

COMMUNIQUÉ DE PRESSE

Paris, le 06/12/2021

CRISE CYBER : UNE COLLECTION DE GUIDES POUR S'ENTRAÎNER, GÉRER ET COMMUNIQUER

Face à la recrudescence de la menace cyber, les organisations, entreprises et institutions doivent se préparer à faire face et apprendre à réagir pour maintenir leurs activités en cas de d'attaque informatique. L'ANSSI propose trois guides complémentaires afin d'appréhender pas à pas la gestion de crise cyber et ainsi faciliter la prise de décision.

Toutes les organisations, y compris les plus sécurisées, peuvent connaître une cyberattaque. La crise d'origine cyber peut engendrer une paralysie majeure, avec, entre autres, l'arrêt des activités, l'impossibilité de délivrer des services, l'exfiltration de données sensibles et des pertes financières lourdes. Ces bouleversements soudains et aux impacts incertains forcent, dans l'urgence, les organisations à s'adapter et à fonctionner de manière dégradée. Source de stress, cette crise complique la prise de décision rapide, pourtant vitale pour en limiter les impacts. L'anticipation et la préparation des entreprises et institutions, qui font souvent défaut, s'avère d'une nécessité absolue. Face à ce constat, et pour aider les organisations à faire face aux attaques informatiques, l'ANSSI publie une collection de guides sur la crise. Deux nouvelles publications « *Crise d'origine cyber : les clés d'une gestion opérationnelle et stratégique* » et « *Anticiper et gérer sa communication de crise cyber* » viennent compléter le guide « *Organiser un exercice de gestion de crise cyber* » paru en 2020. Destinés aux dirigeants, aux responsables de la sécurité, aux gestionnaires des risques et des crises ainsi qu'aux communicants, ces trois guides complémentaires permettent d'appréhender les différents enjeux et de faciliter la prise de décision.



Anticiper et gérer avec sérénité les impacts de la crise cyber

Le guide « *Crise d'origine cyber : les clés d'une gestion opérationnelle et stratégique* » - réalisé en partenariat avec le Club des directeurs de sécurité des entreprises (CDSE) - a pour objectif de partager des bonnes pratiques et des recommandations à toute organisation souhaitant se préparer à réagir efficacement à une crise cyber. Construit notamment grâce aux retours d'expérience d'organisations, publiques comme privées, ayant été ciblées par une cyberattaque, ce guide propose de nombreux conseils en lien avec les préoccupations des équipes impliquées dans la gestion de la crise.

Ces recommandations insistent par ailleurs sur la nécessité de mobiliser des fonctions distinctes mais complémentaires dans les processus de préparation et de décision en temps de crise : le volet stratégique et opérationnel.

Les 18 fiches proposées dans ce guide permettent de présenter ce double point de vue sur les actions à mener dans les différentes étapes d'une gestion crise d'origine cyber afin de permettre une meilleure appréciation des enjeux des différentes parties-prenantes.

<https://www.ssi.gov.fr/guide/crise-dorigine-cyber-les-cles-dune-gestion-operationnelle-et-strategique/>



Communiquer grâce à une stratégie pré-définie

Même les plus aguerris des communicants ne sont pas à l'abri d'être déstabilisés lorsqu'une crise cyber surgit. Avec des codes, des enjeux et un écosystème parfois très différents de leur cœur de métier, les communicants doivent également maîtriser les réflexes et les outils à déployer pour faire face à la crise. En développant les spécificités liées au cyber, ce guide « *Anticiper et gérer sa communication de crise cyber* » - réalisé en partenariat avec Cap'Com - démontre qu'une bonne communication de crise cyber reprend avant tout une stratégie de communication de crise. Les conseils et les recommandations opérationnelles fournies dans ce guide se basent sur les situations rencontrées par l'ANSSI depuis sa création, grâce à son rôle d'assistance auprès de victimes.

Adaptées à la gestion de situations qualifiées de « sensibles », qui précèdent souvent une éventuelle crise médiatique, les recommandations se destinent à toute personne qui a un rôle clé à jouer en matière de gestion de crise.

Il vise également à donner des outils et des conseils à d'autres métiers, techniques et décisionnels, pouvant intervenir aux côtés des communicants.

<https://www.ssi.gov.fr/guide/anticiper-et-gerer-sa-communication-de-crise-cyber/>



S'entraîner pour déployer les bons réflexes

Afin que les entreprises et les institutions soient prêtes, il est aussi primordial de s'entraîner de manière transverse, en associant aussi bien les directions métier, les dirigeants et les employés que les experts cyber. Le guide « *Organiser un exercice de gestion de crise cyber* », réalisé en partenariat avec le Club de la continuité d'activité (CCA) vise ainsi à accompagner, pas à pas, les organisations dans la mise en place d'un exercice vraisemblable et formateur, pour les joueurs comme pour les organisateurs.

Plus particulièrement, il s'adresse à toute personne souhaitant mettre en place un exercice de niveau décisionnel visant à entraîner la cellule de crise stratégique de son organisation. Afin de pouvoir être utilisé et adapté par le plus grand nombre, il comporte un exemple complet d'exercice de crise sur la thématique de l'attaque par rançongiciel. L'exercice est construit en quatre étapes, qui sont explicités et illustrés par des fiches pratiques.

« Une attaque enrayée par une bonne préparation ne fait pas de bruit ! Aujourd'hui, le risque est bien réel et le manque d'anticipation, souvent dévastateur. Le vol de données, la paralysie partielle ou totale des services numériques ont des impacts opérationnels, juridiques, financiers et réputationnels absolument critiques. La préparation, l'outillage, l'entraînement sont donc indispensables pour protéger l'activité en cas d'attaque informatique. Fruit d'une riche expérience, développée au fil des années par l'ANSSI et ses partenaires, ces guides ont vocation à vous accompagner face à une menace cyber croissante ». explique Guillaume Poupard, Directeur Général de l'ANSSI.

<https://www.ssi.gov.fr/guide/organiser-un-exercice-de-gestion-de-crise-cyber/>

Demain, les entreprises et institutions qui maîtriseront le risque numérique et qui auront la capacité de se relever d'une crise d'origine cyber seront génératrices de confiance. Ces guides, fruit de l'expérience de l'ANSSI, de ses partenaires et de victimes de cyberattaques, aideront les organisations à se préparer efficacement face à la menace cyber.

À PROPOS DE L'ANSSI

L'Agence nationale de la sécurité des systèmes d'information (ANSSI) a été créée par le décret n°2009-834 du 7 juillet 2009 sous la forme d'un service à compétence nationale.

L'agence assure la mission d'autorité nationale en matière de défense et sécurité des systèmes d'information. Elle est rattachée au secrétaire général de la défense et de la sécurité nationale, sous l'autorité du Premier ministre.

AGENCE NATIONALE DE LA SÉCURITÉ DES SYSTÈMES D'INFORMATION
ANSSI - 51, boulevard de la Tour-Maubourg - 75700 PARIS 07 SP

www.ssi.gouv.fr - presse@ssi.gouv.fr



Contacts Presse

Roxane ROSELL
roxane.rosell@ssi.gouv.fr
06 49 21 63 80

presse@ssi.gouv.fr