Projet de recherche n°5: État des lieux des menaces et enjeux de la cybersécurité

Contexte

Sur les aspects techniques,**plusieurs faiblesses**seront des éléments majeurs :

> Les **cyber activités** offrent de **nouveaux usages**, de **nouveaux services** et **modèles économiques** mais elles reposent sur des **technologies vulnérables**, elles souffrent de **failles techniques**, cibles ou vecteurs d'attaque, incitant les cybercriminels à **les exploiter quasi-quotidiennement** de façon détournée et malveillante, pour **s'insinuer passivement dans les systèmes**, en prendre le contrôle ou les détériorer.
> Les dispositifs de sécurité souffrent de **technologies de protection vieillissantes**, agissant sur les **flux d'informations** : cryptographie, classification, profiling, ou sur les **architectures périmétriques qui les véhiculent** : cloisonnement, relais/filtrage, ces faiblesses constituent autant d'opportunités pour les cybercriminels.
> L'analyse de la cybermenace repose sur **l'analyse d'actions malveillantes** dans des péta-octets de traces : l'automatisation de l'analyse est actuellement mise à mal, confrontée à**une quantité considérable de faux-positifs et faux-négatifs**, les experts humains sont dépassés, les cyberattaquants n'hésitent pas à **tester les systèmes en continu** pour détecter et exploiter les **failles détectées.**

Cet état des lieux distingue un ensemble de déterminants cruciaux de l'économie et des enjeux de sécurité:

> La **continuité d'opération** des fournisseurs d'accès à Internet et la **stabilité des infrastructures numériques** ;
> La **résilience de services** aussi bien pour les opérateurs d'**infrastructures vitales** (santé, hôpitaux, services publics, énergie, etc.) que pour des **services publics et régaliens** (administrations, défense) ;
> La **sécurité des paiements et des transactions électroniques**, qui encouragent la **criminalité numérique** en lui offrant une **incitation à la consommation de biens numériques**obtenus illégalement (torrent, streaming illégal, contrefaçon de logiciels, vols d'accès, usurpation d'identité).
> L'investissement de **renouvellement et de progression générationnelle des infrastructures numériques** (fibre, très haut débit) qui repose sur le maintien d'une profitabilité et d'une visibilité des coûts d'investissement à long terme.

Vecteurs de propagation des cyberattaques

Les facteurs ayant propulsé la**prolifération des attaques entre 2008 et 2016**ne sont pas seulement d'ordre technique. Si le **savoir-faire technique**s'est fortement démocratisé sur cette période, il n'a connu que **très peu d'innovations de rupture** : les attaques utilisent pour la plupart des **méthodes connues**, à l'exception des **attaques ciblées (Advanced Persistant Threats)** qui ont majoritairement bénéficié d'**innovations provenant de disciplines connexes** (machine learning notamment).

Les incitations économiques de l'**économie grise de la sécurité informatique**, et les défaillances des modèles économiques en présence sur le marché, sont les principaux **vecteurs de la montée en puissance des attaques** sur le plan global. Ces éléments nouveaux comprennent :

La**forte croissance des marchés parallèles** - et légitimes - des exploits (découvertes de failles pouvant être exploitées pour mener une attaque). Le paiement des découvertes de faille a connu, en valeur, une croissance sans précédent (selon les estimations, entre 200% et 300%).
La **location de capacités offensive**s s'est de son côté démocratisée, avec la possibilité de l**ouer des botnets pour des coûts inférieurs à 500$.**
La **détérioration de la perception de ce qui est « légitime »** par les consommateurs (perception de la paternité, de la propriété du numérique, du libre usage, du « droit » de visionner des matériaux en streaming, etc.).
La **croissance des modèles économiques** adossés aux réseaux sociaux, qui crée une**réserve de valeur marchande**au sein de cibles particulièrement mal protégées. La **monétisation des réseaux sociaux** constitue une incitation forte pour la petite criminalité informatique (vols d'identité, vols d'identifiants CB, etc.).
La **délocalisation des données**, **l'accès à distance** (cloud) et la **numérisation des monnaies** constituent une autre incitation économique à la criminalité informatique, créant un transport de données susceptible d'être monétisé sur le marché gris ou illicite de la cybercriminalité (vols d'identifiants en masse, extorsions, chantage aux données auprès de marchands ou d'opérateurs OIVs).

https://esd.cnam.fr/projets-de-recherche-cooperation-scientifique/projets-de-recherche/projet-de-recherche-n-5-etat-de