les parties prenantes clés doivent avoir leur mot à dire dans la préparation de votre plan de sécurité. Il peut s'agir de la direction, des responsables des ressources humaines, des représentants juridiques, des responsables de la conformité et des parties prenantes tierces, comme les fournisseurs de technologie et les relations publiques.

2. Mettez-les à l'épreuve

Votre plan de sécurité peut sembler parfait en théorie, mais il ne sert à rien s'il ne fonctionne pas quand il le faut. Des exercices réguliers assurent que chacun a une idée claire de ce qu'il doit faire en cas d'urgence, et permettent d'identifier et de corriger les points faibles du plan. C'est en forgeant qu'on devient forgeron !

3. Clarifiez les stratégies de communication

Si vous n'avez pas mis en place de stratégie de communication claire, une violation de la sécurité peut entraîner un chaos absolu, tant à l'intérieur qu'à l'extérieur de votre organisation : les employés se mettront à paniquer sans réfléchir, des informations différentes seront envoyées à différents services et personne n'aura une vision claire de ce qui se passe réellement. Votre plan de communication doit inclure des instructions claires précisant qui doit communiquer avec qui, par quels canaux de communication, et à quel niveau de détail, pour chaque étape du processus d'incident. Les communications impliquent non seulement l'équipe responsable de la réponse aux incidents, mais aussi toutes les parties concernées, y compris les clients et la presse. Votre stratégie doit donc tenir compte de tous ces aspects.

4. Simplifiez les choses

Votre plan de réponse aux incidents est comme un manuel de stratégie de combat, il doit donc être facile à suivre dans le feu de l'action. Vous ne voulez pas que votre personnel perde un temps précieux à essayer de comprendre un document trop compliqué lorsque votre organisation fait l'objet d'une attaque. Certes, il doit être détaillé, avec des étapes et des procédures particulières, mais il doit aussi être clair et exploitable.

Comment Kaspersky peut vous aider

Nous pouvons vous aider à renforcer la protection de vos données grâce à des services tels que Kaspersky Optimum Security – qui complète vos compétences en matière de cybersécurité en ménageant vos ressources, grâce à un EDR efficace et à une recherche des menaces gérée, mais sans coûts prohibitifs ni complexité – ou encore des services spécialisés de formation à la sécurité, de réponse aux incidents et de communication en cas de crise.

En savoir plus

Recommandations de lecture

Enseignements tirés du travail à distance
La protection contre les ransomwares à l'heure du travail flexible
Guide d'achat sur la sécurité optimale