RÉPUBLIQUE FRANÇAISE
Liberté
Égalité
Fraternité

COMMUNIQUÉ DE PRESSE

Paris, le 16/01/2024

COMMENT REMÉDIER À UNE CYBERATTAQUE ? L'ANSSI PUBLIE SA COLLECTION DE GUIDES DÉDIÉS AU SUJET

L'Agence nationale de la sécurité des systèmes d'information (ANSSI) publie aujourd'hui trois guides dédiés à la remédiation d'incidents cyber. **Cette collection, première du genre et destinée aux acteurs de l'informatique et de la cybersécurité, est le fruit de l'expertise unique de l'agence dans ce domaine.** Au travers de ces guides, l'ANSSI partage sa doctrine et ses bonnes pratiques, élaborées à partir des interventions qu'elle mène depuis sa création auprès de victimes d'attaques informatiques.

Lorsqu'une cyberattaque a lieu : des choix structurants à effectuer

Après la détection d'une cyberattaque, la victime est souvent prise de court par les choix importants qu'elle doit faire, lui permettant de survivre et d'assurer la continuité de son activité. La remédiation est ce processus permettant l'éviction de l'attaquant, la reprise de contrôle du système d'information (SI) compromis et la reconstruction de ses services.

Suivant les priorités des entités attaquées, le choix peut être fait d'une remédiation rapide, assurant la remise en activité de services touchés mais dont le niveau de sécurité, d'abord faible, sera à consolider dans la durée. Une seconde alternative, plus longue, consiste en une reprise totale du contrôle du SI ; plus efficace dans le temps, celle-ci vise un niveau de sécurité plus élevé.

« *Bien pilotée, et suivie à haut niveau dans l'organisation, la remédiation peut devenir une véritable opportunité d'amélioration significative de la résilience de l'organisme qui subit une cyberattaque.* » explique ainsi Emmanuel Naëgelen, le directeur général adjoint de l'ANSSI.

Cette résilience est cruciale car bien souvent, les victimes identifiées comme cibles d'intérêt feront l'objet de tentatives de cyberattaques ultérieures. Ainsi, récemment, une entité a effectué une remédiation incomplète lui ayant néanmoins permis d'augmenter son niveau de détection. Lorsque l'attaquant s'est à nouveau manifesté, il a pu être décelé aussitôt et une seconde remédiation menée avec l'ANSSI a permis de l'évincer. La troisième tentative de retour a été détectée et contenue grâce à la réorganisation du SI réalisée précédemment.

RÉPUBLIQUE FRANÇAISE
Liberté
Égalité
Fraternité

Un corpus de guides pour accompagner les organisations à chaque étape

« *Fruit d'une riche expérience dans l'intervention auprès de victimes d'incidents de cybersécurité, l'ANSSI donne dans cette collection les clés pour aider les dirigeants mais également les équipes techniques et opérationnelles à maîtriser ce type d'incident.* » poursuit Emmanuel Naëgelen. Engagée aux côtés de son écosystème cyber, l'agence a travaillé à l'élaboration de trois guides s'articulant ainsi :

- **Un volet stratégique qui présente les enjeux de la remédiation** et apporte les clés de décision nécessaires aux dirigeants dans la détermination des objectifs et la sélection du plan de remédiation ;
- **Un volet opérationnel qui dévoile les principes du pilotage et de la mise en œuvre** du projet de remédiation, tout en apportant des outils opérationnels aux responsables des équipes techniques ;
- **Un volet techn**ique qui détaille l'accomplissement technique de la remédiation : il contient pour l'instant un document présentant les actions d'investigation, d'éviction et de supervision du Tier 0 Active Directory[1] afin de reprendre le contrôle d'un système d'information.

La remédiation : un enjeu clé pour tous

Si l'ANSSI développe aujourd'hui sa collection de guides autour de cette compétence unique, c'est pour ajouter une pierre importante à l'édifice de la réponse à incident cyber. En effet, la remédiation s'impose, avec l'investigation et la gestion de crise – à laquelle l'agence a déjà dédié trois guides – comme l'une des dimensions majeures de la réponse aux cyberattaques. À l'approche des Jeux olympiques et paralympiques 2024, cet enjeu concerne l'écosystème cyber dans son ensemble. L'agence propose donc de partager son expérience en matière de remédiation avec les prestataires afin de faire monter en maturité l'offre privée en matière de remédiation. Cette collection, construite pour et avec la communauté cyber, a intégré ses retours, reçus lors de l'appel à commentaires public lancé en avril 2023. Il a vocation à s'enrichir progressivement de nouveaux contenus.

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

cyber.gouv.fr

[1] L'Active Directory est un service d'annuaire introduit par Microsoft qui permet de centraliser des informations relatives aux utilisateurs et aux ressources d'un SI. Cœur de confiance de l'Active Directory, le Tier 0 Active Directory contient l'ensemble des ressources ayant un contrôle sur les identités de l'entreprise et donc sur l'ensemble des ressources intégrées à l'Active Directory.

RÉPUBLIQUE FRANÇAISE
Liberté
Égalité
Fraternité

Contacts Presse

presse@ssi.gouv.fr
06 49 21 63 80

Roxane ROSELL
roxane.rosell@ssi.gouv.fr

Leila LEGRAND
leila.legrand@ssi.gouv.fr

Victor PLOUÉ
victor.ploue@ssi.gouv.fr