Le hacking n'est pas une fatalité. G. Litzistorf – 6 oct 2017

Régulièrement des noms évocateurs comme WannaCry font les grands titres.
WannaCry a eu un faible impact en Suisse car l'attaque visait des ordinateurs dépourvus de **défense périmétrique** comme un routeur xDSL ou un pare-feu.
Cette défense est capable d'empêcher qu'un hacker (Charly) sur internet ne puisse attaquer directement votre ordinateur utilisant une **adresse privée**.
Charly peut contourner cette défense en vous envoyant un **email malicieux** afin de vous inciter à cliquer sur le lien qui déclenchera le chiffrement de vos données stockées sur le disque et la demande d'une rançon.
A ce stade Charly utilise deux mécanismes distincts : il compte sur la **naïveté de l'être humain** (qui restera toujours le maillon faible) et sur les **défauts (failles, bugs, …) du logiciel.**

Il est grand temps que les utilisateurs, les entreprises et les gouvernements qui achètent des produits Microsoft exigent que ces logiciels respectent les bonnes pratiques de développement et de tests unitaires rigoureux puisque WannaCry utilisait des failles du protocole SMB 1.0 et que ce protocole très ancien est présent dans toutes les versions Workstation et Server depuis Windows 2000 !

Profitons-en pour rappeler qu'il est facile de se prémunir contre ce type d'attaque en faisant régulièrement une **sauvegarde de ses données** personnelles et en **évitant de cliquer sur un email bizarre**.

La réponse aux cyberattaques passe par la formation des utilisateurs qui doivent acquérir les fondamentaux en matière de sécurité des systèmes d'information.
La défense périmétrique permet de confiner des installations critiques telles que barrage, hôpital, aéroport, centrale nucléaire ou centre de production dans des réseaux intranet isolés du monde internet.
A titre d'exemple le paquet qui quitte le centre de commande SIG du Lignon pour commander les pompes du jet d'eau utilise ce type de réseau privé.

Toute démarche sécuritaire devrait être initiée par une **analyse des risques**. Quel est le préjudice ; quelle est la perte financière si mon serveur de messagerie est indisponible pendant un jour ? Quels sont les principaux risques ? Disponibilité de mes données, confidentialité d'une transaction bancaire, …

Le hacking n'est pas une fatalité.
Dans le cas récent de prise de contrôle d'une centrale électrique par des hackers, l'analyse du risque était laxiste.
Par **soucis de confort**, elle peut tolérer que le personnel de la centrale ou un sous-traitant soit autorisé à accéder aux ressources informatiques depuis internet.
Un **employé complice** peut faciliter l'accès à Charly.
Un **employé naïf** peut aussi récupérer la clé USB trouvée sur le parking, franchir la sécurité physique du bâtiment puis connecter cette clé USB à son ordinateur permettant au cheval de Troie d'agir.

Parmi les dispositifs populaires de sécurité figure l'antivirus qui fonctionne selon un **modèle de liste noire** et est capable de bloquer des attaques connues par son éditeur. Il est donc inefficace aux attaques WannaCry tant que l'éditeur ne l'a pas identifié et tant que l'utilisateur n'a pas mis à jour son antivirus. On parle de ***zero-day exploit*** pour tout logiciel malveillant inconnu de votre antivirus.

Le **modèle de sécurité liste blanche** offre une nette amélioration puisqu'il interdit tout par défaut. L'administrateur du pare-feu de l'entreprise doit ajouter des règles de sécurité pour autoriser par exemple le groupe des secrétaires à accéder à certains serveurs sur internet.
Ce modèle de sécurité est heureusement en vigueur dans l'aviation où "**tout ce qui n'est pas écrit est interdit**".

L'analyse des risques permet d'identifier les ressources à protéger.
Les **moyens de défenses sont physiques** (je ferme ma porte à clé), **logiques** (les PCs du bâtiment A ont accès à internet ; pas ceux du bâtiment B), et **organisationnels** (l'employé respecte les directives écrites telles que l'interdiction de brancher une clé USB à son PC).

Le confort de l'utilisateur est très souvent incompatible avec un bon système de défense.