Forum international de la cybersécurité : pourquoi les entreprises ont aussi besoin de développer leur cyber-résilience et pas seulement leur capacité a se défendre

Ce mardi 22 janvier se tient le 10e Forum International de la Sécurité à Lille. Le thème central est intitulé "hyperconnection, le défi de la résilience".

Avec Gérôme Billois

Atlantico : A l'objectif de cyber sécurité, de plus en plus important pour les entreprises qui sont sous la menace d'attaques majeures, on adjoint désormais celui de cyber-résilience. De quoi s'agit-il et quoi cette résilience est devenue tout aussi importante pour les entreprises que leur cyber-sécurité ? La cyber sécurité n'est-elle plus suffisante en soi ?

Gérôme Billois : La cyberrésilience est un thème qui a émergé lors de l'été 2017 après les deux vagues d'attaque mondiales successives, Wannacry et Notpetya qui ont démontré que des centaines d'entreprises ou institutions publiques pouvaient être très durement touchées par des cyberattaques. En quelques heures celles-ci pouvaient effacer des milliers de PC, des milliers de serveurs, et ce à une échelle internationale. On était jusqu'ici dans une démarche de cybersécurité où chacun sécurisait son information, en voulant éviter les attaques.

2017 a donc joué le rôle d'électrochoc dans les consciences : on s'est rendu compte qu'on allait forcément être la victime d'une cyberattaque, et ce même si on se prépare au maximum. A un moment où un autre, quelque chose peut me toucher : il est donc nécessaire dès lors de réfléchir plus loin, à sa résilience, c'est-à-dire à sa capacité à surmonter un événement très grave.

Cette question de la résilience s'est donc ajoutée comme un des piliers des stratégies de cybersécurité au sens large. Il s'agit d'avoir la capacité après une attaque à reconstruire vite son système d'information.

Avant l'été dernier, il y avait des stratégies de résilience fondé sur l'existence de deux salles informatiques synchronisées en temps réel qui permettent, en cas d'incendie ou de dysfonctionnement d'un serveur que celui de secours prenne immédiatement le relais. Le problème, c'est que face à une attaque cyber, cela ne fonctionne pas parce que l'attaque est tout autant synchronisée en temps réel que le système de secours. L'été dernier, les systèmes nominaux comme de secours ont été détruits simultanément. Cela nous a ouvert les yeux, même si on avait déjà eu des alertes avec les cas de Saudi Aramco en Arabie Saoudite ou de Sony Pictures en 2014. Cela semblait alors lointain et lié à des contextes géopolitiques. Cet été, on a vu en quelques heures que des entreprises comme Saint Gobain, Maersk, Merck, et bien d'autres grosses entreprises ont été touchées très durement. Ce n'est plus de la théorie mais de la pratique désormais.

Quelles sont les composantes clé d'un bon programme de cyber résilience ?

Il y a trois piliers :

Le premier est d'anticiper au maximum pour ne pas rompre quand survient l'attaque. Cela passe par une bonne protection évidemment, à commencer par les règles de bases de la cybersécurité :

- maintenir ses systèmes à jour

- appliquer les correctifs

- gérer les mots de passe d'administration

Ce sont des tâches techniquement simples mais qui dans la pratiques sont compliquées à réaliser et demandent énergie et engagement.

Il faut aussi introduire la diversité son système d'information. On a pu observer que lors de ces attaques, tous les PC ont été visés. Aujourd'hui, il serait donc souhaitable d'introduire des machines sous Mac OS, sous Linux, ou d'avoir la possibilité de démarrer des machines mises de côté préventivement avec des clés USB. Le but étant d'éviter d'être 100% identique et donc, le jour de l'attaque, 100% détruit. Cela n'est pas simple parce que cela nécessite de l'argent, de maintenir deux systèmes différents, d'avoir des compétences dans ces deux systèmes etc.

Il faut enfin donner la capacité à sécuriser les systèmes qui amplifient les attaques. On trouve souvent dans une entreprise des équipes d'administrateurs dotés d'outils leur permettant d'appliquer une modification sur tous les autres ordinateurs. Une fois piratés, ces systèmes permettent d'endommager tous les autres ordinateurs bien évidemment. Ces systèmes administrateurs ou antivirus, ou de déploiement de correctif doivent être particulièrement sécurisés.

Le second pilier est d'être en capacité de réagir très rapidement quand on est touché. On le voit avec Petya, qui s'est répandu en une heure de temps. Pour cela, il faut réfléchir à son organisation de crise, s'entrainer pour que les équipes qui ne sont pas habituées à ces attaques soient à même de gérer ces crises. De la même façon que les pompiers s'entrainent toute la semaine pour pouvoir gérer un feu à n'importe quel moment, il faut que les équipes de gestion de crise s'entrainent très régulièrement pour ne pas être désarçonné le jour où cela arrive.

Il faut être en mesure de sauver ce qui peut l'être en cas d'attaque, afin de garantir qu'on dispose de systèmes de sauvegarde. Ceux-ci ont été détruits lors des récentes attaques.

Le dernier pilier est celui de la reconstruction, c'est-à-dire se doter de moyens qui permettent de se remettre très vite sur pied. En moyenne, il faut savoir qu'un technicien est capable d'installer entre 4 et 6 ordinateurs par jour. Quand il y en a 10.000, c'est problématique. Une possibilité est de faire participer les employés à la reconstruction, et donc de les embarquer.

Une idée centrale de la cyber-résilience semble sa capacité à penser le long terme. Comment construire cette capacité de pensée active poussée dans un cadre souvent soumis à l'immédiateté ?

C'est un vrai changement de stratégie. La sécurité était pensée comme uniquement technique, avec des changements de mots de passe et l'installation de logiciels pour se défendre. Il faut aujourd'hui penser en termes de métiers prioritaires de l'entreprise, et donc d'estimer lesquels doivent être sécurisés en priorité en cas d'attaque. Cela signifie aussi pour les directions de s'engager sur des budgets. On parle d'investissements de dizaines voire de centaines millions d'euros, afin de rattraper le retard souvent accumulé.

Et c'est d'autant plus important que cela implique d'intégrer à cette dynamique non seulement tous les collaborateurs mais aussi tous les fournisseurs des entreprises. Il y a une chose qu'on oublie souvent, c'est qu'une entreprise est dépendante d'une chaine de fournisseurs qui eux-mêmes peuvent être touchés par des attaques similaires. La résilience doit donc être organique.

On parle donc d'investissements très lourds. On sait que les grandes firmes sont capables d'investir cet argent. Mais qu'en est-il des PME qui n'en ont pas les moyens ?

C'est un vrai sujet. On a vu cette année des PME mettre la clé sous la porte suite à des attaques. C'est un sujet très compliqué, notamment parce qu'on a un manque de compétences criante sur le marché. Les solutions demandent un vrai niveau technique, laissant entrevoir une grande zone de risque que l'Etat tente aujourd'hui de couvrir, notamment avec le site cybermalveillance.gouv.fr (ACYMA) qui est une plateforme centralisée pour mettre en relation les TPE et PME avec des spécialistes reconnus qui sont capables de leur venir en aide rapidement.

La majorité des PME/ETI ne voient pas encore le risque, c'est certain, là où les grandes ont bien compris les enjeux.

Quels sont les capacités de formation que ce soit comme étude supérieure ou comme formation continue de notre pays ?

Rien n'existait vraiment jusqu'il y a peu. Une initiative nommée cyber.edu tente aujourd'hui d'intégrer dans les grandes écoles des concepts de cyber-sécurité et de cyber-résilience. Et donc donner une formation qui petit à petit se répande. L'initiative est louable et sera efficace, mais uniquement sur le moyen terme, le temps que les étudiants rentrent sur le marché du travail et se forment pendant

quelques années avant de faire valoir son expérience.

Mais on est aujourd'hui dans une situation où sur le terrain, c'est assez critique.