Cyberattaques dans les hôpitaux, universités, administrations... Comment mieux résister ?

Mohammed Chergui-Darif, Tiberghien B.

Auteurs : Mohammed CHERGUI DARIF – Doctorant en Sciences de Gestion – IMPGT ;
Bruno TIBERGHIEN – Maître de conférences HDR en sciences de Gestion – IMPGT

Les organisations publiques à l'épreuve des cyberattaques :

Quelle stratégie de résilience technologique et organisationnelle ?

Collectivités territoriales, administrations publiques, hôpitaux, écoles et universités, aucune de ces organisations publiques n'est à l'abri des cyberattaques. Selon Arnaud Coustillère, chargé de la cyberdéfense française, une cyberattaque recouvre l'ensemble des actions volontaires, offensives et malveillantes menées au travers du cyberespace et destinées à provoquer un dommage aux informations et aux systèmes qui les traitent, pouvant ainsi nuire aux activités dont ils sont le support (Coustillière, 2020).

Selon l'Agence de l'Union Européenne pour la cybersécurité, 24,21% des cybermenaces recensées depuis juillet 2021 à travers le monde visaient spécifiquement des administrations publiques[1]. Cependant, ce risque reste largement sous-estimé en France, comme le souligne une étude du Clusif de 2020 menée auprès de collectivités territoriales (malgré le fait que près de 30% d'entre elles ont subi des attaques par rançongiciel en 2019)[2]. Ces attaques ont connu une augmentation considérable sur les organisations publiques françaises depuis la crise du Covid-19[3]. Les hôpitaux français sont des cibles privilégiées depuis une dizaine d'années[4].

Le 07 juin 2023, Aix-Marseille Université, a connu une cyberattaque qui a eu pour effet le blocage total et temporaire de l'ensemble de ses services numériques pour les étudiants, les enseignants-chercheurs et les personnels administratifs. La direction du numérique de l'établissement ayant très rapidement isolé son réseau, cette mise hors d'accès a permis de préserver l'intégrité du système informatique, d'éviter des dégâts potentiellement importants et d'assurer un retour rapide à la normale.

Si un niveau élevé de sécurité permet de contrecarrer et résorber la plupart des tentatives d'intrusion, ces phénomènes posent de sérieux défis en matière de résilience technologique et organisationnelle à nos administrations publiques. En effet, **comment assurer la continuité des services publics tout en protégeant les systèmes d'informations et les données personnelles des utilisateurs (personnels et usagers) ?**

La résilience dans les technologies numériques : anticiper, protéger et maintenir l'activité face aux chocs et aux crises

[1] https://www.enisa.europa.eu/publications/enisa-threat-landscape-2022
[2] https://clusif.fr/newspaper/le-risque-associe-aux-rancongiciels-demeure-sous-evalue-dans-les-collectivites-territorialesclusif/ - Le Clusif : association de référence de la sécurité du numérique en France.
[3] https://theconversation.com/cyberattaques-contre-les-collectivites-territoriales-le-pire-est-il-a-venir-196427 ; https://theconversation.com/cyberattaques-et-kidnapping-des-donnees-comment-proteger-les-organisations-des-rancongiciels-155384
[4] https://theconversation.com/cyberattaques-des-hopitaux-que-veulent-les-hackers-192407

La notion de résilience renvoie de manière générique à une capacité à résister, absorber et/ou rebondir face à un choc traumatisant, que cela soit à un niveau individuel, organisationnel, territorial voire sociétal. Sur le plan organisationnel, la résilience implique des capacités dynamiques visant à anticiper, résister, s'adapter ou encore se transformer, se réinventer (Du Boys & Tiberghien 2021).

Appliquée au domaine des technologies du numérique, la résilience implique à la fois des mesures de sauvegarde, de protection des données, mais aussi de maintien de l'activité qu'il convient de définir de manière préventive afin qu'elles puissent être déployées efficacement et rapidement le cas échéant (Oracle-KPMG, 2020). Au-delà des aspects purement techniques, les dimensions organisationnelles et communicationnelles apparaissent également cruciales. Dès lors, **quelle stratégie adopter pour une résilience technologique et organisationnelle face aux attaques numériques ?**

Nous avons interrogé un expert en cybersécurité pour comprendre pourquoi les organisations publiques sont des cibles de choix pour les cyberattaques. Il a partagé des stratégies pour se préparer et répondre à de potentielles attaques tout en maintenant les services.

- **Les raisons de la vulnérabilité des administrations publiques aux cyberattaques : un éclairage par les contraintes de ressources et de finalité**

Alors que les entreprises privées, centrées sur le profit, peuvent investir fortement en cybersécurité, les administrations publiques, orientées vers l'intérêt général, ont généralement des moyens plus restreints, limitant leur capacité à recruter des experts dans ce domaine, attirés par les salaires plus élevés du secteur privé. Ces contraintes renforcent leur vulnérabilité face aux cyberattaques.

- **Développer une démarche préventive de gestion des risques liés aux cyberattaques**

Afin de mieux anticiper les risques liés aux attaques cybernétiques, plusieurs méthodes peuvent être mobilisées que ce soit d'un point de vue technique ou organisationnel.

Sur le plan technique :

- **L'application du principe du moindre privilège** : consiste à considérer et faire en sorte qu'aucun équipement, dans un réseau, ne fasse confiance à un autre. Même les communications internes devraient être considérées comme non sécurisées et les interactions vérifiées.
- **L'utilisation de systèmes de gestion de l'information et des événements de sécurité (SIEM)** : ces systèmes collectent des données sur la performance, les transmissions réseau, les journaux des systèmes d'exploitation et d'autres paramètres. Ces informations sont analysées en temps réel pour détecter toute anomalie ou activité malveillante.
- **Une configuration appropriée du réseau :** comprendre la configuration du réseau est crucial pour anticiper et prévenir les attaques.

Sur le plan organisationnel :

- **La certification :** obtenir une certification d'une autorité compétente peut aider à prouver que le système a atteint un certain niveau de sécurité.
- **La cartographie du système d'information :** comprendre le système d'information, même s'il est complexe, est essentiel. Cela peut aider à identifier les failles potentielles et les chemins que pourrait prendre un attaquant.
- **La communication en période de crise :** il est important de communiquer efficacement avec les utilisateurs pendant une crise pour les rassurer, tout en étant factuel sur la situation. Des erreurs de communication de crise peuvent entraîner des répercussions négatives sur la confiance des utilisateurs.
- **La formation du personnel :** il est primordial de former les collaborateurs des administrations sur ces risques liés aux cyberattaques, surtout pour leur permettre de reconnaître les tentatives d'hameçonnage.

Dans quelle mesure les administrations publiques peuvent-elle assurer une continuité du service public en cas d'attaque ?

Le cas de l'entreprise GitHub, même s'il ne met pas en scène une administration publique, est particulièrement inspirant. En 2018, GitHub a été victime de ce qui a été qualifié de plus grosse cyberattaque de l'histoire[5], ce qui ne l'a pas empêché de maintenir son service grâce à une organisation bien pensée (réplication de données, existence de serveurs alternatifs) et une préparation préalable à ce genre d'attaque.

La vulnérabilité des administrations publiques face aux cyberattaques est un défi de taille à relever. Les solutions résident dans une approche proactive et multiforme combinant des mesures techniques et organisationnelles. Il est indispensable d'adopter le principe de moindre privilège, d'investir sur des SIEM et de mieux préparer son système technologique à ce genre d'attaque. Sur le plan organisationnel, la certification, la cartographie du système d'information, la gestion de la communication de crise et la formation du personnel sont à prioriser. L'histoire de GitHub démontre qu'une stratégie de cybersécurité proactive et résiliente permet de garantir la continuité des services même en situation de cyberattaque majeure.

Références bibliographiques

Coustillière, A. (2020). « La transformation numérique du ministère des Armées », *Hérodote,* 2020/2 (n° 177-178), p. 165-177.

Du Boys, C. & Tiberghien, B. (2021). « Résilience territoriale et résilience financière : Quelle articulation conceptuelle et pratique ? Étude exploratoire sur les stratégies de résilience de 8 villes européennes », *Management international-Mi*, 26(spécial), 149-167.

Oracle & KPMG (2020), *Cloud Threat Report*: *Addressing Security Configurations Amidst a State of Constant Change*.

[5] https://siecledigital.fr/2018/03/02/github-grosse-attaque-ddos/