< EXERCICE DEFACEMENT >

FICHE EXERCICE

< EXERCICE DEFACEMENT >

DEFINITION

Le défacement est la modification d'une page web / d'un site, afin de partager de fausses informations ou de faire passer un message de revendication.

On considère que la compromission d'une page d'une organisation sur un réseau social peut indirectement avoir un effet similaire à un défacement - même s'il ne s'agit pas d'un défacement au sein du SI d'une organisation.

Il se distingue de la création d'un site miroir illégitime à des fins de fraude.

OBJECTIFS

- Tester la capacité d'une organisation à faire un « rollback » rapide sur un site institutionnel d'importance ;
- Tester la capacité à gérer la communication de l'organisation dans le cas de faux messages diffusés au travers d'un site défacé ;
- Tester la capacité à investiguer le périmètre de compromission potentielle et les interconnexions avec d'autres systèmes ;
- Tester la capacité de communication sans un des moyens de communication institutionnelle.

DURÉE

Cet exercice est généralement assez court et ne dépassera une poignée d'heures, à moins d'être combiné à un autre scénario.

PUBLIC VISÉ

Cellules opérationnelles : SI, SSI, Equipe communication, Equipes métiers dans des cas spécifiques (ex: sites e-commerce, SAV, etc.).
Externes : Prestataires de gestion de crise (réponse à incident, gestion informatique, cabinet de conseil en crise/ communication de crise) et/ou prestataires d'externalisation du SI (ex: prestataires d'hébergement web).

PRÉPARATION, RESSOURCES ET LOGISTIQUES

- Ce scénario peut être envisagé comme une sous-partie d'exercice pour ajouter de la complexité ou de la pression ;
- Pour plus de réalisme, il est envisageable de réaliser une copie du site défacé avec un exemple de modification ;
- En cas d'hébergement externalisé, il est utile de vérifier les moyens d'alerte du prestataire en charge du site.
- La pression médiatique doit être adaptée en fonction de l'effort attendu, car elle va être le principal facteur de pression dans un contexte d'impact métier limité ;
- Pour un scénario et un exercice plus ambitieux, il est recommandé de choisir un site avec des données personnelles et/ou des interactions clients.

< EXERCICE DEFACEMENT >

IMPACTS

Internes :

- Inquiétude des collaborateurs, pouvant conduire à un stress relatif ;
- Perte de confiance dans la sécurité du SI.

Externes :

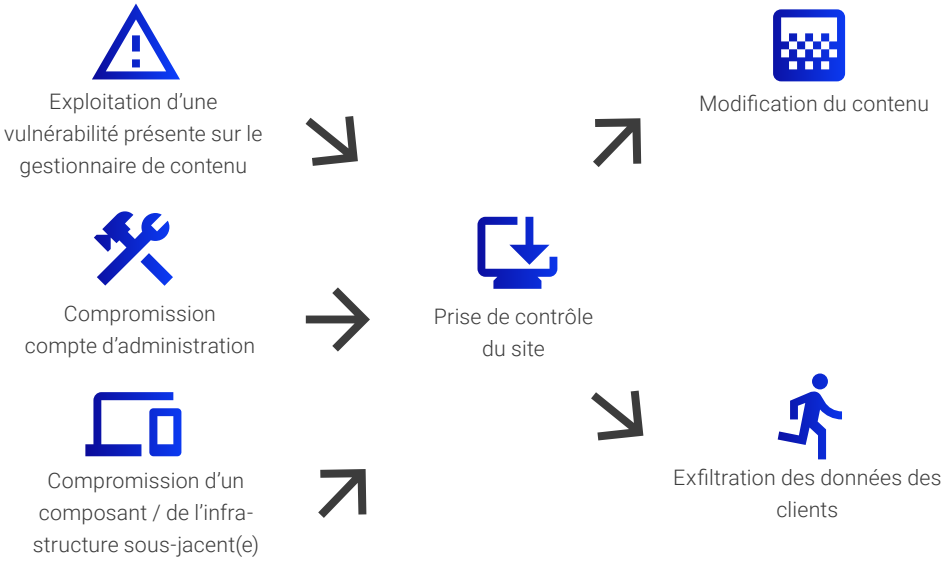
- Forte inquiétude des clients et partenaires sur la sécurité du SI, pouvant conduire à des actions préjudiciables à l'organisation (annulation de commandes, retraits d'argent, etc.) ;

ELÉMENTS ÉVALUABLES

- Evaluation de la chaîne d'alerte, notamment dans le cas de l'implication d'un prestataire ;
- Méthodologie d'investigation de l'origine de la compromission ;
- Nombres d'usages du site web couverts par des options alternatives (ex: vente, communication vers le grand public, etc.).

EXEMPLE D'UN SCENARIO D'ATTAQUE

Profil d'attaquants :
Hacktivistes, criminels souhaitant se déployer via un SI tiers ou faire de la fraude, script-kiddie/chercheur en sécurité.



PHASES DE L'EXERCICE

Ce type d'exercice est généralement assez court : il se concentre principalement sur la levée de doute et la remédiation des effets.

1. Phase de détection de la compromission / du défacement du site
2. Phase de gestion des effets (uniquement si le site a une importance métier)
3. Phase de remédiation et communication de crise

< EXERCICE DEFACEMENT >

BÉNÉFICES ATTENDUS

- Maîtrise de l'environnement SI autour du site défacé ;
- Renforcement de la sécurité des sites web de l'organisation ;
- Construction de *playbooks* de réponse à ce type d'attaque ;
- Identification de moyens de déploiement alternatifs de sites en cas d'urgence.

COMPÉTENCES DÉVELOPPÉES

- Gestion du stress pour les équipes concernées ;
- Capacité à identifier des sites miroirs utilisant du typosquatting (enregistrement d'un nom de domaine très similaire au site imité) ;
- Communication de crise sans une des chaines de communication officielles ;
- Compétences de remédiation du défacement selon les modalités d'attaque.

VARIANTES

Débutant : Atelier / Exercice sur table pour étudier une situation de compromission et construire des premiers réflexes.
Intermédiaire et avancé : A combiner au sein d'un exercice plus complexe.

POSSIBLES DIFFICULTÉS ET BIAIS

- Cet exercice est assez simple. Pour des organisations assez matures, il peut être compliqué d'en tirer une forte valeur ajoutée. Toutefois, d'autres aspects peuvent être considérés pour plus de complexité, tels que l'exfiltration de données ou l'envoi de messages malveillants en parallèle du défacement *(voir fiche correspondante)* ;
- Le scénario peut se concentrer sur la compromission d'un site en particulier. Toutefois, les moyens de déploiement de ce site peuvent être mutualisés à d'autres applications – nécessitant une justification sur l'absence d'extension du périmètre de compromission.

Contributeurs : Accenture, Airbus, ANSSI, BNP Paribas, Bouygues Telecom, Deloitte, ENEDIS, Française des Jeux, MACIF, Ministère de l'Intérieur et des Outre-Mer, Renault, SANOFI, Schneider Electric, SNCF, Technip Energies, Wavestone.

< Studio des Communs >

CAMPUS CYBER

POUR EN SAVOIR PLUS : WIKI.CAMPUSCYBER.FR
MAIL : COMMUNAUTES@CAMPUSCYBER.FR / 5 - 7 RUE BELLINI 92800, PUTEAUX

FICHE EXERICE - DEFACEMENT