

ENTREPRISES

RÉFLEXES CYBER +

Lancement/Bilan

LANCEMENT

**Merci d'être présents pour participer à la simulation
RÉFLEXES CYBER, un dispositif de jeu de rôle, ludique et
sérieux conçu par l'Agence nationale de la sécurité des
systèmes d'information (ANSSI).**

1. Pourquoi participer à cette session ?

Il est courant de penser que les cyberattaques sont uniquement l'affaire des équipes informatiques.

En cas d'incident, ce ne sont pourtant pas eux qui communiqueront vers les clients ou les administrés pour indiquer que des services ne peuvent plus être rendus. Ils ne décideront pas non plus de ce qui doit être remis en marche le plus rapidement possible.

Aujourd'hui, **les liens entre les métiers doivent donc se renforcer**, et chacun doit prendre conscient du risque cyber et de ses potentiels impacts pour son organisation.

LANCEMENT

1. Pourquoi participer à cette session ?

RÉLEXES CYBER vous invite, pendant quelques heures, à expérimenter les conséquences réelles d'une cyberattaque sur une organisation.

L'objectif est double :

1. Vous démontrer que la cybersécurité est un **enjeu essentiel pour le fonctionnement** d'une organisation et qu'il est important de se préparer à la survenue d'une cyberattaque.
2. Vous partager, à l'issue de la session, des conseils et bonnes pratiques pour **adopter les bons « Réflexes Cyber »** en cas d'attaque.

2. Programme

À titre indicatif, voici les **moments clés** de la session.

- **Début du jeu :h.....**
- **Fin du jeu :h.....**

Pause de 5 minutes

- **Début du débriefing :h.....**
- **Fin de la session :h.....**

LANCEMENT

3. Comment se positionner en tant que joueur ?

Vous allez prendre **le rôle de directeurs et directrices** d'une branche ou d'un service d'une **organisation fictive**.

Chacun d'entre vous se verra **confier au hasard une carte rôle** détaillant vos missions. Vous êtes invités à vous glisser dans ce rôle en respectant le cadre défini.

En cas de questions, vous pouvez vous tourner vers la personne chargée d'animer la séquence.

Jouez le jeu, même si le rôle ne vous satisfait pas pleinement !

4. Comment se déroule la simulation ?

Avec vous, une ou plusieurs personnes chargées de l'animation simuleront une situation de crise cyber et distribueront tout au long de la séquence **des cartes évènements** pour « pimenter » le jeu.

Vous les recevrez sous **format (fictifs) d'appels, de SMS ou de mails.**

Réagissez à ces évènements tout au long du jeu.

4. Comment se déroule la simulation ?

Pour cela, vous pouvez **échanger entre vous, vous organiser ou encore interroger** les personnes en charge de l'animation dans le cas où vous auriez besoin de précisions sur la situation, ou vous voudriez partager une action.

Attention, en tant que responsable métiers, vous n'êtes pas en charge de la mise en œuvre directe des actions.

Vous êtes invités à **donner des orientations à vos équipes fictives**, qui sont simulées par l'animation. C'est donc votre interlocuteur clé pour faire avancer la situation.

4. Comment se déroule la simulation ?

Enfin, n'hésitez pas à **organiser des points de situation** et à **ne pas surréagir** aux évènements, qui seront nombreux.

Tout au long du jeu, une ou plusieurs personnes assureront un **rôle d'observation** en vue de noter et d'analyser vos actions et réactions.

Elles ne sont pas là pour vous juger, mais pour prendre note de certains détails afin de vous aider à tirer les meilleurs enseignements de cette expérience.

5. Comment se clotûre la session ?

La simulation se clôturera par **un temps de débriefing**.

Vous pourrez vous exprimer pour partager ce que vous avez retenu de cette session.

Les personnes en charge de l'observation partageront aussi leurs retours et quelques conseils proposés par l'ANSSI.

Rappelons enfin que cette séquence a un **objectif pédagogique** : vous ne serez pas jugés pour vos actions et décisions. L'animation et l'observation veilleront à maintenir un **climat bienveillant**, et nous vous invitons à en faire de même.

MISE EN SITUATION

Nous sommes le dernier lundi du mois de février.
Il est 9h du matin.
Vous allez débiter la réunion de direction hebdomadaire.

Vous représentez les responsables d'une PME de 70 collaborateurs, spécialisée dans la gestion d'une plateforme logistique pour des clients industriels et commerciaux. Votre entreprise assure la gestion des flux de marchandises, le stockage, et la livraison pour de nombreux clients, dont certains acteurs majeurs de l'e-commerce.

Contexte socio-économique

Votre entreprise a connu une forte croissance ces dernières années, portée par l'essor de l'e-commerce. **Vous avez atteint un chiffre d'affaire de 7 millions d'euros l'année dernière.**

Mais la **hausse des coûts** énergétiques et des matières premières **pèse sur vos marges**. Vous avez récemment investi dans une nouvelle flotte de véhicules électriques pour réduire vos coûts opérationnels, mais cet investissement a fragilisé votre trésorerie.

En interne, **les employés sont mécontents** des conditions de travail, notamment des horaires prolongés, du manque d'ergonomie sur certains postes et des cadences imposées par la forte demande. Plusieurs d'entre eux menacent de faire grève si des mesures ne sont pas prises rapidement.

Contexte numérique 1/2

Dans le but de se moderniser, **votre entreprise a mené un chantier de transformation numérique** il y a 2 ans. Elle a été menée avec le soutien d'un prestataire informatique. Le maintien en condition opérationnel est aujourd'hui assuré en interne.

Les outils suivants sont hébergés **sur les serveurs internes** (les baies informatiques sont installées au sein de l'entreprise) :

- Le site internet.
- Le système de gestion logistique (type ERP), qui prend la forme d'une logiciel interne développé pour gérer les stocks, les commandes, les expéditions et les retours. Il est intégré avec les systèmes des clients pour automatiser les flux d'informations.
- L'outil de gestion des ressources humaines (gestion des paies, des congés et des absences).
- Certains fichiers internes (la migration est en cours sur le Cloud).

Contexte numérique 2/2

L'entreprise utilise un **serveur de messagerie en mode SaaS** (type Office 360, Google Workspace, ...).

Un antivirus et un pare-feu ont été installés pour protéger les actifs de la commune. Un audit a récemment démontré que les actions de prévention étaient insuffisantes. Le plan d'action n'a pas encore été validé

BILAN

Bravo de vous être prêtés au jeu !

BILAN

La simulation de crise que vous venez de vivre a eu pour objectif de vous familiariser aux conséquences d'une cyberattaque.

Très concrètement, le groupe attaquant a réussi à déployer un logiciel malveillant pour chiffrer – à savoir rendre inaccessibles - les données nécessaires au bon fonctionnement des activités de votre organisation.

Ces données ont également été volées avec l'objectif de les revendre.
Pour éviter cela, le groupe d'attaquant vous a proposé de payer une rançon.

1. Comment partager ses retours d'expérience ?

Il vous est maintenant proposé de participer à une séquence de débriefing en 2 temps :

1. Un retour d'expérience des joueurs et de l'observateur sur 3 thématiques ;

- Les joueurs sont invités à prendre la parole pour partager leurs impressions – **1 à 2 min par joueur**
- L'observateur prend ensuite le relais – **4-5 min.**

2. Les conclusions de l'exercice et les actions à venir.

BILAN

1. Avez-vous réussi à organiser votre dispositif de crise ?

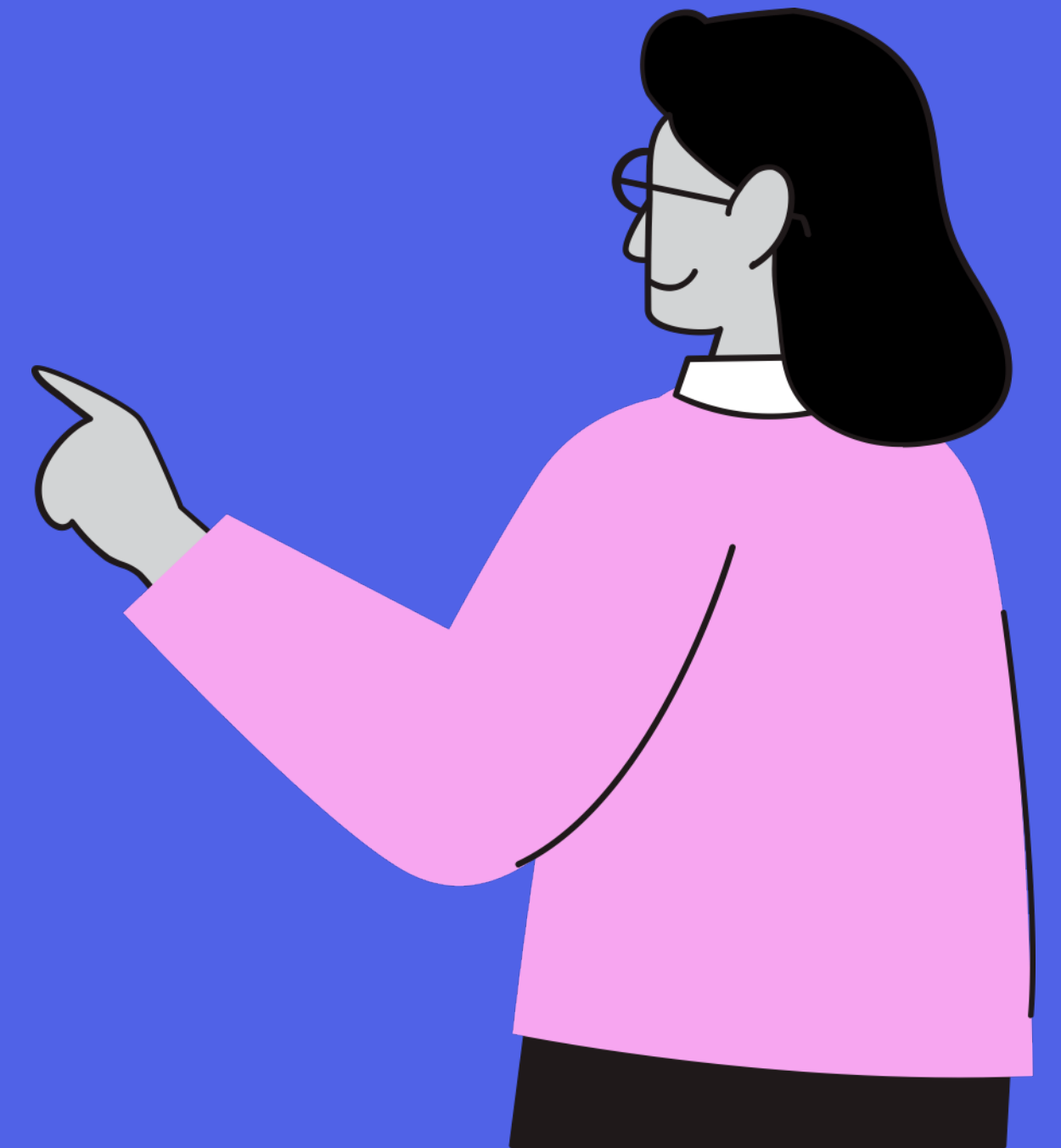
- Des points de situation ont-ils été réalisés ?
- La cellule a-t-elle utilisé des outils (ex : main courante) ?
- Des difficultés ont-elles été rencontrées ?

2. Les impacts de la crise ont-ils été identifiés ? Des premières solutions ont-elles été proposées pour y faire face ?

- Des soutiens extérieurs ont-ils été sollicités ?
- Des difficultés ont-elles été rencontrées ?

3. Une communication claire sur la situation a-t-elle été partagée ?

- Le personnel a-t-il été informé de la situation ? Des consignes ont-elles été données ?
- Les parties externes ont-elles été informées de la situation ?
- Les autorités ont-elles été prévenues voire impliquées ?



2. En conclusion

Les **conséquences** de l'attaque ont été **immédiates et nombreuses** :

- Arrêt des activités,
- Impossibilité de délivrer des services
- Pertes financières
- Perte de confiance.

Pour limiter les impacts, une **organisation de crise** a dû être mise en place rapidement.

Le travail initié par les équipes va encore durer plusieurs semaines voire plusieurs mois : lorsque tout est à l'arrêt et qu'on ne peut plus avoir confiance dans son informatique, **la gestion d'une cyberattaque s'apparente à un marathon...**

2. En conclusion

Pour tenir dans le temps, il est nécessaire de **bien s'organiser**, de **s'entourer** et de **prendre les décisions** qui semblent les plus adaptées au contexte social, économique voire politique de l'organisation.

Mais **savoir bien réagir** n'est qu'un des volets de ce qu'on appelle la cybersécurité.

Pour que votre organisation soit **plus résiliente face aux attaques**, il faut nécessairement **mettre en place des outils et procédures** qui permettent de se protéger de ce risque.

2. En conclusion

Mettre à jour ses systèmes, paramétrer ses boîtes mail pour se protéger du phishing, activer son antivirus, sont autant de bonnes pratiques à suivre pour renforcer sa sécurité.

Il est aussi important de savoir détecter des tentatives d'intrusion, des mails frauduleux, pour pouvoir mettre en place des actions de protection.

La cybersécurité ne relève pas de la seule responsabilité des équipes informatique ou des prestataires : être vigilant sur le contenu du mail, utiliser des mots de passe forts, savoir qui contacter en cas de situation anormale sont des actions à la portée de tous les collaborateurs.

3. Pour aller plus loin

Pour initier une **stratégie de cybersécurité**, l'ANSSI vous propose maintenant de passer un second cap grâce à **3 actions clés** :

1. **Téléchargez les Fiches Réflexes** indiquant quels premiers gestes suivre en cas d'incident et diffusez-la au sein de votre organisation !
2. **Complétez les modèles fournis** pour recenser les numéros utiles à joindre en cas d'attaque.
3. **Poursuivez votre montée en maturité sur messervices.cyber.gouv.fr**, la plateforme des services et ressources cyber gratuits pour vous aider et pour commencez à améliorer votre maturité cyber.

Depuis ce site, demandez votre **diagnostic cyber gratuit** accompagné par un Aidant cyber qui vous permettra d'identifier **6 actions simples et rapides** pour vous protéger contre les cyberattaques.



Merci pour votre participation !