Exercice de crise cyber

Face aux défis des conséquences d'une cyber attaque réussie, améliorer la cyber résilience

Nous contacter : contact@almond.consulting

Testez votre organisation et préparez vos équipes à faire face à une crise d'origine cyber.

- Les cyber attaques visent toutes les entreprises et peuvent engendrer des crises majeures auxquelles les mieux préparées vont survivre et en faire des opportunités de démontrer leur résilience.
- Comment ferez-vous pour limiter les impacts et gérer la situation lorsque vous serez touchés ?
- Vos chaînes de décision / commandement et vos opérationnels sont-ils prêts à faire face à une vraie attaque ?

Notre Offre

Préparer l'exercice de crise cyber

- Sélectionner les **modalités de réalisation** selon votre degré de maturité : typologie d'exercice (sur table, simulé avec stimuli…), timing et intensité, éléments à tester (alerte, gestion, sortie…)
- Déterminer les **objectifs à tester pendant l'exercice** afin d'évaluer les points forts et les axes d'amélioration (communication, exigences légales, documentation, organisation de la cellule de crise…)
- Créer un **scénario sur mesure**, en fonction de vos priorités, de votre environnement, de vos RETEX… L'exercice doit être réaliste !
- Développer le scénario avec nos **experts en gestion de crise** et nos **experts CERT Almond**
- Préparer des **outils** : chronogramme, stimuli, support d'animation…

Réaliser l'exercice de crise cyber

- **Sensibiliser des participants à la gestion de crise cyber** en amont de l'exercice de crise afin de s'assurer de leur niveau de connaissance et de leur implication dans l'exercice.
- **Gamifier & mobiliser** : mettre les participants dans des conditions propices grâce notamment à des Ice breakers.
- **Animer l'exercice pour mettre les joueurs en situation**, respecter le chronogramme préparé en amont et réaliser les stimulis préparés (appels téléphoniques, mails, vidéo, tweet…)
- **Observer les joueurs** en se focalisant sur les objectifs fixés de l'exercice. L'observateur notera des constats en matière d'organisation (logistique, communication, utilisation des outils…), de processus (alerte, décisions prises, responsables…), de comportements (dominant, absent, anticipateur…)

Analyser et améliorer

- Consolider un **retour d'expérience des participants** à chaud et à froid (questionnaire).
- Rédiger un **rapport** présentant les points forts de la gestion de crise et les axes d'amélioration.
- Formaliser des **actions concrètes techniques et organisationnelles** pour augmenter la cyber résilience.
- Présenter des **propositions de complexification** des prochains exercices de crise. Les exercices de crise doivent s'inscrire dans une démarche globale de capitalisation et d'apprentissage progressif sur tous les axes de la gestion de crise.

Bénéfices

1. **Évaluer la communication entre les parties prenantes internes et avec les parties prenantes externes dans un contexte de cyber crise**
2. **Définir les rôles et les responsabilités de chaque acteur (RSSI, équipes IT, CERT, Top Management)**
3. **Évaluer l'adéquation des processus et des procédures existantes dans un contexte de crise cyber**
4. **Recenser les actions impactantes pour l'organisation (Qui peut déconnecter une application métier ? Quels sont les critères ? Comment procéder ?)**

Notre proposition de valeur

Des sessions animées avec des techniques de conduite de changement et de gamification pour favoriser la montée en compétence

Des exercices construits sur mesure, selon vos spécificités et vos besoins

Des experts internes : techniques, en sécurité de l'information, en gestion de crise et en protection des données

Almond

Paris | Nantes | Strasbourg | Lyon | Genève

https://almond.consulting