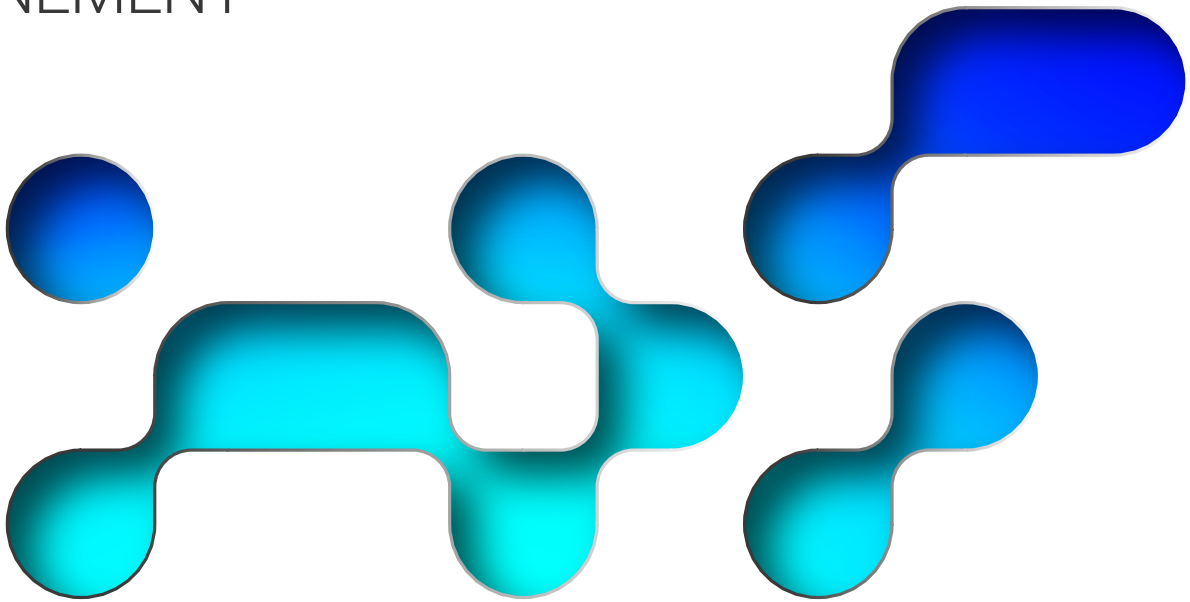
CAMPUS CYBER

FICHE MÉTHODE

CHAÎNE D'APPROVISIONNEMENT

GROUPE DE TRAVAIL : GESTION DE CRISE CYBER
ET ENTRAINEMENT



RÉPUBLIQUE FRANÇAISE
Liberté
Égalité
Fraternité

BANQUE DE FRANCE
EUROSYSTÈME

AMRAE
la Maison du risk management

CCA
Club de la Continuité d'Activité

CDSE
CLUB DES DIRECTEURS DE SÉCURITÉ DES ENTREPRISES

CESIN

CLUSIF

EXERCICE CHAÎNE D'APPROVISIONNEMENT

DÉFINITION

Une **attaque sur la chaine d'approvisionnement** (EN: Supply chain attack) est une attaque qui vise un **fournisseur de service ou partenaire.** Les attaquants visent par exemple à arrêter certains systèmes critiques ou à s'installer dans les systèmes à des fins d'espionnage, comme ce fût le cas dans l'attaque de SolarWinds.

OBJECTIFS

- **Impliquer son écosystème** de prestataires ou de tiers, et de tester notamment **les interconnexions et la stratégie d'isolation** (procédure « bouton rouge ») ;
- **Tester les sollicitations de contournement** de l'indisponibilité d'un prestataire (procédure « bouton vert ») ;
- **Tester l'interaction avec les écosystèmes industriel ou sectoriel** possiblement simulés par l'animation, et la **capacité à établir de la confiance** vers l'écosystème ;
- Tester la **communication immédiate** autour de la crise.
- **Sensibiliser** les métiers sur les dépendances à la chaîne d'approvisionnement

DURÉE

Selon type d'exercice – durée plus longue étant nécessaire dans le cas d'une campagne de mise à jour de vulnérabilité.
Nous préconisons d'organiser l'exercice sur une demi-journée, une journée pour un exercice plus ambitieux.

PUBLIC VISÉ

- **Cellule décisionnelle :** COMDIR, communication, juridique, métiers, fonctions centrales, avec intégration forte des équipes achats / commerciales pour gérer la relation avec le fournisseur et juridiques sur la répartition des responsabilités ;
- **Cellules opérationnelles :** SI, SSI, équipes métiers ;
- **Externes :** Fournisseurs, autorités, prestataires de réponse.

IMPACTS

Internes :

- Fuite de données / Compromission du SI ;
- Sabotage / Indisponibilité des services vitaux;
- Impacts financiers ou systémiques.

Externes :

- **Remise en question** par des partenaires dans la fiabilité de l'organisation ;
- Possible **impact juridique** en fonction des donées ou des services affectés .

PRÉPARATION, RESSOURCES ET LOGISTIQUES

Partir d'un service critique que l'on souhaite affecter, et **identifier les services sous-jacents** pouvant être compromis, via une cartographie des interdépendances.
Préparer des injects/réponses sur la présence et l'impact de la compromission d'un service numérique (notamment s'il est fictif) ;

- **S'inspirer d'attaques précédentes** pour construire le chronogramme en cohérence avec la menace. Il est plus intéressant de jouer vis-à-vis d'une technologie réelle, quitte à ne pas faire jouer le fournisseur ;
- Identifier **les moyens de communications** avec le fournisseur et **les SLAs** (accords de niveau de service) attendus. Si le fournisseur est impliqué : prévenir de l'existence d'un exercice, travailler sur les objectifs et le RACI du dispositif. Si le fournisseur n'est pas impliqué : identifier des ressources pouvant le simuler ;
- Si le scénario traite d'une vulnérabilité, il est possible d'utiliser un scan du parc pour **produire une cartographie** – uniquement pour les jeux avec simulation.

EXERCICE CHAÎNE D'APPROVISIONNEMENT

ELÉMENTS ÉVALUABLES

- **Vitesse de prise de contact** avec le fournisseur et informations communiquées ;
- **Capacité à identifier** un périmètre touché par la vulnérabilité / compromission d'un fournisseur.

Enjeux pouvant être évoqués et chantiers pouvant être lancés (suivi d'actions / valorisation des apprentissages de l'exercice) :

- Capacité à **repartir sur une base saine** préexistante du code du prestataire ;
- Capacité d'**audit et d'évaluation de la sécurité** d'une solution déployée par un fournisseur sur le SI ;
- **Audit des prestataires** présents sur le SI ;
- **Prise en compte des enjeux** de la chaîne d'approvisionnement dans les orientations et décisions prises.

VARIANTES

Thématique à privilégier pour des organisations industrielles (au sens large) et/ou matures.

Débutant : Test d'alerte / mobilisation avec un fournisseur (atelier / TTX).

Exercice technique / opérationnel, pour la cellule de crise cyber.

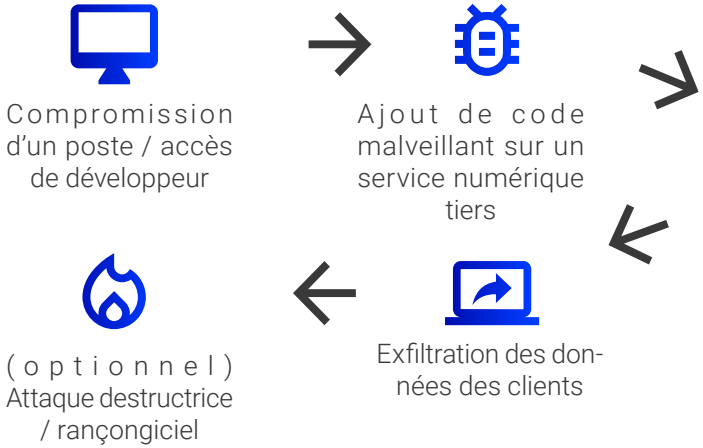
Expérimenté : Exercice multi-cellules avec opérationnelle et décisionnelle.

EXEMPLE DE KILL CHAIN

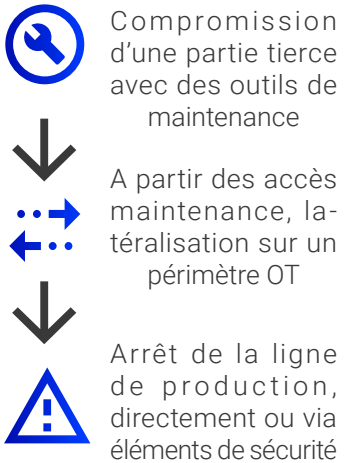
Profil d'attaquants :

Etatique ou supportés par un Etat, criminels souhaitant se déployer via un SI tiers ou faire de la fraude, hacktiviste

Compromission de la chaîne logicielle



Compromission de la chaîne OT



Phases de l'exercice

1. Phase d'annonce d'une compromission par un partenaire ou médias / d'une recommandation vis-à-vis d'une technologie par un régulateur / direction.
2. La détection n'est pas forcément interne – le produit sera peut être déjà indisponible avant la détection de l'attaque. Enjeu : signaux faibles et relations fournisseurs .
3. Identification des impacts SI et métiers, y compris en cas d'interactions avec la chaîne d'approvisionnement
4. Phase d'identification d'une solution de mitigation (avec/sans fournisseur).
5. Phase d'échanges avec l'écosystème pour informer les tiers sur la situation.

EXERCICE CHAÎNE D'APPROVISIONNEMENT

BÉNÉFICES ATTENDUS

- Développement de mode **dégradé** / mode de **contournement** avec les équipes métiers ;
- Identification de la documentation et de la cartographie manquante vis-à-vis des partenaires ;
- Développement de la **réponse à la perte d'un prestataire** ;
- Sensibiliser à l'**importance du partenaire** (pour sécuriser les liens ou identifier des alternatives) ;
- Identifier le **processus de communication** avec les fournisseurs (contacts, moyens, SLAs – accords de niveau de service) ainsi que des informations partageables ou non ;
- **Identification de risques juridiques** en cas de perte d'un partenaire ;
- Entrainement à la **remontée des sauvegardes** à large échelle ;
- Orchestration de la **reconstruction** ;
- Travailler sur les **interfaces du dispositif** de crise en place.

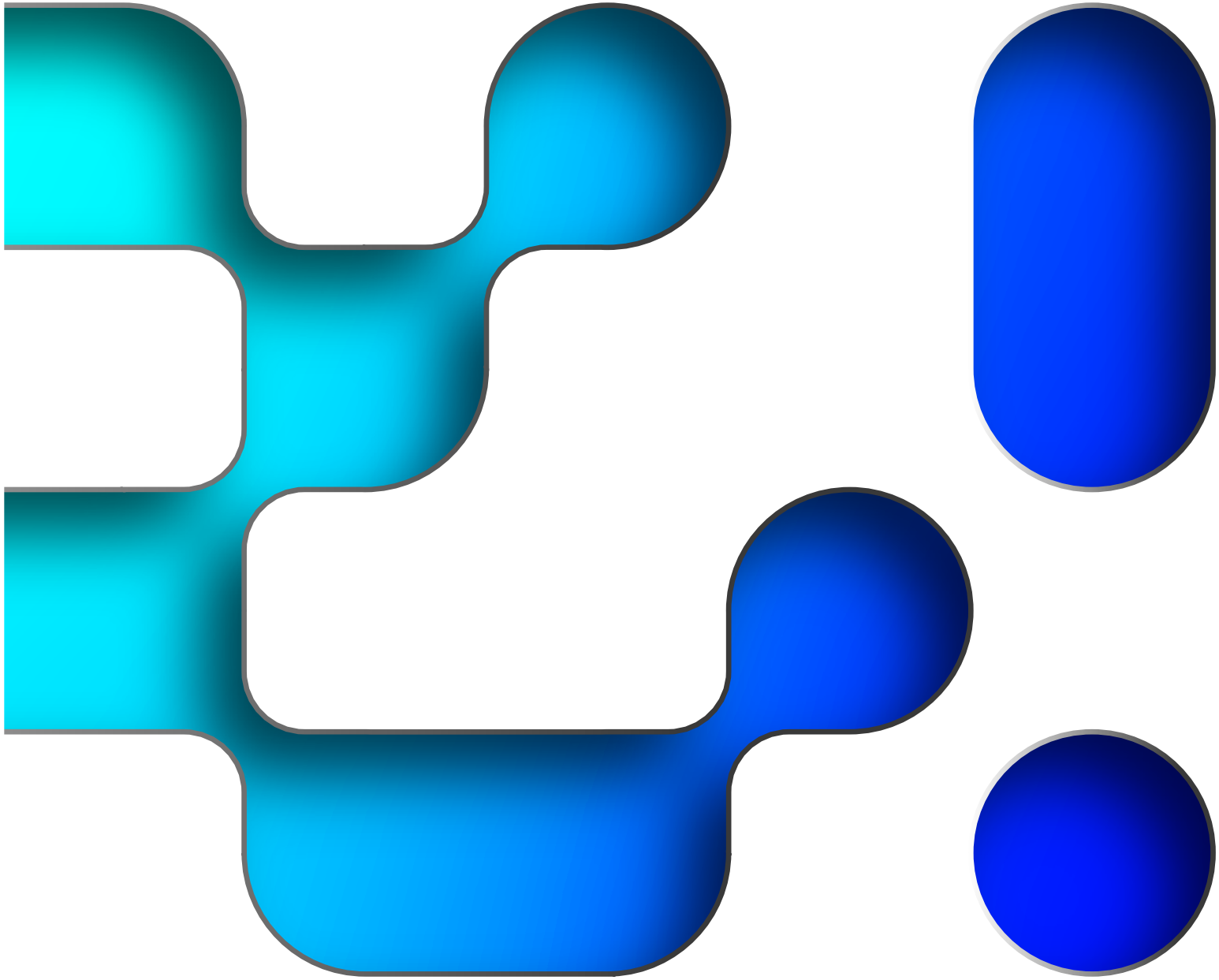
COMPÉTENCES DÉVELOPPÉES

- Maitrise de l'environnement SI, des interconnexions avec l'externe, des accès et privilèges des prestataires ;
- Compétences de communication avec des acteurs moins réguliers (fournisseurs, régulateur, fournisseur de CTI, etc.) pour consolider l'information sur la situation ;
- Capacité de collaboration avec l'écosystème (notamment au sein d'un secteur, de réseaux de coopération, etc.) ;
- Savoir assurer la mise en place d'un patch en interne et chez un partenaire / tiers ;
- Capacité à maitriser l'application d'un correctif en urgence sur un périmètre large ou difficile à établir.

POSSIBLES DIFFICULTÉS ET BIAIS

- Il est difficile d'identifier une brique logicielle sur le SI (si fictif, difficile de tirer des impacts sur lesquels on peut construire, si réel, demande un effort important pour avoir la cartographie) ;
- La confiance dans le fournisseur (documents, informations partageables, etc.) n'est pas toujours facile à évaluer– **la ségrégation de l'information est à définir en préparation** ;
- Le cas d'un service "en monopole", peut créer des difficultés pour la communication de crise (impossibilité de partager sur un incident tant que le service ne l'a pas fait). La taille du fournisseur peut avoir un impact dans la relation lors de l'exercice ;
- **Possible sentiment d'évaluation** pour le fournisseur – intérêt d'avoir une posture de co-construction s'il participe. **Eviter un exercice avec plus de deux** fournisseurs en même temps ;
- Pour certains services, il est possible de jouer de manière plus technique (isolation, restauration d'un code source non vérolé, etc.) sur un environnement test/backup ;
- Possible dépassement capacitaire du prestataire de par la multiplication des demandes vs ses ressources limitées (ex: prestataire de distribution de postes de travail, sur un impact très large, il sera impossible de trouver suffisamment d'experts car les prestataires sont dimensionnés pour le travail quotidien, pas pour une situation de crise) ;
- Prendre en compte les sujets de conformité avec des obligations réglementaires qui peuvent être non atteintes dans le cas du retour sur une version précédente plus à jour vis-à-vis des réglementations.

Contributeurs : Accenture, Airbus, ANSSI, BNP Paribas, Bouygues Telecom, Deloitte, Française des Jeux, SUEZ



CAMPUS CYBER
5 - 7 RUE BELLINI
92800
PUTEAUX

https://campuscyber.fr/