INTRODUCTION : LA CYBERSECURITE

Par Philippe Duluc - Vice Président ACN

La cybersécurité est indissociable du cyberespace, cette nouvelle dimension dans laquelle les entreprises, les institutions et les gouvernements développent leurs activités vers leurs clients ou leurs administrés. Amenée par l'internet, elle n'existait pas il y a 20 ans ; elle est aujourd'hui devenue le support vital d'une grande partie de nos activités. Elle est marquée par des transformations de fond qui accroissent les risques de sécurité.

La première d'entre elles est portée par la convergence vers internet : tous les réseaux s'interconnectent en un réseau IP unique qui relie objets, machines et hommes, poussé par le besoin et par les coûts. Cela ouvre des possibilités infinies de pénétrations dans les systèmes d'informations, et d'atteinte des outils de travail.
Ensuite avec la consumérisation les terminaux grand public débordent sur le monde professionnel, poussé par grands VIP et par les coûts (exemple iPhone) dérogeant aux stratégies de sécurité orientées maitrise et contrôle. C'est aussi le cas de la dépérimétrisation : la frontière entre les sphères professionnelles et personnelles s'estompe (BYOD : bring your own device, télétravail, etc.) et la protection des données personnelles peut prendre le pas sur celle du patrimoine des entreprises. Enfin, l'externalisation et la mutualisation amènent conjointement le cloud computing (réduction de coûts) avec des questionnements sur la localisation des données (accès légal des autorités locales notamment) et sur la résilience.

Cette nouvelle dimension expose à de nouvelles menaces qui évoluent elles aussi de plus en plus vite, en dangerosité, en complexité et en taille :

- vol massif de données personnelles par la voie informatique motivé principalement par des gains financiers ;
- atteintes ciblées à la disponibilité ou l'intégrité (défiguration ou saturation de sites web par exemple) avec une motivation idéologique (cybermanifs) ou cupide (chantage);
- attaques ciblées et sophistiquées visant à dérober subrepticement de l'information sensible (attaque de Bercy visant des informations relatives à la position française vis-à-vis du G20 en 2011, attaque d'une grande entreprise française pendant 2 ans avant d'être détectée) avec une motivation stratégique ou économique ;
- des cyber-attaques visant à endommager physiquement des installations (attaque d'automates industriels Siemens par le ver Stuxnet par exemple, voir fiche SCADA)

Ces nouvelles cyber-menaces, en particulier les deux dernières catégories ci-dessus, sont particulièrement insidieuses et dangereuses. Tout d'abord on peut supposer qu'elles sont beaucoup plus nombreuses que les quelques cas répertoriés et révélés à ce jour. En effet, les victimes rechignent à les rendre publiques, voire même seulement à engager des poursuites judiciaires, par crainte d'un effet négatif d'image et aussi de faire connaitre d'éventuelles faiblesses encore exploitables. Ensuite, les méthodes et les outils informatiques utilisés se vulgarisent. C'est inévitable dans la durée et c'est ce qui s'est passé avec la première génération d'outils d'attaque que le crime organisé s'est approprié : sur des sites pirates, s'équilibrent offre et demande, comme par exemple la location d'un botnet de bombardement pour quelques centaines d'euros la journée.

L'ACN s'est donnée comme mission de représenter l'ensemble de la chaine technologique de la confiance qui permet aux clients de maitriser ces nouveaux risques. Cette représentation est aussi large que possible et rassemble des éditeurs, des équipementiers, des laboratoires de recherche, des opérateurs, des sociétés de services ou des intégrateurs, et de toutes tailles (PME à multinationale). L'un des premiers objectifs reste de fournir une description fine et évolutive de l'écosystème de la cybersécurité en tenant à jour à jour un référentiel sous forme de fiches thématiques (menaces, technologies, grands enjeux, etc.) accessibles via les liens qui suivent.

Philippe Duluc
Vice-président d'ACN