Je pense qu'il y a effectivement un manque de prise de conscience, un utilisateur classique n'a pas forcément conscience qu'en utilisant un outil numérique, s'il ne prend pas certaines mesures de base, il peut se mettre en borgée sur Internet.
Nous sommes tous des victimes potentielles des pirates informatiques et aujourd'hui le cyber-piratage prend de très nombreuses formes, on le sait.
Alors ce mois-ci, octobre 2023, c'est le cyber mois, une nouvelle édition du mois de la cyber sécurité, lancée par les instances européennes spécialisées dans la cyber-sécurité.
Ça nous concerne tous, particuliers, petites entreprises, collectivités locales, etc.
On en parle avec le directeur de la plateforme gouvernementale cybermalveillance.gouv.fr Jérôme Notin, bonjour, pouvez-vous nous rappeler exactement ce qu'est le cyber mois ?
Le cyber mois, c'est une initiative qui a aujourd'hui 11 ans.
Historiquement, ça a été lancé par l'ENISA, qui est l'Agence européenne de sécurité des systèmes d'information. Et puis chaque pays a, à travers son autorité nationale, des légations pour organiser des actions pour sensibiliser les publics.
En général, on pense aux grands publics. L'année dernière, nous avons eu le privilège avec l'NSI de copiloter cette action, le cyber mois, l'European Cyber Romance.
Et cette année, notre dispositif, parce que nous sommes orientés à plutôt petites victimes, c'est-à-dire les particuliers, plutôt les TPE, PME, plutôt les petites collectivités.
Donc nous avons pris le pouvoir, si je puis dire, sur l'organisation du MROPIN cyber sécurité.
Donc nous avons réuni un collectif évidemment avec les membres du groupement d'intérêt public, mais pas que. Donc un collectif qui a vocation à travailler, qui a travaillé ensemble pour faire que, pendant ce mois européen de la cyber sécurité, on sorte un petit peu de notre sphère et notre écosystème de cyber et qu'on aille à la rencontre des publics qui, pour certains, n'ont pas encore saisi tous les enjeux de cyber sécurité.
Vous pensez qu'on sous-estime la menace aussi bien du côté des particuliers que des petites entreprises ? Je pense qu'il y a effectivement un manque de prise de conscience. On est tous utilisateurs, que ce soit à titre personnel ou à titre professionnel d'outils numériques, et on n'a pas forcément, alors nous évidemment si, mais un utilisateur classique n'a pas forcément conscience qu'en utilisant un outil numérique, s'il ne prend pas certaines mesures, et l'idée c'est pas de monter des fornotes numériques ou d'être extrêmement paranoïaque, mais si il ne prend pas certaines mesures de base, eh bien il peut se mettre en bongée sur Internet.
Si on prend toujours un petit peu dangereux, mais si on prend l'image de la sécurité routière, aujourd'hui on sait que quand on prend ses longs véhicules, on doit être agent, on doit mettre sa ceinture de sécurité, on doit respecter la signalisation. Malheureusement, encore beaucoup trop de personnes à titre privé, mais à titre professionnel également n'ont pas conscience qu'il faut, quand on nous propose des mises à jour, faire les mises à jour, quand on a des données qui sont assez sensibles, les sauvegarder, déconnecter les sauvegardes de son réseau, pour que si jamais on est victime par exemple de ronds songeiciels, et on sait que c'est une menace donc depuis le nombre de années qui adressent les collectivités et les entreprises, donc c'est une vraie menace qui a du sens, parce qu'elle peut bloquer vraiment l'activité de la structure, et donc voilà, si on a une sauvegarde déconnectée, pas trop ancienne, et bien si on est victime de ronds songeiciels, on va pouvoir réinstaller un système d'information propre, une fois qu'on aura conservé l'épreuve pour les épaules teintes, et une fois qu'on aura possiblement

identifié le vecteur de compromissions, c'est-à-dire comment les civerculiaires sont entrés, donc on va pouvoir installer un système d'information propre et réinstaller ces sauvegardes, j'espère pas trop ancienne. Alors malgré tout, on voit que les incidents se multiplient, les victimes sont toujours plus nombreuses, entreprises ou particuliers, est-ce que quand on est victime d'une chantal ou d'un vol de données, d'une usurpation de mot de passe et ensuite de vol d'argent, et qu'est-ce qu'on peut faire, alors on n'a plus que ses yeux pour pleurer en fait.
Alors la première des choses c'est qu'on va sur cibermalveillance.gov.fr, donc là on va pouvoir, soit si on a su qualifier la menace et à travers des moteurs de recherche, pouvoir qualifier, normalement on a un article qui correspond à cette menace où on offre la possibilité aux victimes, particuliers, entreprise ou collectivité, de faire ce qu'on appelle un parcours d'assistance, c'est-à-dire qu'on va lui poser quelques questions, on va qualifier la menace et on va lui donner les conseils. Donc ces conseils peuvent aller jusqu'à potentiellement une mise en relation avec des prestataires de proximité, nous avons 1200 prestataires de proximité sur le territoire national dont certains sont labélisés, on a également créé un lavel, et donc voilà quand c'est une remédiation qui est considérée comme technique, il y a les premiers conseils en première intention et puis la possibilité d'être mise en relation avec un prestataire. J'évoquais tout à l'heure l'intérêt du dépôt de plainte, il est aussi fondamental pour ne pas dire citoyen de déposer plainte parce que plus les services d'enquête disposeront de plainte et donc d'éléments techniques, plus ils auront une capacité d'identification des auteurs et donc de faire possiblement cesser les infractions. Alors on voit que de plus en plus des hôpitaux ou des collectivités locales aussi, des mairies sont attaquées, pour quelle raison ? Les collectivités locales sont la cible des cybercriminels, on a souvent des questions d'élus, des collectivités de DGS ou autres qui nous disent mais pourquoi ils nous attaquent nous ? On n'a pas d'argent, on sait
que les collectivités n'ont pas forcément beaucoup d'argent, on sait qu'elles ne peuvent pas et c'est tant mieux payer des rensoins si par exemple on est victime de rensoins juiciels mais on sait également
et les cybercriminels le savent également que les collectivités disposent des données désadministrées,
c'est une richesse, c'est une mine d'informations, c'est de l'or pour ces gens là, ils vont collecter s'ils ont compromis un système d'information d'une collectivité, petite ou grande, ils vont collecter le nom, le prénom, la date de naissance, éventuellement le numéro de sécu et éventuellement le cof familial,
l'adresse mail, éventuellement les coordonnées bancaires donc beaucoup d'informations qui ensuite vont être revendues à d'autres groupes cybercriminels pour faire des attaques très personnalisées, pour ne pas dire ciblés en tout cas très personnalisées auprès de ces victimes et qui vont beaucoup plus facilement tomber dans le panneau et là pour le coup répondre favorablement un appel téléphonique d'infos conseillés bancaires, cliquer sur un lien très personnalisé donc qui va envoyer sur une page qui contient des infos où ils vont enrichir d'autres informations donc c'est toujours très imprimantal tout ça, donc voilà la donnée détenue par la collectivité, elle a beaucoup de valeur pour être revendue ensuite à d'autres groupes de cybercriminels.
Avant les cyberattacks, le risque c'était d'attraper un virus qui allait bloquer notre ordinateur, aujourd'hui on voit se multiplier des attaques qui sont plus humaines entre guillemets,

ça passe par le spam téléphonique, les sms et même les appels téléphoniques avec des vrais gens au bout du fil, comment lutter contre ça ? C'est vous l'avez dit effectivement il y a non un coutume de dire que la mère de boucée d'attaque c'est l'amsonnage, l'amsonnage c'est on va vous inviter à faire une action pour que vous tombiez dans le panneau et que vous délivriez des informations,
l'amsonnage il y en avait relativement peu il y a encore quelques années, là c'est la première menace pour l'ensemble de nos publics, que ce soit les particuliers, les entreprises ou les collectivités,
donc là c'est pour ça pourquoi les gens viennent chercher de l'assistance chino, parce qu'on l'a dit c'est quelque chose qui va leur permettre d'avoir des éléments très personnalisés,
et si moi je vous appelle, je vous dis vous êtes jérôme koumomba, est-ce que vous êtes bien nés là ? Est-ce que votre numéro de carte de bancaire c'est bien celui-ci ? Est-ce que votre numéro de carte bancaire c'est bien celui-ci ? Il y a de fortes chances que vous répondiez oui, que vous soyez en confiance, et par contre en deuxième intention je vais vous dire oh mon pauvre monsieur koumomba, vous êtes victime d'une fraude, en ce moment sur votre compte je vais vous
envoyer des codes, vous allez me les donner, on va annuler toutes ces opérations, et comme ça vous serez remboursé par nous la banque, puisque bien évidemment je me présente comme le service fraude,
donc voilà, il y a un niveau de, il y a une première phase de collecte d'informations qui peut être automatisé, et ensuite comme on va faire de beaucoup de victimes avec un taux de réussite important, parce qu'on aura cette information qui va mettre en confiance la victime, et bien ça vaut le coup d'avoir cette activité si je peux me permettre, si on a vraiment sur un point de vue financier, ça vaut le coup d'avoir cette activité cybercriminale, parce qu'on peut générer quand même beaucoup beaucoup de revenus. Alors est-ce qu'on peut malgré tout rester optimiste et espérer
faire baisser cette cybermenace, Jérôme Notain ? On peut faire baisser cette cybermenace, ça coûte pas cher, ça coûte quelques bonnes pratiques au sein des structures, ça coûte un petit peu d'argent en faisant rappel à un prestataire qui va sécuriser le système d'information. On peut dire qu'il y a nos amis britanniques, moi j'adore leur approche, qui ont une doctrine donc qui s'appelle
active cyberdefence. L'idée c'est de dire, nous collectivement au niveau britannique, on doit être un petit peu meilleure que les autres, parce que les cybercriminels ce sont des gens feignants, et si les britanniques sont bien sécurisés, les cybercriminels iront attaquer d'autres pays. Et je pense que quand on est, alors à titre particulier, c'est un petit peu plus compliqué, mais quand on est un chef d'entreprise ou un responsable dans une collectivité, on doit avoir cette démarche. L'idée c'est d'être vraiment un tout petit peu meilleur que les autres et de résister aux attaques, parce que c'est de la pêche au chavu en général, et que c'est relativement facile de s'en protéger si on a respecté les bonnes pratiques. Par exemple, on a adhéré à la charte qu'on propose en ce mois d'octobre 2023, qui est une sorte de guide pour justement faire qu'on soit un petit peu mieux protégé. Et donc je pense que ça peut apparaître comme égoïste, mais si collectivement on fait tout cela, et bien si Jérôme C est mieux protégé que Jérôme N le lundi, et que le
mardi Jérôme N, alors c'est des temps plus longs, même si on est dans ton cours en cibère, mais

vous voyez l'idée, Jérôme N ensuite va devoir se protéger et incrémentalement on va mieux être protégé. En étant mieux protégé, on va augmenter la difficulté auprès des cybercriminals s'ils veulent vraiment nous attaquer, et quand on augmente la difficulté, il y a plus de chances de faire des
erreurs, et donc quand ils font des erreurs, on peut plus facilement les identifier et les interpeller. Alors à l'occasion de ce cyber mois d'octobre 2023, vous lancez un certain nombre d'initiatives, Jérôme Notain, cibermalveillance.gov.fr, quels sont elles? Différentes initiatives,
alors ça commence par par exemple sur notre plateforme le référencement de différents événements qui peuvent avoir lieu à Paris, mais surtout en province, qui sont ouverts au public et qui permettent justement de faire qu'on puisse aller à la rencontre des gens qui parlent cyber sécurité. Le 2 octobre, nous avons une action coup de poing sur les réseaux sociaux, il y a différentes vignettes qui peuvent être récupérées et qui ensuite peuvent être diffusées sur les réseaux sociaux, un peu pour forcer les algorithmes de ces réseaux sociaux à faire que les mois, enfin le hashtag cyber responsable en fait, apparaissent au niveau du maximum de pages,
et puis plutôt à destination des professionnels, nous avons une charte de 8 engagements qui est disponible et qui permet pour un patron d'entreprise, pour un élu dans une collectivité, de comprendre
en fait quelles sont les premières mesures à mettre en place. Là je parle plus aux gens qui ont compris, qui ont compris, qui ont un vrai intérêt à se sécuriser, mais qui ne savent pas comment forcément faire. Moi j'ai un exemple que j'aime beaucoup, c'est dans la structure nommer un référent cyber sécurité. On sait que les petites structures ont très rarement des DSI,
donc sans parler de chaînes de cyber sécurité, donc par contre il peut y avoir dans la structure publique privée, une personne un peu geek qui est un peu meilleure en tout cas à plus d'apétence à aborder ces sujets d'informatique en ce sens large et en particulier de cyber sécurité,
et donc si on nomme une personne référente au sein de sa structure, eh bien quand un agent d'une collectivité, quand un collaborateur d'une entreprise a un doute sur un email,
a un doute sur le comportement de sa machine, eh bien elle pourra aller voir cette personne,
donc le référent lui poser les questions et assez naturellement voir si effectivement il y a un problème. Et on peut aussi bien sûr aller sur cybermalveillance.gouv.fr, la plateforme que vous dirigez, Jérôme Notin, merci beaucoup.
Sous-titrage ST' 501