Volet joueur

RÉPUBLIQUE FRANÇAISE
Liberté
Égalité
Fraternité

Exercice de gestion de crise cyber

Fiche « Bonnes pratiques » de gestion de crise cyber

✓ **Pourquoi les attaques d'origine cyber réussissent-elles trop souvent ?**

La sécurité du numérique n'est pas un état stable	La transformation numérique augmente les risques
Des nouvelles vulnérabilités apparaissent quotidiennement et les modes opératoires des attaquants évoluent perpétuellement	Vecteur d'innovation et de croissance, la transformation numérique présente aussi des risques en augmentant la surface d'attaque (ex. convergence IT/OT) ou concept de SI étendu (Cloud)
Les systèmes d'information sont vulnérables	**L'environnement technologique est en perpétuelle évolution**
La sécurité des systèmes d'information est souvent mal prise en compte dans le cycle de vie des systèmes	La transformation rapide des technologies, des équipements et des usages créent un environnement en perpétuelle évolution, qui ne facilite pas la maîtrise de la sécurité des systèmes d'information

✓ **Les spécificités d'une crise d'origine cyber**

- **Une double temporalité :** impacts immédiats et une remédiation longue pouvant s'étendre sur plusieurs semaines voire plusieurs mois ;
- **Une absence d'unicité de lieu de réalisation :** potentielle propagation à d'autres organisations en raison de l'interconnexion des SI ;
- **Une menace s'adaptant** aux mesures d'endiguement et de remédiation ;
- **Une incertitude** concernant le périmètre de la compromission ;
- **Une complexité** pour comprendre les objectifs de l'attaquant et attribuer l'origine de l'attaque ;

✓ **Les clés pour une gestion de crise cyber réussie**

La préparation	La gestion de crise
• Connaitre et maîtriser ses systèmes d'information • Mettre en place un socle de capacités opérationnelles garantissant un niveau adapté de résilience numérique • Formaliser une stratégie de communication de crise cyber • Adapter son organisation de crise au scénario cyber • Préparer ses capacités de réponse à incident • S'entraîner pour pratiquer et s'améliorer	• Activer son dispositif de crise • Piloter son dispositif de crise • Soutenir les équipes de gestion de crise • Activer ses réseaux de soutien • Communiquer efficacement • Conduire l'investigation numérique • Mettre en place un mode de fonctionnement dégradé pour les métiers impactés • Durcir et remédier • Préparer et industrialiser la reconstruction • Organiser sa sortie de la crise • Tirer les leçons de la crise (RETEX)

Les guides de la collection « Crise »

Organisation d'un exercice de crise cyber

Co-production CCA

Gestion d'une crise d'origine cyber

Co-production CDSE

Communication de crise d'origine cyber

Co-production Cap'Com