< EXERCICE SYSTÈMES INDUSTRIELS >

FICHE EXERCICE

< SYSTÈMES INDUSTRIELS >

DEFINITION

Un exercice « Système industriel » porte sur la compromission de l'environnement OT (Operational Technology). Ainsi, des équipements SCADA, automates, objets connectés, etc. de la chaine de production peuvent être touchés de par leur durée de vie, les normes spécifiques à respecter, la nature de leurs protocoles et les restrictions de mise-à-jour.

Ces attaques peuvent impacter les activités industrielles (production, traitement, logistique, pilotage, etc.), mais peuvent également conduire à un rebond vers le Système d'Information bureautique. Ces exercices peuvent être joués conjointement avec d'autres scénarios (notamment supply chain, rançongiciel, espionnage, etc.).

OBJECTIFS

- Sensibiliser les équipes opérationnelles aux conséquences des crises d'origine cyber ;
- Tester les plans de continuité d'activité sans outil informatique et le retour à la normale ;
- Affiner les processus de réponses et de reprise face aux menaces cyber ;
- Enrichir d'un volet cyber les réflexes en matière de sureté des équipements et des collaborateurs ;
- Renforcer les défenses et la protection des systèmes industriels ;
- Faciliter les interactions entre les équipes opérationnelles et informatiques.

DURÉE

Entre ½ et 1 jour.
Les plans d'urgence sûreté/sécurité sont présupposés être fonctionnels afin de se concentrer sur les spécificités cyber.

PUBLIC VISÉ

Cellule décisionnelle : Comité de Direction étendu, dont direction des sites industriels.
Cellules opérationnelles : Informatique bureautique et industrielle, Sécurité Informatique, Qualité, RSE, Continuité d'activité, Maintenance, Sûreté…
Externes : Prestataires des systèmes industriels, dont responsable de la maintenance.

PRÉPARATION, RESSOURCES ET LOGISTIQUES

- Le scénario doit être construit en prenant en compte les technologies en place et l'écosystème de prestataires. Pour ce faire, il est recommandé d'intégrer dans l'équipe d'organisation un expert interne des systèmes industriels et de leur cartographie ;
- Le scénario doit intégrer des enjeux techniques, stratégiques et commerciaux ;
- Une sensibilisation des équipes opérationnelles en amont de l'exercice est recommandée en cas de premier exercice de crise cyber, en présentant les impacts des possibles attaques ;
- Avec des ressources importantes, un « lab » virtuel peut être envisagé pour simuler le système industriel.

< SYSTÈMES INDUSTRIELS >

IMPACTS

Internes :

- Impact sur la sûreté, mise en danger des collaborateurs ;
- Arrêt de la production et pertes financières ;
- Vol de processus stratégiques (R&D, fabrication, etc.), fuite de secrets industriels.

Externes :

- Mise en danger de la population ou de l'environnement (secteur agroalimentaire, traitement d'eau, etc..) ;
- Perte de confiance, mesures conservatoires ;
- Dégradation de la réputation/image de l'organisation ;
- Non-conformité réglementaire ou contractuelle.

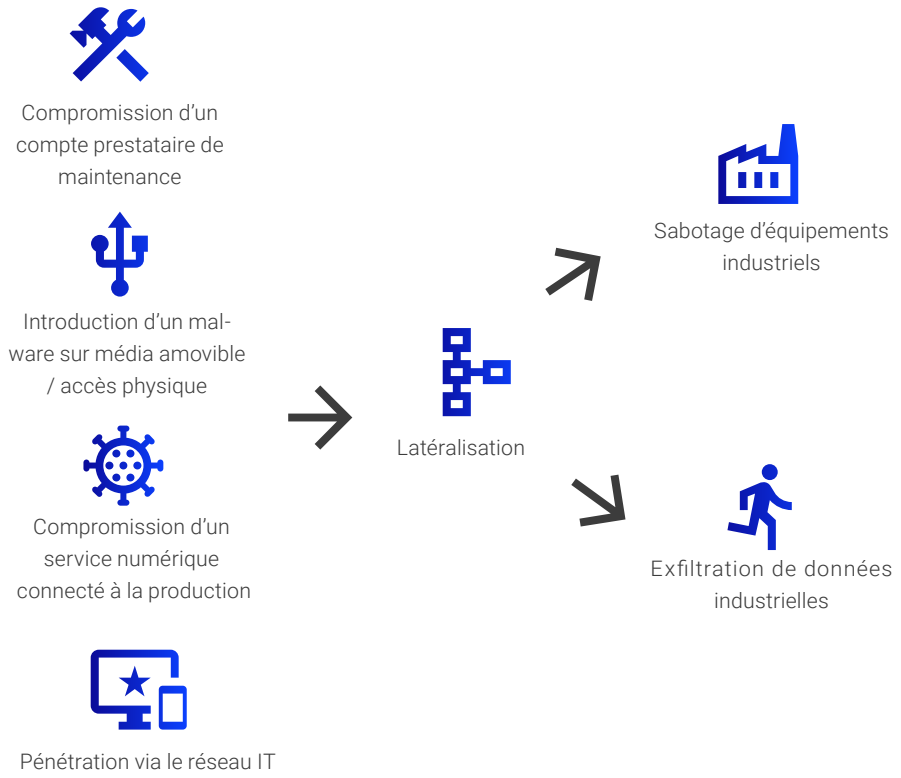
ELÉMENTS ÉVALUABLES

- Identification des temps d'indisponibilité / de remise en service de la chaine de production par les équipes
- Taux d'application des protocoles opérationnels et de sûreté industrielle en place
- Compréhension des aspects cyber par les équipes des systèmes industriels
- Identification des écarts entre les alertes outils de supervision numérique et les impacts opérationnels
- Temps de réponse / qualité de la réponse de la part des fournisseurs (si impliqués dans l'exercice)
- Ecarts vis-à-vis des normes existantes (dans un pays ou secteur donné)
- Flux de communication et processus d'escalade (du site vers le régional, du régional vers le central et entre équipes bureautiques et industrielles)

EXEMPLE DE SCENARIO

Profil d'attaquants :

Etatiques / paraétatiques (pour les secteurs sensibles), espionnage industriel / concurrence, criminels, hacktivistes, insiders.



PHASES DE L'EXERCICE

1. Phase de détection de l'attaque
2. Phase de gestion des impacts physiques et industriels et investigation
3. Phase de mise sous contrôle via protocoles à suivre

< SYSTÈMES INDUSTRIELS >

BÉNÉFICES ATTENDUS

- Identification de dépendances métiers et des impacts marché/secteur en cas d'indisponibilité ;
- Identification de moyens de continuité d'activité métier ;
- Identification de potentielles faiblesses SSI de la chaine de production, de périmètres plus vulnérables ;
- Développement d'un plan d'action de sécurisation ;
- Sensibilisation des équipes de production / opérationnelles, parfois non acculturées aux aspects de sécurité informatique ;
- Amélioration des processus de gestion de crise.

COMPÉTENCES DÉVELOPPÉES

- Compréhension des technologies OT (IIoT, convergence IT / OT, SCADA, etc.) ;
- Compétences techniques : durcissement / configuration des machines/systèmes OT ;
- Appropriation des plans de continuité d'activité en place ;
- Compréhension de l'impact des cyberattaques sur les systèmes industriels ;
- Coordination entre les équipes de secteurs/acteurs différents (équipes opérationnelles, directeur d'usine, équipe de sécurité, équipes informatiques) ;
- Développement de réflexes de sureté dans un contexte de non-contrôle de l'informatique.

POSSIBLES DIFFICULTÉS ET BIAIS

- Difficulté de mobiliser les parties prenantes décisionnelles, opérationnelles et techniques afin de conduire un exercice de gestion de crise de bout en bout ;
- Manque de formalisation/standardisation des processus au sein d'une usine/environnement industriel ;
- Nécessité de maintenir l'activité industrielle réelle, impossibilité de réaliser de vraies simulations techniques (impacts financiers, opérationnels, etc.) ;
- Dépendances fortes vis-à-vis des tierces parties (prestataires, fournisseurs de service, politiques) ;
- Pour les entreprises sensibles, nécessité de faire appel à des personnes ayant des habilitations spécifiques ;
- Limites techniques et expertises nécessaires dues à la nature des machines/systèmes industriels.

VARIANTES

Débutant : Sensibilisation ou exercice sur table pour découvrir les impacts des crises d'origine cyber (dépendant des exigences sectorielles).
Confirmé : Simulation avec un scénario spécifique (appel de personnel sur sites ; partie prenante opérationnelle incluse).

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 - SYSTÈMES INDUSTRIELS