Cybersécurité: La check-list pour la gestion de crise

Conseils pour la planification et la mise en œuvre de la continuité de l'activité avec Zscaler

zscaler™

En période d'incertitude, tout CxO souhaite en priorité protéger la santé et le bien-être de ses employés. Lorsqu'une catastrophe survient, les entreprises doivent plus que jamais être agiles, non seulement dans leur développement, mais également dans leur fonctionnement. Lorsque celui-ci est perturbé par une crise, adopter un plan de continuité d'activité ne doit en aucun cas entraîner la fragilisation des mesures de cybersécurité.

En situation de crise, un responsable de la sécurité informatique (RSSI) doit agir rapidement et de manière décisive. Voici huit objectifs stratégiques clés que Zscaler suggère aux responsables de la sécurité informatique de se fixer en temps de crise:

1. Permettre aux employés de travailler à distance et leur fournir l'assistance nécessaire. →
2. Mettre en place et suivre les opérations de sécurité et le travail à distance des équipes de surveillance. →
3. Se préparer à l'augmentation des risques de cybermenace, notamment des attaques opportunistes. →
4. S'assurer que les fournisseurs tiers peuvent prendre en charge vos systèmes. →
5. Adapter les priorités en matière de sécurité de l'entreprise. →
6. Se préparer à l'ajustement et à l'examen du budget. →
7. Garantir la conformité aux règlements, même si elle devient difficile à respecter. →
8. Diriger en période de crise →

Chaque crise est différente. La liste de contrôle ci-dessous est un plan d'action de gestion de crise destinée aux responsables de la sécurité informatique.

1. Permettre aux employés de travailler à distance et leur fournir l'assistance nécessaire.

Lorsqu'une crise survient, surtout s'il s'agit d'une épidémie virale, les employés doivent être en mesure de travailler à distance. Les RSSI doivent prendre en compte les facteurs suivants.

- ## Quel sera l'impact des connexions à distance des employés sur le fonctionnement des data centers?
  - Les procédures de correction et de mise à jour pourraient être perturbées si on n'y veille pas.
    - Examiner et établir des procédures de correction et de gestion à distance des systèmes.
  - Les recherches d'appareils compromis et de violations de la cybersécurité doivent être effectuées à distance suivant la procédure suivante:
    - Créer de nouvelles procédures pour le personnel de cyber-réparation travaillant à distance.
    - Créer de nouveaux processus d'investigation et d'expertise pour les employés et les actifs distants.
    - Hiérarchisation: prioriser les investigations et se concentrer d'abord sur les initiatives critiques.
  - Lorsqu'il n'y a personne sur site, les réseaux sans fil de bureau deviennent une faille de sécurité attrayante pour les pirates:
    - S'assurer que les réseaux sans fil sur site peuvent être sécurisés à distance, ou éteints à distance s'ils ne sont pas utilisés.

- ## Les licences pour les produits et les services seront-elles compatibles avec le travail à distance?
  - Déterminer si le nombre de licences pour terminaux changera avec l'augmentation du télétravail.
  - Déterminer si le nombre de licences d'outils de cybersécurité (y compris les antivirus, la détection et la réponse des terminaux, l'accès aux identités et leur gestion) changera avec l'augmentation du télétravail.
  - Déterminer si l'utilisation croissante d'appareils personnels pour le travail à distance affectera le nombre de licences.

- ## Comment le passage au télétravail affectera-t-il les contrôles de sécurité des appareils de l'entreprise?
  - Déterminer comment le travail à distance affectera vos contrôles de sécurité:
    - Faire un inventaire des contrôles (utiliser NIST Cybersecurity Framework comme guide) et une analyse.
  - Vérifier que les contrôles à distance fonctionnent :
    - Les contrôles basés sur les data centers peuvent perdre leur efficacité s'ils sont effectués sans un VPN (lequel pourrait être surchargé en cas de pic d'accès à distance).
    - Au besoin, identifier les contrôles compensatoires (administratifs/techniques).
    - Déterminer le risque et l'impact sur les mécanismes de protection contre la perte de données (DLP).

- Établir un plan de réponse en cas de perte de visibilité:
  - Déterminer d'autres moyens de recevoir les données télémétriques, car vous ne pourrez peut-être plus communiquer avec les terminaux.
  - S'assurer que les mécanismes par défaut de mise à jour sont activés.

Comment gérer le nettoyage des logiciels malveillants?

- Définir un moyen de nettoyer les terminaux distants. Si ce n'est pas possible, établissez une procédure permettant aux employés de le faire eux-même.

Comment sensibiliser les employés sur les questions de sécurité sans communication ni événements en personne?

- Établir un procédure de sensibilisation et d'éducation aux meilleures pratiques de cybersécurité.
- Ajouter des « rappels en matière de sécurité » aux communications planifiées des cadres supérieurs.

2. Mettre en place et suivre les opérations de sécurité et le travail à distance des équipes de surveillance.

Vos équipes du data center et de la sécurité sont également à leurs domiciles depuis lesquels ils s'attellent à aider les employés. Cela peut avoir un impact sur la sécurité et les procédures informatiques.

- ### Comment communiquer et diffuser les informations aux équipes informatiques distantes?
  - Établir des listes de diffusion, des chats en groupe, des réunions (virtuelles) régulières.
  - Avoir recours à des outils de vidéoconférence comme Zoom ou WebEx.
  - Vous procurer des outils de collaboration comme Slack, Microsoft Teams ou Google Chat.

- ### Comment les équipes informatiques vont-elles accéder aux outils et effectuer les contrôles depuis leur domicile?
  - Modifier les règles de politique d'accès pour permettre l'utilisation à distance.
  - Si possible, permettre l'accès à distance via des portails Web ou des applications clients.

- ### Quel sera l'impact sur la réponse aux incidents?
  - Établir un plan de réponse aux incidents de sécurité distants.
  - Mettre en place un plan de réparation des incidents distants.

- ### Comment les identités seront-elles fournies et enlevées?
  - Assurez-vous que les accès peuvent être accordés ou retirés à distance aux employés.
  - Au besoin, réduire les privilèges pour minimiser les risques.
  - Définir si une procédure SLAM (starters, leavers, and movers [nouveaux, partants et affectés]) nécessite la présence physique de l'employé ou d'un membre de l'équipe d'orientation pour les besoins suivants:
    - Remise ou récupération d'actifs
    - Nettoyage (physique et informatique) d'actifs
    - Signature de documents
  - Au besoin, se préparer à distribuer les mécanismes Token ou MFA via des systèmes de courrier ou de colis.

- Quel sera l'impact du télétravail sur les services de sécurité tiers?
  - Déterminer et documenter les exigences liées à l'accès par des tiers.
  - Prioriser l'accès par les tiers en fonction de l'urgence et de l'instantanéité.
  - Établir une procédure d'octroi et de révocation de l'accès aux tiers.

3. Se préparer à l'augmentation des risques de cybermenace, notamment des attaques en situation.

Des crises comme l'épidémie de COVID-19 en 2020 entraînent généralement une recrudescence des attaques dites « opportunistes » par des logiciels malveillants.

Lorsque les entreprises utilisant des VPN pour l'accès à distance augmentent leur nombre de télétravailleurs, la distance de backhauling MPLS et la surface de menace s'étendent également. Il n'est pas facile de faire évoluer les modèles de périmètre de sécurité basés sur le VPN pour prendre en charge un plus grand nombre d'accès à distance. Certains employés peuvent alors être tentés de contourner les pare-feux et se connecter directement à Internet. Les pirates informatiques détectent ces failles et les exploitent. Pire encore, le désir d'être informé sur le crise peut entraîner une baisse de la vigilance: des escrocs cyniques tentent alors de faire circuler des logiciels malveillants déguisés en informations importantes sur la crise.

Les experts en cybersécurité (comme l'équipe ThreatLabZ de Zscaler) confirment le lien entre les crises et l'augmentation des violations de données. Les RSSI doivent faire face aux nouveaux risques de menace qui surviennent en période de crise.

- Évaluer les risques: les utilisateurs distants sont-ils vulnérables aux attaques de phishing ou à d'autres pièges?
  - Rappeler les politiques de sécurité aux employés et les sensibiliser aux escroqueries en temps de crise.
  - Insister sur l'importance de redoubler de vigilance en temps de crise.

4. S'assurer que les fournisseurs tiers peuvent prendre en charge vos systèmes.

Les fournisseurs tiers de services de sécurité adapteront également leurs opérations pour répondre aux demandes liées à la crise. Assurez-vous auprès de vos fournisseurs tiers que la prise en charge de vos systèmes ne subira aucune modification pouvant affecter l'environnement.

- Les fournisseurs de sécurité prendront-ils en charge les modifications apportées à vos opérations en réponse à la crise?
  - Vérifier la prise en charge par les fournisseurs tiers:
    - S'assurer que l'accès aux systèmes tiers est maintenu, même à distance.
    - Examiner la faisabilité des plans de continuité des activités (BCP) ainsi que les services de crise de chaque fournisseur.
    - Notez que les fournisseurs de services de sécurité gérés (MSSP) en particulier pourraient ne pas prendre en charge le télétravail. Comment pourriez-vous vous préparer à cette éventualité?

5. Adapter les priorités en matière de sécurité de l'entreprise.

En période de crise, une entreprise doit se concentrer sur les interventions les plus urgentes. L'attention accordée aux questions de cybersécurité pourrait donc baisser.

- ## Comment assurer la sécurité en temps de crise?
  - Au besoin, modifier les niveaux de risque acceptables pour les actifs de l'entreprise:
    - Faire un inventaire des actifs matériels et logiciels.
    - Assurer la meilleure visibilité possible sur les facteurs de risque pour les actifs.
    - Effectuer une étude, comparée des performances et de la sécurité et, au besoin, ajuster les politiques de sécurité.
  - Évaluer la tolérance au risque que vous comptez adopter en cas de passage au télétravail.
  - Insister sur l'importance de la sécurité sans toutefois faire obstacle aux changements ou aux actions nécessaires. (La sécurité restera un facteur déterminant pour une réussite durable.)

- ## Pouvez-vous voir les nouveaux processus, déploiements et appareils?
  - Définir des mécanismes d'obtention, d'exploitation et d'évaluation à distance des rapports (flux, journaux, télémétrie).
  - Établir des processus permettant de traiter ces informations à partir de systèmes extérieurs à l'entreprise.

6. Se préparer à l'ajustement et à l'examen du budget.

En période de crise, les dépenses consacrées aux interventions d'urgence peuvent primer sur elles liées à la sécurité. Le financement de projets peut devenir difficile, voire impossible à obtenir. La sécurité pourrait même être reléguée au second plan pour permettre de répondre aux besoins opérationnels immédiats.

- Votre budget opérationnel ou de planification sera-t-il affecté?
  - Inventorier, hiérarchiser et, au besoin, trier les plans, les appareils et les services essentiels.
  - Accepter de supprimer les éléments non essentiels (et accepter la nouvelle conception de ce qui est « essentiel »).
  - Réaffecter le budget dédié aux voyages, aux événements et aux initiatives futures pour renforcer les priorités de sécurité.

7. Garantir la conformité aux règlements, même si elle devient difficile à respecter.

Même en temps de crise, les entreprises sont dans l'obligation de se conformer à la réglementation.

- Comment les changements opérationnels et structurels effectués en réponse à une crise affecteront-ils la capacité de votre organisation à se conformer aux exigences réglementaires?
  - Déterminer, puis documenter l'impact des nouveaux déploiements d'appareils et de processus sur les flux de données et les exigences de sécurité.
- Les opérations de réponse à la crise auront-elles un impact sur la capacité de votre organisation à se conformer aux exigences en matière de résidence de données?
  - Déterminer où sont stockées les données et comment le chemin des données en transit pourrait être affecté.
  - Vérifier que les règles de conformité sont respectées sur les nouveaux chemins des flux de données. Cela pourrait nécessiter des changements dans l'administration du cloud et du data center, et même l'ajout de nouvelles redondances de données dans différents sites.
  - S'assurer que le SSL et les autres mesures de sécurité sont utilisés lorsque c'est nécessaire, et respecter les lois applicables en matière de confidentialité des données.
- Les organismes de réglementation ou les gouvernements modifieront-ils règles de conformité en temps de crise?
  - Surveiller les communications réglementaires affectant les exigences de conformité.
  - Créer (ou au moins, prévoir de créer) des procédures de réponse aux ajustements des exigences réglementaires en temps de crise.

8. Diriger en période de crise

En situation de crise, tout le monde travaille avec peu d'informations et doit réagir aux événements à mesure qu'ils se produisent. Étant donné l'importance du maintien de la sécurité, un RSSI ne peut se permettre d'agir dans la précipitation. La clairvoyance, l'humilité, la franchise et la fermeté sont indispensables à une communication de crise efficace. Trop communiquer sans objectif précis agace, alors que communiquer trop peu des trous d'information. Établir des plans d'action clairs et les faire connaître.

- ## Avec qui vous faudra-t-il communiquer?
  - Vous assurer que les acteurs de sécurité interne connaissent bien les rôles, les responsabilités, les actions et les procédures.
  - Assurez-vous que les acteurs externes et les clients sont informés des changements affectant les opérations.

- ## À quelle fréquence devrez-vous communiquer?
  - Communiquer les changements importants et immédiats lorsqu'ils se produisent.
  - Communiquer vos plans en phases mesurables et traçables, avec des statistiques et des étapes de progression claires.
  - S'assurer que l'information n'est pas juste diffusée, mais qu'elle est reçue, comprise et mise en œuvre. Établir des procédures de mesure de l'efficacité de la communication.

- ## Avec qui coordonnerez-vous la communication?
  - Mettre en place une équipe interne de communication de crise.
  - Consulter les groupes sectoriels pour comparer les meilleures pratiques en matière de communication.
  - Rechercher des ressources gouvernementales pertinentes (locales, étatiques ou fédérales).

- ## Comment un RSSI peut-il prendre au mieux les devants en matière de communication de crise?
  - En tant que professionnel de la sécurité, vous avez de l'expérience en matière de gestion des crises. Vous devez donc:
    - Mener la préparation et la réponse de votre organisation.
    - Aider les acteurs de votre organisation à évaluer les conséquences des décisions d'urgence.
  - Soyez un leader posé:
    - Vous servir de l'information, de la pédagogie et de la préparation pour combattre l'anxiété, l'incertitude et la panique.

La plate-forme cloud Secure Access Service Edge de Zscaler a été conçue spécifiquement pour permettre une connectivité directe via des points d'accès Internet locaux, garantissant que les entreprises (ainsi que tous leurs télétravailleurs) restent opérationnelles en périodes de crise.

Le programme de continuité des activités de Zscaler permet aux organisations de garantir des services de sécurité de classe mondiale, même dans les circonstances les plus difficiles.

En savoir plus

À propos de Zscaler

Zscaler a été fondé en 2008 sur un concept simple mais puissant: à mesure que les applications migrent vers le cloud, la sécurité doit également s'y déplacer. Aujourd'hui, nous aidons des milliers d'organisations mondiales à se porter vers des opérations basées sur le cloud.