La Cyber sécurité en période de guerre

AMUSEC 2023

Yves Jehanno

Contexte

- La guerre actuelle aux portes de l'Europe oblige à repenser notre vision de la cyber sécurité
- Un peu plus à l'Est, avec l'obtention par le dirigeant chinois de son troisième mandat et la guerre de la Russie en Ukraine, de nombreux experts prédisent une augmentation des cyberattaques commanditées par des États.
  - La Chine pourrait multiplier les cyberattaques contre Taïwan, Hong Kong et d'autres pays opposés au régime.
  - Pendant ce temps, la Russie devrait parrainer des attaques contre les pays soutenant l'Ukraine.

Est-ce un phénomène nouveau ?

- La guerre Israël-Hezbollah des 33 jours en 2006 a également marqué le début de l'intense collaboration entre l'Iran et le Hezbollah dans le cyberespace.
- En 2010, la découverte de l'opération Stuxnet, qui neutralise momentanément le programme nucléaire de la République islamique.

La guerre du digital ?

- Le développement de la cyberarmée iranienne entraîne, quasi simultanément, la mise sur pied d'une unité d'action électronique au sein du système opérationnel du Hezbollah.
- Ladite *Hezbollah Cyber-Army* (HCA) commence à opérer activement durant le « Printemps arabe » de 2011, il faut attendre 2015 et les révélations concernant sa campagne Volatile Cedar (ciblant des centaines de serveurs abrités par des organisations israéliennes et américaines)
- Comme les activités de cyberespionnage et de cybersabotage, les opérations de désinformation et de cyberinfluence du Hezbollah visant à modifier la perception d'audiences cibles sont placées sous l'autorité directe de la chaîne de commandement paramilitaire et obéissent à ce titre à la même logique offensive.

L’exemple de la Corée du Nord

- La **Corée du Nord** qui est soupçonnée de tirer 10 à 15 % de ses recettes extérieures d’actions de piratage. On pense que les effectifs de l’armée de pirates de la Corée du Nord, appelée Bureau 121, se montent à environ 6000 personnes. Le pays ermite consacrerait 10 à 20 % de son budget militaire pour financer des opérations en ligne..

Et en Europe ?

Le 18 octobre 2022, le chef de l'agence de cybersécurité allemande (BSI), Arne Schönbohm a été révoqué après des informations de médias faisant état de liens avec une association présumée proche des services secrets russes.

« Le ministère de l'Intérieur a déclaré, de son côté, « prendre au sérieux » les allégations contre Arne Schönbohm, et « enquêter de manière exhaustive » à ce sujet. « Le ministère étudie toutes les options sur la façon de gérer cette situation », a-t-il ajouté sans préciser davantage.

C'est la ZDF qui a déterré l'affaire

Le conflit Russie - Ukraine ?

Un malware cible le système militaire DELTA ukrainien

Le système DELTA fournit des informations en temps réel à l'armée ukrainienne. Des emails sont envoyés vers les utilisateurs pour les inciter à installer un malware.

"Le système Delta fournit aux militaires ukrainiens de précieuses données sur l'armée russe et contribue à la coordination de nos troupes sur le champ de bataille", or, ce programme si important pour Kiev a été piraté le 1er novembre dernier par un groupe de hackers russes se présentant sous le nom de "Joker DPR" (DPR étant l'acronyme de la République populaire de Donetsk sous contrôle russe)..

Nouvelle loi Russe promulguée en février 2019 ?

La Russie interdit Internet pour ses militaires en service

La Douma vient d'approuver une loi restreignant l'utilisation du smartphone à ses militaires en service, et interdisant l'accès aux réseaux sociaux

- Le texte prévoit l'interdiction de la moindre publication sur les réseaux sociaux (comme Odnoklassniki ou Vkontakt) pour les soldats, ainsi que la restriction des applications pouvant transmettre des données audio, photo, vidéo ou de géolocalisation vers Internet.
- Officiellement, ses auteurs le justifient par la volonté d'éviter que des services de renseignements étrangers ou des groupes terroristes puissent accéder à des données sensibles sur l'armée. En réalité, cette nouvelle loi vise pour Moscou à garder le contrôle sur les traces numériques laissées par ses soldats.

Nouvelle loi Russe promulguée en février 2019 ?

- Ces dernières années, différentes fuites dans les médias occidentaux ont en effet jeté le discrédit sur des positions officielles du gouvernement russe. En 2014 par exemple, le site d'investigation Bellingcat révélait la mort de 40 soldats russes en Ukraine à partir d'une publication Instragram d'un des soldats du régiment.
- Le 15 février 2019, Vladimir Poutine a réitéré son appel à faire de la Russie un pays avec un « Internet souverain », capable de fonctionner en cas de coupure du pays avec les serveurs mondiaux.

- Objectif principaux=>
  - Hausser le niveau de censure des contenus internet, à l'image de ce que fait la Chine avec son Great Firewall.
  - Ne véhiculer que des informations sous le contrôle de l'état
  - Etre en autarcie numérique en cas de conflit majeur

Quid des états ?

Les cyberattaques constituent un mode opératoire auquel ont régulièrement recours les acteurs étatiques étrangers, qu'il s'agisse d'intrusions informatiques par voie électronique ou par l'insertion physique de supports numériques contenant des charges malveillantes.

Principale menace cybernétique en 2021 et pour les années à venir, les rançongiciels (ransomwares) ciblent les établissements de recherche publics comme privés. La maturité inégale dans le domaine de la cyber-sécurité est en effet une vulnérabilité du domaine académique, y compris pour la recherche de défense.

Enfin, ces ingérences peuvent aller jusqu'à la déstabilisation de chercheurs adoptant des positions non conformes à l'idéologie de certains compétiteurs.

Nos entreprises ?

Dans le cadre des tensions internationales actuelles, des cyberattaques peuvent affecter les entreprises françaises soutiens de l'Etat, en particulier les capacités industrielles de production, d'une part en ciblant les SI industriels, d'autre part en instrumentalisant la chaîne de sous-traitance en procédant à des attaques par rebond.

Pour autant, si l'entreprise peut être directement victime de cyberattaques par voie directe, les possibilités d'attaques via les chaînes de sous-traitance ne doivent pas être négligées

Et dans l'espace ?

Des hackers de Moscou infiltrent un satellite américain

L'agence de cybersécurité américaine, le CISA, a décelé un groupe de hackers lié au Kremlin (Fancy Bear – APT28) dans le réseau d'un satellite privé américain. Les pirates y étaient installés depuis des mois.

La cyberguerre ne fait pas forcément de bruit, mais les batailles continuent dans l'ombre. Un réseau privé de satellite américain a été infiltré par un groupe **de hackers** russe, suspecté de travailler pour Moscou. Des chercheurs du CISA, l'Agence de cybersécurité américaine, ont travaillé sur cette cyberattaque, détaillée lors d'une conférence et retranscrite par le média Cyberscoop le 16 décembre 2022.

Et la France dans tout cela ?

- Dans la revue nationale stratégique 2022, le président Emmanuel Macron fixe comme objectif stratégique No 4 que la France doit disposer d'une résilience cyber de premier rang en 3 points :
    1. Améliorer la résilience cyber de la France, condition de la souveraineté
    2. Consolider les acquis du modèle français
    3. Investir dans la durée pour atteindre le meilleur niveau de résilience cyber

Premières recommandations ?

- Identifier les données stockées sur des serveurs à l'étranger, en particulier ceux situés en Europe de l'Est et caractériser leur sensibilité en vue d'un éventuel rapatriement.
- Contrôler les processus SSI, les amender si nécessaire (ex. segmentation de vos SI, contrôle des accès individualisé, processus de sauvegarde physique hors réseau etc.).
- Mener des investigations sur tout comportement SSI anormal (connexions inconnues, changement de mot de passe non sollicité, comportement anormal dans les logs) ou tentative de cyberattaque.
- Alerter immédiatement en cas de contact cyber suspect (email, approche sur les réseaux sociaux etc.).
- Répartir l'information sensible pour éviter de la concentrer en un seul endroit, sur une seule personne ou une seule entité.

Conclusion

- La cyberguerre n'est certainement pas nouvelle, mais elle sera de plus en plus présente dans nos vies.
- Tous les conflits géopolitiques devront intégrer cet aspect de cyberguerre pour que seuls les pays capables de maintenir les services les plus essentiels (santé, service de l'eau, énergie, transports, équipements, etc.) au cœur des hostilités puissent s'en sortir.
- Nous entrons dans une nouvelle ère. Une ère dans laquelle la cyberguerre n'est plus seulement un problème d'état mais concerne aussi les entreprises et les particuliers. Un seul élément défaillant peut fragiliser l'ensemble d'un système et donc tous ensemble devons veiller par nos comportements responsables à protéger nos libertés.