Deloitte.

Cyber Sécurité – Gestion de crise

Comment faire face à l'imprévisible ?

Anticiper au mieux les risques

Comment se préparer à affronter une situation, la plupart du temps asymétrique, dans laquelle l'attaquant est organisé et a systématiquement un ou plusieurs coups d'avance ? Comment évaluer et adapter les dispositifs de gestion de crise ?

Dans un environnement où la déstabilisation passe de plus en plus par des attaques logiques et physiques, les impacts sont souvent considérables, en termes humains, financiers, d'image et de responsabilités. Il faut adapter le système de gestion de crise.

Il devient crucial de développer des réflexes de gestion de crise, concrets et viables.

Mettre en œuvre un système de management de crise

Quelles sont les conditions d'une réaction appropriée lors d'une crise, ou comment limiter les impacts irréversibles pour vos organisations ?

Il vous faut donc :

- une capacité à piloter en temps réel une situation de crise lorsqu'on ne dispose pas de toutes les infos ;
- une gestion de l'exposition médiatique des conséquences ;
- une capacité à piloter en temps réel les informations clés dont on dispose lors d'une crise ;
- une collaboration des fonctions opérationnelles et des experts.

Les 4 axes clés pour identifier vos capacités de résilience

Le processus
Avez-vous un processus global, partagé et éprouvé de gestion des incidents ?

L'organisation
Avez-vous un dispositif qui vous permet de prendre des décisions difficiles en situation de crise ?

L'évaluation
Vos fondamentaux sont-ils testés, éprouvés ? Votre organisation de crise est-elle entraînée ?

La décision
Avez-vous la capacité, dans une situation de crise, à prendre les décisions nécessaires à la survie de l'entreprise tout en gardant la maîtrise des dommages inévitables ?

Anticiper les risques pour savoir réagir

Nous intervenons à différents niveaux

- Audit de vos acquis, pour évaluer le niveau de résilience de vos dispositifs.
- Formalisation des recommandations pour corriger et améliorer vos dispositifs de manière simple et efficace.
- Préparation à travers des formations collaboratives, des tests et exercices fondés sur des scénarios sur mesure et réalistes en sécurité, continuité et gestion de crise.
- Analyse de l'efficacité de vos plans de communication et de sensibilisation.
- Coaching gestion du stress/ personnalité
- Coaching sur les réflexes de gestion de crise, de communication interne et externe.
- Aide à l'inscription de vos dispositifs dans un plan de maintien en condition opérationnelle.
- Accompagnement en cas de crise réelle.

Pourquoi Deloitte ?

- Centre opérationnel de gestion de crise
- Plus d'une cinquantaine de simulation de war gaming
- Numéro 1 mondial des services de conseil en cyber
- Deloitte, labellisé CNIL pour la procédure d'audit
- Collaborateurs certifiés ISO 22301, ISO 27001, ISO 27005, CISSP, CISA, CISM, CGEIT, IAPP

Exemple de cas pratique issu d'une expérience de demande de rançon

Jour J - 09h00

Un utilisateur envoie à l'équipe SSI/ Blue Team un mail qui lui semble suspect

Objet : Brexit et politique monétaire mondiale
PJ : PDF
Début des investigations par la Blue Team

Jour J - 10h00

Déclenchement de la CSIRT

Investigations/forensics
Contacts privilégiés avec les utilisateurs impactés
Demande de soutien externe
Faut-il couper Internet ?

Jour J - 11h00

Déclenchement d'une cellule de crise DSI

Investigations/forensics
Contacts privilégies avec les utilisateurs impactés
Demande de soutien externe
Faut-il couper Internet ?

Jour J - 11h15

Déclenchement d'une cellule de crise Groupe

Communication vers les parties prenantes
ANSSI, Gendarmerie
Paiement de la rançon ?
Coupure d'Internet ?

Vos contacts :

Michael Bittan
Associé
Leader des activités I Cyber Risk Services
mbittan@deloitte.fr

Chloé Chabanol
Senior Manager
Cyber Risk I Crisis Management
cchabanol@deloitte.fr

PARTENAIRE OFFICIEL PARIS 2024 FRANCE2025

Deloitte
185, avenue Charles-de-Gaulle - 92524 Neuilly-sur-Seine Cedex