TRIP printemps 2022

1er & 2juin

Allocution de Jérôme NOTIN, Cybermalveillance.gouv.fr

Jérôme NOTIN, Directeur général de Cybermalveillance.gouv.fr

(Retranscription, seul le prononcé fait foi)

Jérôme NOTIN, Directeur général de Cybermalveillance.gouv.fr

Le dispositif d'assistance aux victimes d'actes de cybermalveillance a été créé par l'ANSSI (Agence nationale de la sécurité des systèmes d'information) et le ministère de l'Intérieur en 2017 pour traiter ce que l'ANSSI n'adresse pas.

En effet, l'ANSSI, autorité nationale en termes de cybersécurité, s'adresse aux opérateurs d'importance vitale et également aux opérateurs de services essentiels aujourd'hui. Mais pour tous les autres publics, notamment les collectivités, les particuliers et les entreprises qui ne sont pas réglementées, il n'y avait pas de solution. Il a donc été annoncé dans la stratégie nationale pour la sécurité du numérique en 2015 la nécessité de mettre en place un dispositif d'assistance, d'où la naissance de notre dispositif.

Allocution de Jérôme NOTIN, Cybermalveillance.gouv.fr

Jérôme NOTIN, Directeur général de Cybermalveillance.gouv.fr

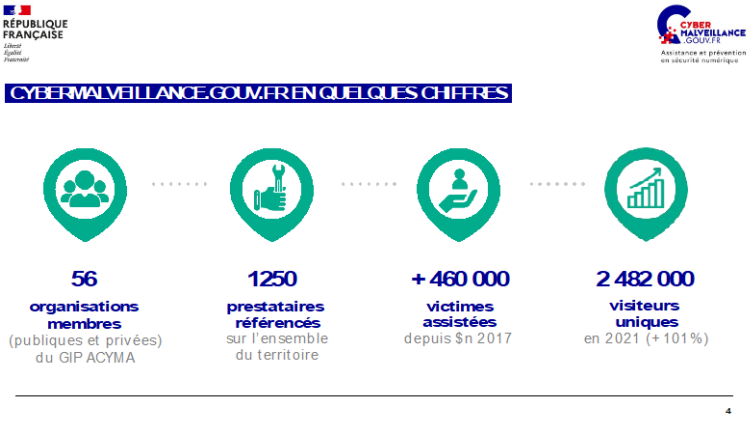
Ses missions sont au nombre de trois.

La première est l'assistance : vous êtes une collectivité victime de cybermalveillance et vous ne savez pas quoi faire. À l'aide de mots clés dans un moteur de recherche, vous allez décrire la cybermalveillance et, si le travail de référencement a été bien fait, vous atterrirez sur notre plateforme et pourrez obtenir des conseils. Une autre approche consiste à faire ce que nous appelons un « parcours victimes », c'est-à-dire que nous posons quelques questions aux victimes afin de qualifier l'incident de cybersécurité et le diagnostiquer. En fonction du diagnostic, nous donnons des conseils pour permettre de résoudre la problématique ; mais lorsque nous considérons que la solution est technique, nous sommes en capacité de proposer la mise en relation avec un prestataire de proximité. C'est la grande originalité de ce dispositif, il n'y en pas d'autres qui fasse cette démarche dans le monde. Le fait qu'une plateforme « .gouv.fr » puisse mettre les victimes en relation avec des prestataires a été philosophiquement assez compliqué à accepter par nos géniteurs, mais nous le faisons, et plutôt très bien !

Deuxième mission, pour faire en sorte que les structures ne soient pas victimes, il est nécessaire de créer des contenus de sensibilisation. Nous verrons quelques exemples de contenus que nous avons pu produire, assez génériques ou destinés aux collectivités.

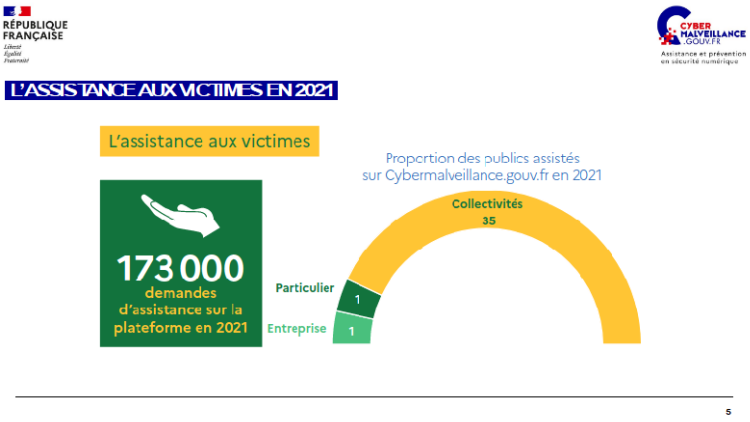
Et puis, afin d'éclairer les pouvoirs publics ou de clarifier nos actions de sensibilisation et de prévention, la troisième mission est l'observation du risque, qui est fondamentale. Aujourd'hui, absolument personne n'est capable de dire combien d'entreprises meurent, combien de collectivités sont bloquées… Nous avons des idées de chiffres mais pas de données précises. La mise en place de cet observatoire est donc aussi un enjeu important pour nous.

Pour porter ces missions, un groupement d'intérêt public a été créé en 2017 avec un collège étatique majoritaire : l'ANSSI (membre fondateur dont le directeur général Guillaume Poupard est le président du GIP), les ministères de l'Économie, de l'Intérieur, de la Justice, de l'Éducation nationale, et des Armées (qui n'est pas membre fondateur). Et puis à côté (sur la droite de la diapositive), un collège privé : vous reconnaissez les logos de l'Avicca, membre très actif que je remercie à nouveau de participer à nos travaux, la Banque des Territoires, Orange à travers Orange Cyberdéfense qui est membre du dispositif, des assureurs, des fédérations, des syndicats, le Medef, la CNIL qui nous a rejoints au 1er janvier, l'AMF également, etc. Soit un panel de structures représentant tout le monde économique et la société civile, puisqu'il y a aussi des associations de consommateurs comme l'INC et l'UFC Que Choisir.



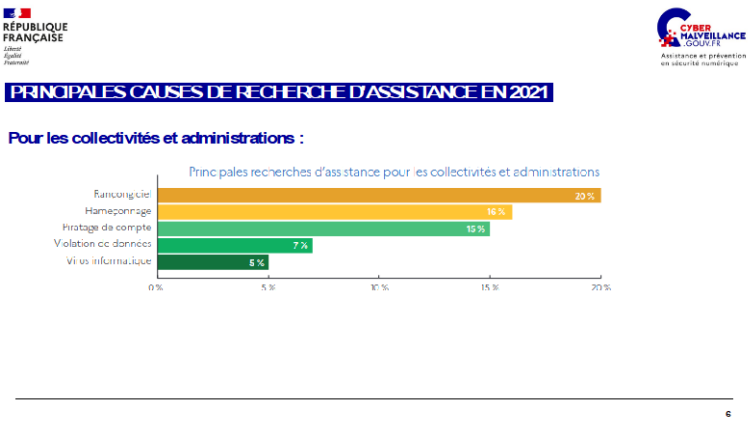
56 structures sont membres du dispositif. Les prestataires référencés et en capacité d'aider les entreprises et les collectivités sont au nombre de 1 250. Depuis la naissance du dispositif en 2017, nous avons réalisé 460 000 parcours, jusqu'au diagnostic et possiblement la mise en relation avec un prestataire.

L'année dernière nous avons doublé, comme tous les ans, le nombre de visiteurs sur la plateforme avec 2 482 000 visiteurs uniques en 2021. Pour 2022, au 1er juin, nous avons dépassé 1,5 million depuis le début de l'année et l'augmentation est toujours importante.



173 000 parcours victimes ont été réalisés sur l'année 2021. La première question que nous posons est de savoir si la victime est une entreprise, un particulier ou une collectivité.

Il y a 90% de parcours particuliers, mais nous savons qu'il y a 40 ou 50 millions d'utilisateurs particuliers du numérique en France, 3 ou 4 millions d'entreprises (y compris les associations), et un peu plus de 35 000 collectivités. Si l'on rapporte le nombre de parcours d'assistance à ces volumes, pour un particulier aidé, nous avons aidé 1,2 à 1,3 entreprises et 35 collectivités. Cela veut dire que, soit les collectivités nous connaissent davantage, malgré notre défaut de notoriété dû à un budget très limité qui ne nous permet pas de faire beaucoup d'actions de communication, même si nos membres (dont l'Avicca) relaient notre existence et notre offre de services ; soit les collectivités sont massivement attaquées, ce qui est bien évidemment le cas. Mais il existe des solutions.



Il est possible de qualifier l'incident que la structure a rencontré. Le détail des parcours victimes montre que les rançongiciels (20%) représentent la première menace, sans surprise car c'était déjà le cas en 2020. Il s'agit de bouts de logiciels qui vont télécharger les données avant de les chiffrer et de rendre inopérants les systèmes d'informations. Ensuite, viennent l'hameçonnage, très important également (16%) pour les entreprises et les particuliers ; le piratage de comptes (15%) ; la violation de données (7%) et les virus informatiques (5%). Tous ces éléments peuvent se retrouver dans notre rapport d'activités.

Vous n'êtes pas seuls, nous avons été créés par le Gouvernement et avec des membres prestigieux pour vous. Dès le début du dispositif, nous avons conçu un kit de sensibilisation avec beaucoup de contenus - une nouvelle fiche est encore sortie la semaine dernière.

La particularité de ces contenus est d'être sous licence ouverte (Etalab 2.0). Cela signifie que vous pouvez utiliser le contenu, et que vous pouvez également télécharger le code source des pdf et y

ajouter votre logo. De nombreuses collectivités l'ont fait pour des usages internes : lorsque l'agent d'une collectivité voit la Marianne, le logo de Cybermalveillance plus le logo de sa collectivité, cela l'interpelle et il prête davantage attention au contenu.

Les collectivités sont un sujet d'importance pour nous depuis plusieurs années. Nous avons donc créé un groupe de travail spécifique vertical (ou métier) que nous appelons GT collectivités, qui a aussi produit de nombreux contenus à l'attention des collectivités. Un premier volet porte sur les principales menaces ; un deuxième volet comprend des témoignages de collectivités ayant subi des actes de cybermalveillance ; et un troisième volet, des témoignages de structures ayant mis en place des actions de sensibilisation pour leurs publics.

L'outil « Alertes cyber » a été lancé par Cédric O à l'été 2021. Il a vocation à informer les entreprises et les collectivités lorsqu'on détecte une vulnérabilité de sécurité importante dont le score de dangerosité est élevé, qui touche potentiellement beaucoup de publics, et dont l'exploitation est en cours (c'est-à-dire que des individus ont démontré qu'ils avaient déjà exploité cette vulnérabilité pour compromettre des systèmes d'information).

Ces alertes cyber ne sont lancées que lorsqu'il existe une solution, c'est-à-dire un correctif - en général, il s'agit d'une mise à jour du produit, souvent des systèmes d'exploitation (Apple, Android, Microsoft…).

Si vous recevez cette alerte, ce n'est pas de l'hameçonnage (même s'il faut bien vérifier le « mail from »). Elle est par ailleurs publiée sur notre plateforme et, au moindre doute, vous pouvez donc vérifier qu'il ne s'agit pas d'une tentative d'hameçonnage. L'AMF nous a rejoint en ce début d'année pour diffuser cette alerte.

En septembre dernier, nous avons développé avec l'AMF et le ministère de l'Intérieur (la gendarmerie principalement) un outil d'auto-évaluation appelé « I.M.M.U.N.I.T.É CYBER ». Cet outil consiste en un questionnaire en 9 points. Si en tant qu'élu d'une collectivité, DGS, ou autres, vous répondez non à une de ces questions, vous êtes invité à prendre contact avec la gendarmerie locale qui réalisera des actions de sensibilisation.

La gendarmerie est très impliquée dans ces sujets et pourra vous fournir des recommandations ; l'objectif étant que vous soyez ensuite capable de répondre correctement au questionnaire.

Nous avons également conçu l'affiche « Que faire en cas de cyber attaque ? » https://www.cybermalveillance.gouv.fr/tous-nos-contenus/bonnes-pratiques/cyberattaque-que-faire-guide-dirigeants. L'ANSSI publie des guides techniques extrêmement bien faits mais qui s'adressent à des spécialistes. Ici, nous avons repris les mesures d'urgence phares (« Que faire en cas de cyberattaque ? »), le tout étant validé par l'ANSSI. Ensuite, il faut faire appel à un prestataire sur notre plateforme, si l'on ne dispose pas dans son entourage d'un prestataire en capacité d'aider.

Une campagne de vidéos est en cours, dont le premier épisode a été diffusé aujourd'hui. Cela fait partie d'un des travaux que nous avons menés suite à la réalisation d'une étude sur la perception du niveau de maturité des collectivités de moins de 3 500 habitants.

Au-delà des chiffres, cette étude montre qu'il existe de nombreux préjugés classiques des collectivités sur la cybersécurité : « je ne suis pas concerné » ; « je n'ai pas le budget » ; « ce n'est pas ma priorité » ; « je n'ai pas le temps ». Nous avons décliné des Fables de La Fontaine dans de

courtes vidéos pour essayer de lever ces préjugés. N'hésitez pas à les consultez et à les diffuser dans vos collectivités.

Un autre travail est issu de l'étude menée sur les collectivités de moins de 3 500 habitants pour remédier au défaut de perception de la réglementation. Avec la CNIL, membre du dispositif depuis le 1er janvier, nous réalisons un guide qui devrait paraître avant l'été rappelant les obligations légales par rapport au RGPD, mais pas uniquement. Cet outil pourra vous éclairer et vous aider dans vos missions.

Lien https://www.cybermalveillance.gouv.fr/tous-nos-contenus/actualites/cybermalveillance-gouv-fr-et-la-cnil-publient-un-guide-sur-les-obligations-et-les-responsabilites-des-collectivites-locales-en-matiere-de-cybersecurite

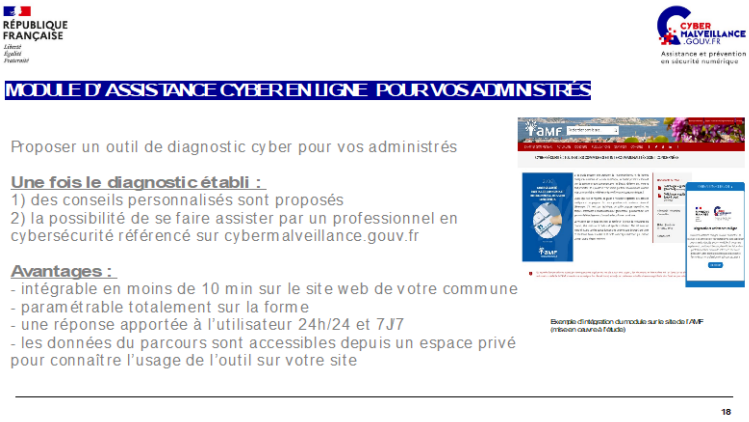
Pour sécuriser, nous avons vu qu'il y a la sensibilisation de l'ensemble des utilisateurs, des agents des systèmes d'information au sens très large, et il y a les aspects techniques. J'ai déjà évoqué les

1 250 prestataires qui sont en capacité d'assister nos victimes, mais ces prestataires n'étaient pas évalués techniquement, parce que leurs publics vont des particuliers jusqu'à de grandes collectivités ou entreprises.

Assez vite, nous avons donc créé au sein du dispositif, avec les fédérations et les syndicats représentants ces prestataires de proximité, un label avec le soutien de l'Afnor. Ce label garantit que le prestataire de proximité dans les territoires est à l'état de l'art par rapport à ce qui doit se faire et par rapport aux besoins des collectivités de petites tailles.

Plus de 200 prestataires sont labellisés « ExpertCyber »à ce jour, sachant que cette démarche a été lancée le 18 février 2021. Les prestataires sont évalués sur une capacité de remédiation, c'est-à-dire d'assistance, mais également sur une capacité d'accompagnement à la sécurisation. Dans le cadre du respect du code des marchés publics, je ne peux que vous inviter à solliciter ces prestataires sur vos projets de sécurisation, parce qu'ils sauront ce qui doit être fait et comment le faire correctement.

Pour les administrés, nous avons réalisé des vidéos assez amusantes et décalées dont vous découvrez sur cette diapositive les visuels (qui peuvent être utilisés). Les vidéos sont aussi disponibles et peuvent être diffusées d'une manière ou d'une autre au sein de vos collectivités.



Enfin, le parcours victimes que nous avons développé a vocation à être intégré dans un module sur toutes les plateformes web de vos collectivités. C'est une annonce que nous ferons la semaine prochaine au FIC (Forum international de la cybersécurité) : 10 de nos membres auront intégré sur leur site ce module qui permettra aux visiteurs de suivre ce parcours, de répondre aux questions, etc. À la fin, un diagnostic sera émis, accompagné de conseils, et il sera possible d'être mis en relation avec un prestataire de proximité.

Notre volonté est d'offrir au maximum de visiteurs une visibilité sur notre dispositif et la possibilité de bénéficier de nos services. L'Avicca fait partie de ces 10 premières structures à proposer cet outil de diagnostic cyber, et je l'en remercie très sincèrement. Mais ce service a évidemment vocation à être déployé le plus massivement possible.

Le Corbeau et le Renard (vidéo) : https://www.youtube.com/watch?v=HaiSXrzBz_M