III

ENSEIGNEMENTS DES INCIDENTS ET ACTIONS DE PRÉVENTION

A
ENSEIGNEMENTS TIRÉS DES INCIDENTS

Nous pouvons tirer de nombreux enseignements des incidents traités par les CSIRT territoriaux. Le principal enseignement est que la majorité des attaques opérées par les acteurs criminels et observées par les CSIRT territoriaux peuvent être évitées avec l'adoption de mesures d'hygiène de cybersécurité adaptées.

LA PLUPART DES CYBERATTAQUES PEUVENT ÊTRE ÉVITÉES AVEC L'ADOPTION DE MESURES D'HYGIÈNE DE CYBERSÉCURITÉ ADAPTÉES

Ce constat est une bonne nouvelle car il montre que les cyberattaques ne sont pas une fatalité et que ce risque peut être géré. Il souligne néanmoins en creux le déficit de maturité notamment des entités de taille petite et moyenne en cybersécurité, constat connu et partagé par la communauté des experts en cybersécurité.

L'un des facteurs aggravants lors de la survenue de cyberattaques est l'absence de données de sauvegardes saines, le plus souvent par l'absence de sauvegardes hors ligne. Cela engendre une perte souvent quasi nette du patrimoine informationnel de l'organisation victime qui la met gravement en péril.

Nous constatons également souvent l'absence ou l'insuffisance de solutions de sécurité déployées pour détecter et répondre à une menace. A cette fin, le déploiement d'une solution technologique de type *Endpoint Detection & Response* constitue une réponse abordable et efficace qui permet de détecter au plus tôt les menaces et en particulier les acteurs de rançongiciel. En cas d'incident avéré, elle offre également une capacité à répondre plus efficacement à l'échelle d'un parc informatique complet.

Enfin, dans de nombreux incidents, le vecteur d'intrusion a été l'exploitation de vulnérabilités de logiciels ou d'équipements de bordure de réseau exposés sur internet. Un simple processus de gestion des vulnérabilités aurait pu éviter un grand nombre de ces incidents.

B
BONNES PRATIQUES POUR SE PRÉMUNIR DES INCIDENTS LES PLUS COURANTS

Face à la multiplication des attaques, l'ANSSI a identifié 5 mesures clés pour protéger efficacement un système d'information et limiter l'impact des cyberattaques lorsqu'elles surviennent. Ces actions constituent les mesures d'hygiène de cybersécurité adaptées pour la plupart des organisations.

L'expérience des CSIRT territoriaux montre qu'avec l'adoption de ces mesures, et en y incluant un processus de gestion des vulnérabilités et de la surface d'attaque, une très grande proportion de ces attaques pourrait être arrêtée.

- RENFORCER LA SÉCURITÉ DE L'AUTHENTIFICATION VIA DES MÉCANISMES D'AUTHENTIFICATION MULTI-FACTEUR
- METTRE EN ŒUVRE UN SYSTÈME DE DÉTECTION MANAGÉ TEL LES SOLUTIONS EDR (ENDPOINT DETECTION & RESPONSE)
- SAUVEGARDER VOS DONNÉES ET APPLICATIONS CRITIQUES AVEC AU MOINS UNE COPIE HORS-LIGNE
- ÉTABLIR UNE LISTE PRIORISÉE DES SERVICES NUMÉRIQUES CRITIQUES ET PRÉPARER UN DISPOSITIF DE GESTION DE CRISE ADAPTÉ À UNE CYBERATTAQUE

C
INITIATIVES NOTABLES DE PRÉVENTION

Les CSIRT territoriaux ont réalisé des initiatives uniques ou spécifiques à leur territoire. Quelques exemples sont présentés ici.

Un exercice de gestion de crise cyber dans les Hauts-de-France en amont des Jeux Olympiques de Paris 2024

En mars 2024, un exercice de gestion de crise cyber a été organisé dans le cadre des Jeux Olympiques de Paris 2024, la métropole lilloise pouvant donc être une cible potentielle en accueillant des épreuves. Le CSIRT Hauts-de-France a ainsi réussi à mobiliser une trentaine de participants, incluant des acteurs clés tels que les acteurs étatiques sur le territoire dont la préfecture du Nord, les parties prenantes des Jeux Olympiques et les acteurs cyber locaux. Cet exercice visait à éprouver la mise en place d'une organisation de gestion de crise, tester des mesures stratégiques et opérationnelles, et évaluer la gestion du stress ainsi que la réactivité et la résilience des acteurs impliqués. L'exercice a été une réussite et cet événement a été salué par le préfet délégué pour la défense et la sécurité qui était présent lors de l'exercice. Cette simulation a permis de renforcer la préparation et la coordination entre les différents acteurs, essentielle pour assurer la sécurité des Jeux Olympiques.

Campagne de détection de vulnérabilités au profit des collectivités locales françaises

À l'initiative du CSIRT de la Région Bretagne, les CSIRT territoriaux français se sont unis pour mener une campagne de recherche en vulnérabilité au profit des collectivités locales. Cette campagne d'envergure a eu lieu en avril 2024, sur l'ensemble du territoire français. La campagne de recherche en vulnérabilités a été réalisée grâce à l'exploitation de bases de données publiques de l'administration. Ce ne sont pas moins de 25 000 noms de domaines d'entités publiques parmi les communes, intercommunalités, conseils départementaux, centres de gestion territoriaux et conseils régionaux qui ont été analysés. 186 entités publiques ont ainsi été identifiées comme présentant des équipements vulnérables à 311 failles critiques, parmi les 25 000 analysés, soit un taux de 0,73% du total. A la date du 26 juin, 25% des vulnérabilités identifiées en avril avaient été corrigées grâce à l'action coordonnée des CSIRT territoriaux.

Déploiement d'un service gratuit de scan de vulnérabilité en Grand Est

En complément du service gratuit d'assistance aux victimes de cyberattaques, le CSIRT de la région Grand Est a adopté un outil de scan de vulnérabilité, intégralement financé par la Région Grand Est, gratuit pour les bénéficiaires. Il peut être mis en œuvre, sur sollicitation du CSIRT, au profit de chaque organisation localisée sur le territoire. Il permet de déceler au plus tôt les défauts de sécurité et les vulnérabilités critiques visibles à partir de l'empreinte internet de chaque bénéficiaire. Ce service est pleinement opérationnel depuis juillet 2024. Une cinquantaine de scans ont été exécutés en 2024. Il permet de recueillir un premier indicateur pertinent concernant le niveau de cybersécurité d'un système d'information. Un rapport est délivré au bénéficiaire qui comprend un plan de remédiation avec des recommandations et des actions à conduire pour corriger les failles détectées.

Star-Hack, un défi avec des étudiants en Nouvelle-Aquitaine

Lancé en octobre 2024, le programme Star-Hack a débuté par un Capture The Flag (CTF) impliquant 15 écoles de Nouvelle-Aquitaine, où 70 étudiants ont obtenu le titre de Cadet Cyber du Campus. En novembre, ces cadets et leurs professeurs référents ont suivi des formations et entraînements intensifs. En décembre, les cadets ont été mis en relation avec des experts parrains, membres du campus. Le programme se poursuivra en 2025. À ce jour, 22 applications ont été testées, révélant 32 failles.

Les matinées de sensibilisation du CSIRT CyberCorsica

Le CSIRT CyberCorsica a initié des matinées de sensibilisation afin d'aller au plus près des territoires, notamment les plus isolés. L'objectif de cette initiative est d'apporter un service de proximité permettant de sensibiliser ses bénéficiaires aux risques numériques, aux enjeux et à la nécessité de tendre vers une maturité numérique. Aucune entité n'est à l'abri d'une cyber attaque peu importe sa taille et le lieu où celle-ci est implantée.

Un cycle d'événements dédiés à la cybersécurité, « L'appel du Cyber Juin » en Normandie

Le CSIRT normand, Normandie Cyber a coorganisé un cycle d'événements dédiés à la cybersécurité, « l'appel du Cyber Juin », initié par le délégué régional de l'ANSSI. Il organise également en lien avec les collectivités locales (EPCI) des demi-journées de sensibilisation incluant une partie de mise en relation directe avec des prestataires cyber régionaux au format B2B.

E
RÉALISATION DE DIAGNOSTICS *MON AIDE CYBER*

Les CSIRT territoriaux, en plus de leur action principale dans le champ de la réponse à incidents, sont également très actifs dans la prévention au travers notamment du dispositif déployé par l'ANSSI *Mon Aide Cyber*.

Les CSIRT territoriaux sont également engagés dans des opérations de sensibilisation déployées dans les territoires notamment à l'occasion du mois de la cybersécurité en octobre mais également tout au long de l'année.

31 salariés des CSIRT territoriaux sont référencés comme aidants dans le dispositif. Ces aidants ont réalisé 189 diagnostics en 2024.

MONAIDECYBER EST UN DISPOSITIF QUI A POUR OBJECTIF D'ACCOMPAGNER LES ENTITÉS PUBLIQUES, LES ASSOCIATIONS ET LES ENTREPRISES SOUHAITANT MENER UNE PREMIÈRE DÉMARCHE DE SÉCURISATION INFORMATIQUE. CE DISPOSITIF EST BASÉ SUR DES AIDANTS.

LES AIDANT DES CSIRT TERRITORIAUX ONT RÉALISÉS 189 DIAGNOSTICS MON AIDE CYBER, REPRÉSENTANT 7% DE L'ENSEMBLE DES DIAGNOSTICS RÉALISÉS.

MonAide Cyber
INNOVATION ANSSI

NOMBRE DE DIAGNOSTICS MONAIDECYBER RÉALISÉS PAR LES CSIRT TERRITORIAUX EN 2024