< EXERCICE EXFILTRATION DE DONNÉES >

FICHE EXERCICE

< EXFILTRATION DE DONNÉES >

DEFINITION

L'exfiltration de données implique qu'un attaquant pénètre dans un Système d'Information (SI) afin d'en extraire discrètement des informations notamment à des fins de revente, d'espionnage, fraude ou de préparation d'attaques ultérieures. Ce scénario peut compléter le scénario d'attaque par ransomware où les données sont extraites avant le chiffrement du système.

OBJECTIFS

Il est important de définir l'enjeu principal de l'exercice : entraîner, tester, contrôler, identifier les manques... afin de définir les objectifs pédagogiques tels que :

- Valider les capacités de l'organisation à qualifier l'incident, réagir et mettre en place des mesures de remédiation ;
- Tester la capacité à identifier les données exfiltrées (nature, source, volume, origine, âge, etc.) ;
- Evaluer la criticité des données exfiltrées en s'appuyant le cas échant sur la politique de classification et de protection de l'information en vigueur dans l'organisation ;
- Vérifier la maitrise des obligations réglementaires en regard de la typologie des données exfiltrées et du secteur d'activité concerné (CNIL, régulateurs sectoriels, etc.) ;
- Mesurer la capacité à prendre en compte, prioriser et répondre aux attentes des différentes parties prenantes (employés, clients, fournisseurs, autorités, médias, etc.) ;
- Sensibiliser les participants à l'existence des risques liés au vol de données et à la nécessité de respecter les règles de protection de l'information de l'organisation.

DURÉE

Exercice court (2h) dans son format sur table. Toutefois, prendre en compte que si la partie qualification est jouée, elle peut prendre plusieurs heures.

PUBLIC VISÉ

L'organisation définit les acteurs à mobiliser selon le scénario.

Cellule décisionnelle : Comité de Direction, dont juridique, DPO, Communication, DSI, et les métiers concernés.
Cellules opérationnelles : Equipes représentées dans la cellule stratégique .
Externes : Prestataires et partenaires si la fuite simulée émerge d'un système externalisé.

PRÉPARATION, RESSOURCES ET LOGISTIQUES

Il est recommandé de s'appuyer sur les experts internes en regard du scénario.

- Pour un exercice plus réaliste, il est pertinent de préparer des bases de données / des fichiers à qualifier lors de la fuite. Une plateforme de simulation de fuites de données peut être utilisée. Attention, la récupération et la qualification des fichiers par les équipes peut prendre du temps !
- Pour complexifier l'exercice, introduire les enjeux liés à la fuite de données personnelles des collaborateurs (et les conséquences de cette fuite sur ces derniers) ;
- Utiliser un vecteur d'exfiltration déjà vécu ou connu voire un vecteur potentiel identifié et non encore utilisé.

< EXFILTRATION DE DONNÉES >

IMPACTS

Internes :

- Possible impact financier (amendes, mesures conservatoires ;
- Possible perte de confiance dans le SI ;
- Perte de confiance des collaborateurs ;
- Possible impact opérationnel durant la mitigation de l'attaque ;
- Perte d'avantages stratégiques.

Externes :

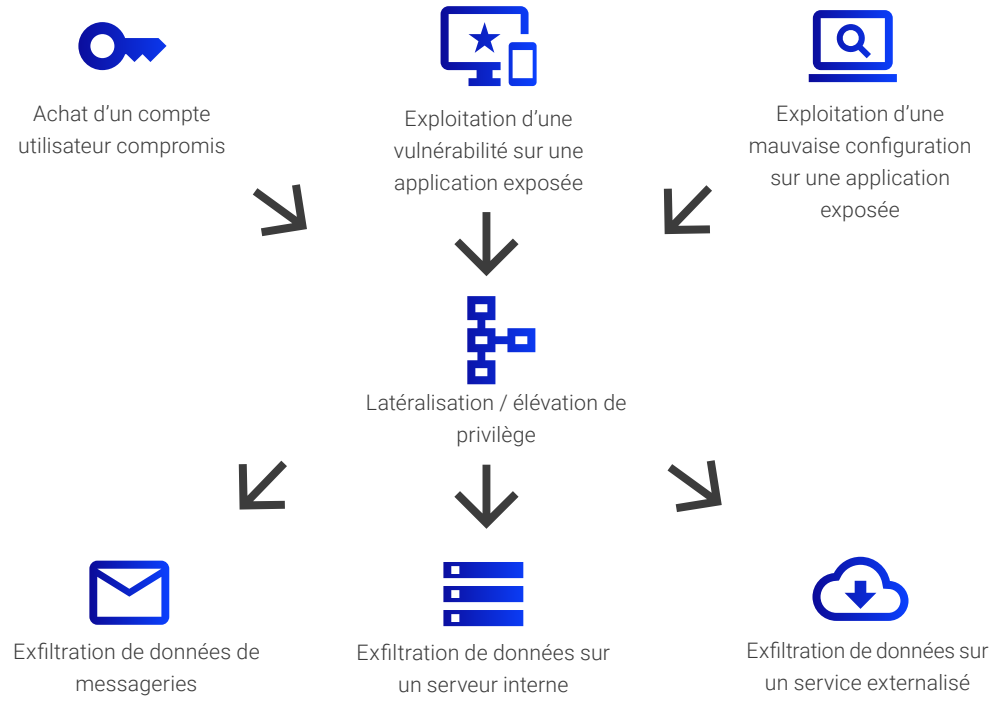
- Perte de confiance et d'image de partenaires, clients, investisseurs, etc. ;
- Non-conformité réglementaire/contractuelle et procédures judiciaires.

ELÉMENTS ÉVALUABLES

- Vitesse de qualification des données exfiltrées ;
- Précision de l'identification du périmètre de la fuite et des impacts ;
- Cadence et qualité des communications vers les parties prenantes ;
- Connaissance des procédures en place pour ce cas de figure.

EXEMPLE DE SCENARIO

Profil d'attaquants :
Concurrents, étatiques, cybercriminels, hacktivisme



PHASES DE L'EXERCICE

1. Phase de découverte de la fuite OU de la présence d'un attaquant sur le réseau ayant exfiltré les données
2. Phase de qualification de la fuite
3. Phase de communication et de mise en place de la réponse adaptée
4. Phase de restitution à chaud et à froid.

< EXFILTRATION DE DONNÉES >

BÉNÉFICES ATTENDUS

- Amélioration des processus de communication de crise ;
- Définition des listes des contacts à mobiliser ;
- Construction d'une liste des actifs et des données contenues, et mise-à-jour de la cartographie des données ;
- Définition de bonnes pratiques vis-à-vis de la protection des fichiers et données ;
- Amélioration du processus de qualification des données (notamment via de l'automatisation) ;
- Développement du volet disciplinaire en cas de fuite interne volontaire.

COMPÉTENCES DÉVELOPPÉES

- Capacité de qualification des données disponibles ;
- Communication de crise auprès des différentes parties prenantes ;
- Compétences légales dans la judiciarisation d'une fuite de données et dans l'apport de preuves nécessaires ;
- Compétences techniques concernant l'expulsion d'un acteur de la menace furtif sur un SI.

POSSIBLES DIFFICULTÉS ET BIAIS

- Cet exercice ne génère pas d'impact opérationnel à court terme, ce qui peut limiter la pression sur les équipes traitants le sujet. La pression médiatique et réglementaire est le curseur permettant de maintenir un niveau de pression suffisant ;
- Le type de données est également à un point d'attention : il est recommandé de ne pas jouer un exercice avec des données de production ou réelles. Des données pseudonymisées peuvent souvent s'avérer suffisantes pour atteindre les objectifs de l'exercice ;
- Il est nécessaire d'inciter les participants des cellules (en particulier de la cellule décisionnelle) à projeter l'impact de la fuite de données à la fois sur l'organisation mais également sur ses clients ou partenaires ;
- La qualification de la typologie de l'attaquant est également à ne pas oublier : elle peut avoir une influence forte sur l'utilisation qui sera faite des données exfiltrées.

VARIANTES

Débutant : Exercice sur table pour étudier une situation de compromission et acquérir les premiers réflexes.
Intermédiaire et avancé : Simulation pour travailler la récupération et la qualification des données.
Le volet technique de l'exercice peut être introduit progressivement selon la maturité de l'organisation.

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 - EXFILTRATION DE DONNÉES