Les cyberattaques ont changé de nature pendant le Covid-19

Rémy Février

Les cyberattaques ont changé de nature pendant le Covid-19

Rémy Février
Maître de Conférences en Sciences de Gestion - EESD, Conservatoire national des arts et métiers (CNAM)

Si les crises, en tant que vecteurs de destruction de valeur ou de cohésion sociale constituent souvent des opportunités de profits supplémentaires pour des délinquants habiles, l'avènement d'un monde hyperconnecté constitue un vecteur d'impact incomparable pour les cybercriminels.

Ces derniers tirent parti de l'ensemble des vulnérabilités offertes par l'utilisation des « systèmes d'information » (SI) par l'ensemble des organisations modernes. Toutefois, la crise actuelle du Covid-19 semble engendrer une rupture de paradigme dans ce domaine, non seulement par l'ampleur des attaques menées, mais surtout eu égard aux cibles choisies. Ainsi, même des organisations épargnées jusqu'alors en période de crise font dorénavant l'objet d'attaques massives et ce phénomène inédit conduit à s'interroger sur une nécessaire adaptation du management stratégique.

Des crises comme catalyseurs d'attaques

La crise de 2008 a constitué un tournant en tant qu'elle a induit de nombreuses cyberattaques contre des institutions (Dexia, Nasdaq) ou des particuliers (fausses opportunités d'investissements prenant prétexte des faillites, phishings visant à pirater des comptes…), toutefois celles-ci visaient principalement le secteur financier.

Une deuxième étape fut ensuite franchie à l'occasion des attentats terroristes de 2015, dans la mesure où immédiatement après les attaques contre *Charlie Hebdo* et l'Hypercacher, plus de 20 000 sites de collectivités territoriales et d'entreprises furent touchés principalement par du « défaçage » (technique consistant à modifier la page de garde d'un site Web). À cela se sont ajoutées fausses rumeurs et prises de contrôle à distance de smartphones. C'était la première fois qu'une crise civile autre qu'économique était utilisée par des cybercriminels.

Bien plus qu'une étape supplémentaire, la crise liée au coronavirus constitue une véritable rupture en matière de cyberdélinquance. Comme l'indique le rapport de mars

2020 d'Europol, jamais le nombre de cyberattaques n'a été aussi élevé : « L'impact de la pandémie Covid-19 sur la cybercriminalité a été le plus visible et le plus frappant par rapport à d'autres activités criminelles », sachant que le succès de ces arnaques repose en partie sur l'angoisse ressentie par de nombreuses personnes face au virus et qui se trouve exacerbé par le fait d'être confiné dans un espace clos. Les cyber-escroqueries se sont ainsi multipliées, à l'image de sites de vente de produits contrefaits (tests d'infection, masques, flacons de gel hydroalcoolique…).

Mais, au-delà des menaces pesant sur les individus, le travail à distance constitue une autre source majeure de vulnérabilité pour les organisations, étant donné que de nombreux salariés confinés utilisent souvent – que ce soit du fait de l'absence de matériel professionnel dédié ou par confort – leurs propres outils informatiques pour travailler à distance. Or ceux-ci ne faisant pas partie du système d'information de l'organisation, ils ne disposent pas des mêmes mesures de sécurisation que les matériels internes et leur usage est de nature à induire une pénétration du SI interne de l'entreprise. Le piratage de ces périphériques extérieur peut donc aller jusqu'à la destruction ou le vol de données à caractère stratégique ou personnel.

À cela s'ajoutent les vulnérabilités exploitées par les cyberpirates dans les outils de travail à distance à l'image du « Zoom bombing », procédé permettant de perturber le bon fonctionnement des téléconférences au travers notamment de messages injurieux et qui a fortement perturbé les cours à distance et les examens de plusieurs universités américaines (Oakland, Berkeley et Duke). La capacité offerte par cette faille de fausser les informations échangées a même conduit à l'émission, par l'agence américaine pour la cybersécurité et la protection des infrastructures (CISA), d'un bulletin d'alerte appelant à n'utiliser que des logiciels disposant d'un haut niveau de sécurité.

La crise du Covid-19 : un changement de paradigme

Mais, au-delà ce ces différents types d'attaques, force est de constater qu'avec la crise du coronavirus une barrière invisible est tombée en matière de cybercriminalité : jusqu'alors – vraisemblablement du fait de leur rôle d'acteurs majeurs de santé publique –, les établissements de soins constituaient des infrastructures bien moins soumises aux cyberattaques en temps de crise que d'autres organisations publiques ou du secteur marchand, attaquées quant à elles quasi-quotidiennement.

Depuis le début de la pandémie, les exemples d'attaques contre les systèmes d'information des hôpitaux et établissements de santé se multiplient dans de nombreux pays, alors même que personne ne peut dorénavant ignorer que de nombreuses vies sont en jeu. Ces intrusions constituent donc une évolution majeure en ce sens que désormais, même la vie humaine n'est plus respectée par certains groupes de hackers, *a*

contrario, du « Maze Team ransomware gang » qui a annoncé officiellement renoncer à toutes attaques de type Randsomware contre des hôpitaux durant toute la crise du Covid-19, mais quel crédit apporter à cette promesse ?
Alors que leurs personnels luttent chaque jour vaillamment pour sauver le maximum de vies, de nombreux hôpitaux ont été attaqués dans différents pays, tout comme des laboratoires spécialisés dans la recherche sur les vaccins. Mais à cela s'ajoute un autre phénomène nouveau : les atteintes aux organisations nationales et internationales de santé publique. Ainsi, le département en charge de la lutte contre le Covid-19 de l'agence fédérale américaine de santé (HSS) a été victime d'une cyberattaque en mars dernier, tout comme la sécurité sociale italienne (INPS), alors même que ces deux pays sont parmi les plus touchés au monde par l'épidémie.

Des hackers ont même cherché à utiliser le nom de l'Organisation mondiale de la Santé (OMS) pour tenter d'extorquer des informations personnelles à leurs victimes. Et tout pourrait n'être que marginal par rapport à ce qu'engendreraient des cyberattaques contre les systèmes d'information industriels des secteurs concernés.

Un nouveau cadre stratégique

Jamais l'analogie entre virus biologique et informatique n'a semblé aussi pertinente. Le concept de risque se jouant des frontières entre les disciplines, il nous semble indispensable d'analyser ce changement de paradigme du point de vue des sciences de gestion. En effet, s'il apparaît clairement qu'une organisation moderne peut difficilement faire l'économie de se positionner vis-à-vis des risques numériques et d'intégrer ces derniers dans sa réflexion stratégique, il apparaît que c'est encore très peu souvent le cas. L'augmentation spectaculaire des cyberattaques durant la crise du Covid-19 nous paraît de nature à induire une nécessaire réflexion sur la nécessité de mieux prendre en compte les organisations de hackers en matière de management stratégique au sein des organisations. Cette prise en compte structurelle des hackers par les décideurs constituerait une étape importante susceptible de favoriser la résilience numérique de l'ensemble des organisations publiques et privées et non plus seulement des opérateurs d'importance vitale.