La sensibilisation : une arme défensive majeure

Par **Jérôme NOTIN**
GIP ACYMA

Lancé en octobre 2017, le dispositif national d'assistance aux victimes Cybermalveillance.gouv.fr est issu de la stratégie numérique du gouvernement présentée en juin 2015 et dont les objectifs ont ensuite été détaillés dans la *Stratégie nationale pour la sécurité numérique* rendue publique en octobre 2015.

Cybermalveillance.gouv.fr a ainsi reçu une triple mission :

- la sensibilisation et la prévention par la diffusion de bonnes pratiques en cybersécurité et potentiellement la diffusion d'alertes contextualisées ;
- l'assistance aux victimes par une aide au diagnostic du problème, des conseils simples et adaptés, une orientation vers les services compétents, voire vers des prestataires spécialisés de proximité susceptibles de les assister ;
- l'observation de la menace afin de détecter les phénomènes émergents pour pouvoir les anticiper et y répondre.

Les publics du dispositif sont les particuliers, les entreprises, les collectivités et les associations, hors opérateurs d'importance vitale.

Il s'est organisé sous la forme d'un groupement d'intérêt public, le GIP ACYMA. Ce partenariat public-privé rassemble donc les acteurs de l'État et de la société civile engagés dans sa mission d'intérêt public de lutte contre la cyber-malveillance. On peut ainsi citer l'Agence nationale de la Sécurité des Systèmes d'Information (ANSSI), qui relève des services du Premier ministre, et le ministère de l'Intérieur qui ont copiloté sa conception, ainsi que le ministère de la Justice, le ministère de l'Économie et des Finances et le secrétariat d'État en charge du numérique. À leurs côtés travaillent de nombreux acteurs de la société civile comme des associations de consommateurs ou d'aides aux victimes, des représentations professionnelles de type fédération ou syndicat, des assureurs, des opérateurs, des constructeurs, des éditeurs… En juillet 2019, le groupement d'intérêt public est fort d'une quarantaine de membres. Outre leur soutien financier, ces membres renforcent et démultiplient les actions du dispositif.

Au fil du développement de son action, le dispositif Cybermalveillance.gouv.fr a pu démontrer, par son originalité et les services qu'il apporte, sa capacité à pouvoir répondre à une réelle attente de ses publics. En effet, près de 29 000 personnes sont venues rechercher de l'assistance sur la plateforme en 2018. Ce nombre de sollicitations a été multiplié par quatre entre les premiers mois et les derniers mois de cette année 2018, passant de 500 en janvier 2018 à près de 4 000 en fin d'année. Et sur les six premiers mois de l'année 2019, le dispositif a déjà assisté plus de 60 000 victimes. Cela représente donc le double de victimes par rapport à l'ensemble de l'année 2018 pour une durée divisée par deux. Cette très forte augmentation s'explique principalement par le fait que les publics concernés par le dispositif commencent à en connaître l'existence.

L'analyse de ces sollicitations et les échanges que le dispositif peut avoir avec son écosystème lui permettent d'adapter son action aux attentes et aux réalités du terrain, et en particulier sur ses actions de sensibilisation et d'alerte sur des menaces émergentes.

L'originalité du dispositif réside également dans le fait qu'il intervient généralement en amont des autres services de l'État lorsque la victime rencontre un incident. Il est en cela un capteur très intéressant pour les pouvoirs publics d'une certaine réalité de la cyber-malveillance pour des victimes qui n'envisagent pas en première intention de déposer plainte, soit parce qu'elles n'ont pas conscience que leur mésaventure pourrait faire l'objet de poursuites, soit parce qu'elles pensent que les poursuites dans la sphère cyber ont peu de chances d'aboutir et que leur démarche ne serait qu'une perte de temps, soit enfin parce qu'elles ont honte d'être victimes ou craignent pour leur image. Le dispositif intervient en incitant systématiquement la victime à déposer plainte chaque fois qu'une infraction pourrait être retenue, mais aussi en l'aidant dans sa démarche au travers des conseils prodigués qui sont élaborés en collaboration étroite avec le ministère de l'Intérieur.

Une des forces du dispositif est ainsi sa capacité à identifier des phénomènes à partir d'événements qui, parfois pris séparément, peuvent être considérés comme marginaux mais dont le rassemblement met en évidence le caractère sériel. C'est ainsi que le dispositif a pu contribuer à l'identification du phénomène cybercriminel de masse qu'est « l'arnaque au faux support technique » dès ses premiers mois de fonctionnement, au travers des rapports techniques d'intervention qui lui sont remontés par ses prestataires référencés. Dans la grande majorité des cas, si les victimes avaient bien eu l'impression à un moment ou un autre de s'être fait arnaquer, elles n'envisageaient généralement pas pour autant de déposer plainte, pour les raisons évoquées précédemment.

L'identification de ce phénomène cybercriminel et les échanges opérationnels qui ont pu être menés avec les services des ministères de l'Intérieur et de la Justice ont conduit à l'ouverture d'une enquête par la section de lutte contre la cybercriminalité du parquet de Paris en mars 2018. Cette enquête, confiée au centre de lutte contre les criminalités numériques (C3N) du pôle judiciaire de la gendarmerie nationale, a conduit à l'interpellation et à la mise en examen d'un réseau de trois individus ayant fait près de 8 000 victimes et à la saisie de près de 2 millions d'euros début février 2019.

Cette possibilité d'identification des menaces au plus près de leur apparition permet également au dispositif d'alerter les populations sur son site Internet et/ou ses réseaux sociaux (Twitter, Facebook, LinkedIn). Grâce au relais et à l'appui de ses membres, plusieurs alertes émises par le dispositif ont été largement reprises par les médias grand public (JT de 20h00), démultipliant ainsi les capacités d'atteindre le plus grand nombre de victimes potentielles.

Les TPE-PME : cibles de choix des cybercriminels

Même si elles ne sont pas exonérées du risque de subir des cyberattaques très variées, les grandes entreprises ou les grandes administrations se sont souvent armées pour y faire face, tant en matière de compétences qu'en moyens techniques. Il n'en est malheureusement pas toujours de même pour les petites et moyennes entreprises, ou les collectivités territoriales. Ces plus petites structures représentent donc une cible de choix pour les cybercriminels qui cherchent évidemment toujours à maximiser leurs profits avec un minimum d'efforts. Les conséquences de ces attaques peuvent être dramatiques pour ces plus petites organisations qui y jouent parfois leur survie économique.

On peut aisément admettre que la priorité d'une entreprise réside dans la réalisation de son activité, dont les systèmes d'information ne sont généralement considérés que comme le simple support. La numérisation des activités en fait pourtant une composante particulièrement critique pour les entreprises. Sans leur système d'information, la plupart des organisations ne peuvent tout simplement plus fonctionner et voient donc leur activité s'arrêter.

Pourtant, les services autour du système d'information sont souvent externalisés auprès de prestataires qui se livrent une concurrence féroce en tirant les prix vers le bas, ce qui est

évidemment toujours un argument très regardé par leurs clients. Cette logique économique va souvent de pair avec un niveau des prestations qui peut s'avérer amoindri, notamment en ce qui concerne le domaine de la sécurité.

De leur côté, les cybercriminels ont bien conscience de cette réalité et des vulnérabilités induites pour ces entreprises qu'ils vont pouvoir exploiter afin d'en tirer profit. Le temps est aujourd'hui révolu (ou presque) du stéréotype du « pirate » marginal, qui s'attaquait seul depuis sa chambre d'étudiant à une multinationale. Les entreprises doivent aujourd'hui faire face à un écosystème cybercriminel qui se structure et se spécialise en expertise et domaines de compétences. Certains groupes criminels se sont ainsi spécialisés dans la réalisation d'outils d'attaques de haut niveau, d'autres dans la recherche de failles ou d'accès dans les systèmes, d'autres encore les achètent pour les mettre en œuvre, d'autres enfin vont exploiter les résultats des attaques. Et sur le fameux *Darknet* dans lequel gravitent ces cybercriminels, tout se vend et tout s'achète.

Au travers des échanges qu'il peut avoir avec les victimes ou ses prestataires référencés, le dispositif Cybermalveillance.gouv.fr constate que les attaques conduites par les groupes cybercriminels sont de plus en plus « professionnelles » et que les dommages qu'elles occasionnent sont de plus en plus conséquents pour les structures qui les subissent.

Parmi ces attaques, celles par rançongiciels (*ransomware*) sont une bonne illustration de l'évolution des techniques et des capacités cybercriminelles. Si, initialement, ces attaques étaient généralement déclenchées à partir de simples pièces jointes ou liens malveillants contenus dans des messages d'hameçonnage (*phishing*) plus ou moins ciblés et mal rédigés, aujourd'hui les entreprises qui en sont victimes voient des modes opératoires radicalement différents les frapper.

Désormais, les cybercriminels cherchent par exemple à pénétrer directement les entreprises par leurs accès extérieurs, que ce soit par les accès de travail à distance ou de télémaintenance. Ils y parviennent soit en exploitant une faille logicielle non corrigée, soit en arrivant à « casser » des mots de passe insuffisamment solides.

Une fois dans la place, les cybercriminels peuvent parfois rester plusieurs jours dans le réseau de l'entreprise victime. Durant cette période de reconnaissance, ils vont cartographier le réseau pour repérer tous les actifs numériques importants. Dans certains cas, et si les cybercriminels y voient un intérêt, ces actifs peuvent être dérobés au passage pour être revendus à d'autres qui sauront en faire usage.

Une fois cette cartographie réalisée, les cybercriminels lancent la partie visible de leur attaque. Celle-ci se déroule généralement en dehors des heures ouvrées de l'entreprise qu'ils ont pu appréhender en l'observant. Ils commencent alors à chiffrer les données de l'entreprise en démarrant par… ses sauvegardes. Les cybercriminels ont bien compris que chaque entreprise a aujourd'hui peu ou prou des sauvegardes. Mais aussi que ces sauvegardes sont généralement, et par facilité, directement accessibles en ligne sur le réseau de l'entreprise qui n'a d'ailleurs souvent aucune autre copie récente de ses données.

À l'ouverture des bureaux de l'entreprise, toutes ses données sont chiffrées et les sauvegardes inaccessibles. Un message de demande de rançon l'attend. Cette rançon représente généralement une portion « acceptable » du chiffre d'affaires de l'entreprise au regard du préjudice qu'elle subit. De quelques centaines d'euros pour une TPE à plusieurs milliers d'euros pour des collectivités, et jusqu'à des centaines de milliers d'euros pour des PME de taille plus importante. Cette variabilité des rançons demandées en fonction des capacités de paiement de sa cible démontre bien que le cybercriminel qui commet l'attaque ne frappe plus au hasard, et qu'en amont et une fois dans la place, il a cherché à savoir quel montant maximal il pouvait extorquer à sa victime.

Les conséquences de ces attaques par rançongiciels ne se limitent pas à la perte financière de la seule rançon, que certaines victimes pourraient être enclines à payer. Il faut en effet toujours y ajouter le coût de la perte de production parfois durant plusieurs jours, liée à l'indisponibilité du système d'information de la victime, ainsi que celui des travaux de remise en état.

Ces exemples montrent qu'une entreprise logiquement focalisée sur son cœur de métier et sur sa réactivité opérationnelle peut se retrouver insuffisamment préparée à subir de telles attaques. Elle peut alors se retrouver désemparée quand elle tombe sous le joug de cybercriminels qui sont pour leur part de plus en plus « professionnels » dans leurs actions.

La sensibilisation : une arme défensive majeure

La sensibilisation reste la meilleure arme des entreprises et des collectivités pour éviter les cyberattaques. Dans le milieu professionnel, cette sensibilisation des employés aux cybermenaces et aux bonnes pratiques à adopter pour les détecter et les éviter est donc primordiale. Or, cela reste souvent un exercice difficile, car les sujets de sécurité numérique sont généralement ressentis comme rébarbatifs, peu parlants et sources de contraintes pour les utilisateurs. Et ce, quel que soit leur niveau dans l'entreprise : du dirigeant à l'employé, en passant par le cadre ou même « l'informaticien ».

C'est partant de ce constat issu des travaux conduits avec ses membres que le dispositif Cybermalveillance.gouv.fr a réalisé en 2018 le premier volet de son kit de sensibilisation pour les collaborateurs, le plus facile d'accès possible. Le kit complet a été finalisé en juin 2019. Il peut être téléchargé gratuitement sur la plateforme du dispositif [1]. Il comprend différents types de supports (courtes vidéos, infographies, fiches pratiques, mémos…). Il s'adresse au collaborateur à propos de ses usages personnels de manière pédagogique et illustrée, sur des sujets qui peuvent également intéresser l'entreprise dans ses usages professionnels. Par exemple, si un collaborateur sait détecter et réagir à un message d'hameçonnage (*phishing*) dans ses usages personnels, il saura également le faire dans ses usages professionnels. Dans ce kit, différents thèmes sont abordés : l'hameçonnage qui est le principal vecteur d'attaque aujourd'hui ; la bonne gestion des mots de passe qui reste une des principales protections des systèmes ; la sécurité des appareils mobiles (smartphones, tablettes) qui présentent des vulnérabilités spécifiques importantes ; la différenciation des usages professionnels et personnels, etc.

Un choix fort a été de le publier sous licence Etalab 2.0. Cette licence permet à toute entité de le modifier, et donc d'ajouter ou de supprimer du contenu. Beaucoup de structures ont par exemple simplement ajouté le logo de leur entité afin que l'adhésion des collaborateurs soit encore plus forte.

Enfin, au titre de la prévention et de la sensibilisation, on peut également citer la préparation à la gestion de la crise qu'engendre pour une entreprise toute attaque informatique majeure. Force est de constater que les entreprises, surtout les plus petites, sont généralement insuffisamment préparées pour affronter ces situations difficiles et pour elles exceptionnelles. De nombreux conseils en première intention sont disponibles sur la plateforme Cybermalveillance.gouv.fr sur les principaux types d'attaques.

La question pour une entreprise n'est donc plus aujourd'hui de savoir si elle sera attaquée, mais quand ?, et si elle est suffisamment préparée pour l'empêcher ou y faire face. Car malheureusement, la cybermalveillance, cela n'arrive pas qu'aux autres.

(1) https://www.cybermalveillance.gouv.fr/contenus-de-sensibilisation/.