ARTICLE

L'ANSSI VIENT DE PUBLIER UN PANORAMA DE LA CYBERMENACE EN 2023. QUE FAUT-IL EN RETENIR À QUELQUES MOIS DU DÉBUT DES JEUX OLYMPIQUES ET PARALYMPIQUES EN FRANCE ?

Droit de la propriété intellectuelle, média et art | 29/02/24 | Florence Chafiol Alexandra Antalis

Lien vers le document : https://www.cert.ssi.gouv.fr/uploads/CERTFR-2024-CTI-001.pdf

Le niveau de la menace informatique continue d'augmenter dans un contexte international tendu avec des attaquants qui perfectionnent constamment leurs techniques pour réduire le risque de détection, de caractérisation et d'attribution des attaques.

Les principales attaques en 2023 sont :

- **L'espionnage stratégique et industriel par des acteurs étatiques ou privés de sociétés qui travaillent dans des domaines stratégiques ou qui assurent la transmission de données sensibles**. L'objectif principal des attaquants est la compromission de réseaux des organisations visées mais il apparait que les attaquants ciblent de plus en plus les équipements qui appartiennent à des individus (notamment les téléphones portables professionnels et personnels). L'ANSSI note également une augmentation des attaques des services de messagerie pour notamment accéder aux courriels.

- **L'attaque à but lucratif avec une augmentation de 30% des attaques par rançongiciel par rapport à 2022**. Elle peut avoir des impacts très importants pour la réputation et la continuité de l'activité des structures visées. L'ANSSI précise à cet égard que les attaques n'ont pas besoin d'être très sophistiquées pour cibler les établissements de santé (qui sont de plus en plus visés par ces attaques) et les collectivités territoriales qui sont encore trop vulnérables

- **Les opérations de déstabilisation prenant la forme d'attaques par déni de service distribué** (inaccessibilité du serveur par l'envoi de multiples requêtes jusqu'à le saturer ou par l'exploitation d'une faille de sécurité afin de provoquer une panne ou un fonctionnement fortement dégradé du service), **d'intrusions dans un système d'information suivies de sabotages ou de publications d'informations exfiltrées**.

En outre, l'ANSSI constate une augmentation du nombre d'attaques destinées à promouvoir des discours politiques, à entraver des contenus en ligne ou à porter atteinte à l'image d'une organisation. Exemple : compromission d'une partie du système d'information d'un média français ayant abouti à la divulgation d'informations en représailles à des publications.

La menace la plus importante à la veille du début des jeux olympiques et paralympiques est l'introduction et le maintien d'attaquants sur des réseaux d'importance critique (énergie, transports, logistiques). Dans ce cadre, **le pilotage de la stratégie de prévention des cyberattaques** a été confié à l'ANSSI. Le dispositif mis en place s'articule autour des axes suivants :

- Parfaire la connaissance des menaces pesant sur les jeux,
- Sécuriser les systèmes d'information critiques,
- Protéger les données sensibles,
- Sensibiliser l'écosystème des jeux,
- Se préparer à intervenir en cas d'attaque affectant les jeux.

Les actions de sécurisation proposées par l'ANSSI consistent en la réalisation d'audits et d'un accompagnement technique pour les entités critiques (avec l'accès à des outils et des services notamment pour évaluer le niveau de sécurité et de gestion de crise).

L'ANSSI précise cependant que bien que certaines attaques soient particulièrement difficiles à prévenir, les attaquants profitent aussi de mauvaises pratiques d'administration ou de gestion des droits et des secrets, de retard dans l'application de correctifs et de l'absence de mécanismes de chiffrement. En outre, l'ANSSI considère que la sous-

traitance de tout ou partie d'un système d'information à une entreprise de services numériques ne peut être effectuée sans s'assurer du niveau de sécurité des services fournis. Elle considère que la responsabilité de la sécurité d'un système d'information reste à la charge de son propriétaire.

A cet égard, la CNIL semble adopter la même approche puisqu'elle sanctionne fréquemment le responsable du traitement pour un incident de sécurité subi par son sous-traitant en considérant que le responsable du traitement n'a pas exercé de contrôle suffisant et régulier sur son sous-traitant.