Compte Rendu de Conférence : Les enjeux de la cybersécurité et de la cyberdéfense au XXIe siècle

Assurer la sécurité cyber à tous les niveaux, que ce soit sur le plan structurel, organisationnel ou technique, s'avère essentiel. Ces préoccupations sont notables aussi bien dans le secteur public que dans le secteur privé.

La contextualisation des enjeux de la cyberdéfense a fait ressortir l'importance de comprendre les menaces, notamment à court terme avec les Jeux Olympiques, influant ainsi sur les orientations futures. Nous avons également abordé les risques quotidiens liés au partage d'informations sensibles sur les réseaux sociaux.

Des définitions clés pour clarifier les concepts fondamentaux de la cybersécurité et de la cyberdéfense :

- Selon le glossaire de l'ANSSI, la cybersécurité est définie comme "l'état d'un système d'information qui résiste aux cyberattaques et aux pannes accidentelles survenant dans le cyberespace."
- La cyberdéfense, quant à elle, englobe l'ensemble des moyens déployés par un État pour défendre ses systèmes d'information jugés d'importance vitale.

L'évolution du cadre juridique en matière de cyberdéfense a été soulignée, indiquant que le Ministère des Armées (minarm) et le Commandement Cyber (comcyber) disposent actuellement de moyens permettant d'engager la lutte informatique offensive, une avancée significative par rapport au passé.

I/ Principales Menaces Cyber et Défis de la Cyberdéfense

A. Menaces Cyber :

- Attaques par Logiciels Malveillants : Les attaques par mail demeurent les vulnérabilités primaires, offrant une facilité d'infiltration dans les systèmes d'information. L'ampleur des flux d'attaques par mail crée une probabilité accrue qu'au moins une personne clique sur un mail malveillant, permettant au virus de compromettre le PC.
- Les ransomwares, notamment depuis juin 2018 avec le RGPD, obligent les entreprises à déclarer les fuites de données.

B. Phishing et Ingénierie Sociale : Une inondation considérable d'ordinateurs est provoquée par le phishing, qui devrait persister et s'intensifier. Les gains multiples, qu'ils soient lucratifs, organisés par des hackers, ou soutenant des actions subversives étatiques, contribuent à la persistance des ransomwares. La France se classe parmi les trois pays les plus attaqués sur le plan cyber.

C. Intelligence Artificielle (IA) : Les tendances des deux dernières années ont montré l'IA comme un outil prometteur dans la détection d'attaques mais de la même manière un nouvel outil très utile pour les hackers (automatisation des attaques, usurpation d'identité, de la voix et/ou des visages). Des programmes dédiés à l'IA, tels que celui développé par la gendarmerie nationale au sein du COMCYBER-MI (Ministère de l'intérieur), démontrent de réelles avancées en termes de détection et de prévention. Un espoir technologique fort.

II/ Défis de la Cyberdéfense :

- Défi capacitaire et Innovation : Le COMCYBER, la DGA et la DGSE sont les acteurs principaux de la cyberdéfense en France (pour le périmètre du ministère des Armées), et apportent un soutien à l'ANSSI dans son périmètre étatique. La sécurité des systèmes d'information du MinArm repose sur 4 critères de sécurité essentiels et incontournables : Disponibilité, Intégrité, Confidentialité et Traçabilité (DICT) permettent d'évaluer les risques pour une protection renforcée.Cette dernière appelle à des besoins croissants de nouvelles technologies, innovation et recherches en IA.
- Défi des Ressources Humaines : La pénurie de profils et d'expertise en cybersécurité est un défi majeur. La formation continue est essentielle, mais le défi réside dans le budget et les ressources pour développer, former et mettre en œuvre des initiatives ambitieuses. Malgré un marché saturé, recruter les bonnes personnes reste complexe, nécessitant une formation interne et une gestion du temps pour le personnel militaire.
- Coopération France & Monde : La prise de conscience au niveau mondial sur la cybersécurité a considérablement augmenté au cours des 15 dernières années.

III/ Recours et Bonnes Pratiques :

A. Utilisation de Logiciels Antivirus et Anti-Malwares : L'usage de logiciels antivirus et anti-malwares est préconisé tant dans un contexte professionnel que personnel pour prévenir les attaques.
B. Mise à Jour Régulière des Systèmes et Logiciels : Une mise à jour constante des systèmes et des logiciels est recommandée pour garantir une protection efficace contre les vulnérabilités.
C. Sensibilisation des Utilisateurs et Formation : Un plan de sensibilisation et de formation, tant au niveau personnel que professionnel, est essentiel pour informer les utilisateurs des meilleures pratiques en matière de sécurité.
D. Engagement du Ministère de l'Intérieur dans la Cybercriminalité et la Cybersécurité : Le Ministère de l'Intérieur est fortement engagé dans la lutte contre la cybercriminalité, soulignant l'importance accordée à la sécurité dans le cyberespace.

IV/ Comment Se Protéger :

- Protégez vos accès avec des mots de passe solides : L'utilisation de mots de passe robustes est fondamentale pour sécuriser l'accès à vos comptes et données sensibles.
- Sauvegardez régulièrement vos données numériques : La sauvegarde régulière des données numériques permet de minimiser les risques de perte en cas d'incident.
- Appliquez immédiatement les mises à jour de sécurité : l'application rapide des mises à jour de sécurité sur tous vos appareils renforce la protection contre les vulnérabilités.
- Utilisez un antivirus : l'installation d'un antivirus est une mesure essentielle pour détecter et neutraliser les menaces potentielles.

- Téléchargez uniquement sur les sites officiels : limitez le téléchargement d'applications aux sites officiels pour éviter les logiciels malveillants.
- Méfiez-vous des messages inattendus ou alarmistes : La vigilance face aux messages inattendus ou alarmistes est cruciale pour prévenir le hameçonnage.
- Vérifiez les sites d'achats : lors des achats en ligne, que ce soit personnel ou professionnel, assurez-vous de la légitimité des sites.
- Maîtrisez vos réseaux sociaux : contrôlez l'accès, les autorisations et les informations relayées sur vos réseaux sociaux.
- Séparez les usages professionnels et personnels : Évitez les confusions en maintenant une séparation claire entre les usages professionnels et personnels de vos équipements et messageries.
- Évitez les réseaux Wifi publics ou inconnus : Privilégiez la sécurité en évitant les réseaux Wifi publics ou inconnus, une recommandation détaillée sur www.cybermalveillance.gouv.fr.