canton de vaud
LIBERTÉ ET PATRIE

Direction générale du numérique et des systèmes d'information

Avenue de Longemalle 1
1020 Renens

Evolution des cybermenaces – Rappel des règles essentielles de prévention

Renens, le 15 octobre 2021

Cyberrésilience : rappel des mesures principales de prévention pour mieux faire face aux cyberattaques

Mesdames les Syndiques, Messieurs les Syndics, Mesdames les Municipales, Messieurs les Municipaux, chères Mesdames, chers Messieurs,

Comme l'actualité ne cesse de nous le rappeler, l'augmentation des cyberattaques n'épargne pas notre canton. Alors que les communes vaudoises apparaissent de toute évidence comme des cibles pour les pirates, Mesdames Christelle Luisier et Nuria Gorrite, conseillères d'Etat en charge respectivement des relations avec les communes et du numérique, ont proposé à l'UCV et l'AdCV la tenue d'une séance le 11 novembre afin de renforcer le dialogue Canton-Communes en matière de cybersécurité.

Dans l'intervalle, nous vous adressons ce courrier pour rappeler les mesures de prévention et de réaction, dont l'application permet de réduire l'impact sur nos administrations en cas de cyberattaque. Ces conseils viennent s'ajouter à ceux donnés dans le cadre du programme « Au top pour ma commune », destiné aux personnes nouvellement élues.

En cas d'attaque, la permanence Cybercriminalité de la police cantonale est joignable au 117. Nous joignons aussi à ce courrier un récapitulatif des mesures urgentes à prendre dans une telle éventualité.

Pour information, les cybercriminels ont en effet trouvé un filon qu'ils exploitent aujourd'hui sans réserve : les attaques par rançongiciels. Ces dernières ne cessent d'évoluer, mais, en résumé, elles consistent à s'introduire dans un système informatique en profitant d'une ou de plusieurs vulnérabilités comme, par exemple, un e-mail contenant une pièce jointe avec du contenu malicieux. Passée cette étape, les pirates cherchent alors, de manière plus ou moins automatisée, à chiffrer des fichiers ou des bases de données pour les rendre indisponibles et demander ensuite le paiement d'une rançon contre les clés de chiffrement. A noter qu'ils profitent aussi parfois de dérober les données accessibles en masse pour mettre davantage de pression sur les victimes, les menaçant de les divulguer si elles ne paient pas une rançon qui ne cesse d'être augmentée chaque jour.

Il est tout aussi nécessaire de rappeler, dans ce préambule, qu'une cyberattaque n'est pas une maladie honteuse et que, pour les pirates, une seule vulnérabilité peut permettre de compromettre tout un système informatique. En résumé, personne n'est intouchable et le risque zéro n'existe pas en matière cyber.

Toutefois, comme le précise le Centre national pour la cybersécurité, le NCSC, **il est indispensable de s'assurer de la mise en place des 5 mesures de prévention suivantes contre les cyberattaques** :

1) Sécurisation des accès à distance : les accès à distance, comme le VPN, le RDP ou autres, ainsi que tous les autres accès aux ressources internes (par ex. messagerie électronique, Sharepoint, etc.) doivent obligatoirement être sécurisés avec un second facteur (authentification à deux facteurs). Concrètement, les personnes souhaitant accéder à ces ressources à distance devront renseigner non seulement leurs identifiants (premier facteur), mais aussi un code à usage unique supplémentaire (second facteur) – par exemple un SMS. **L'authentification forte devrait aujourd'hui être une obligation pour les accès à distance.**

2) Sauvegardes hors ligne : il est nécessaire de créer régulièrement des copies de secours de vos données. Pour cela, un principe des générations (quotidien, hebdomadaire, mensuel - au moins deux générations) doit être utilisé. Il s'agit aussi de s'assurer à chaque fois que le canal sur lequel sont effectuées les copies de secours est physiquement séparé de l'ordinateur et du réseau, et protégé après l'opération de sauvegarde.

3) Gestion des correctifs et des cycles de vie des actifs informatiques : en matière de sécurité, tous les systèmes doivent être systématiquement et régulièrement mis à jour pour éviter en particulier que des cybercriminels puissent exploiter des vulnérabilités et voler par exemple des informations de connexion. Les logiciels ou les systèmes qui ne sont plus actualisés par le fabricant (fin de vie) doivent être désactivés ou transférés dans une zone du réseau séparée et isolée.

4) Blocage des pièces jointes et des liens à risque dans les courriels : la messagerie électronique reste un canal privilégié d'attaque pour les cybercriminels, raison pour laquelle il est nécessaire de bloquer la réception de pièces jointes dangereuses sur votre messagerie, y compris les documents Office avec macros. La sensibilisation et la formation de vos collaboratrices et collaborateurs à reconnaître les courriels suspicieux, par exemple avec des exercices de prévention du phishing, est essentielle.

5) Surveillance des fichiers journaux (logs) : une surveillance continue de l'environnement IT et des changements au sein de celui-ci est une nécessité pour réagir rapidement et ainsi réduire les impacts d'une cyberattaque. En particulier, surveiller les accès à distance, les accès à Internet et les droits définis dans l'Active Directory (le service d'annuaire de Microsoft, qui centralise l'identification et l'authentification d'un réseau) est essentiel.

Nous sommes conscients que de nombreuses communes externalisent l'exploitation et la maintenance de leurs systèmes informatiques à des sociétés tierces spécialisées. Elles doivent donc être partie prenante de l'amélioration des mesures de protection contre les cyberattaques que vous jugez nécessaires pour votre Commune. Nous profitons de rappeler que la responsabilité de leur bonne mise en œuvre reste du ressort de la Commune et que celle-ci doit en conséquence obtenir de ses prestataires informatiques les assurances nécessaires que ces risques sont correctement pris en compte.

Nous vous transmettons ci-dessous quelques liens utiles :

- Les informations du Centre national pour la cybersécurité NCSC : https://www.ncsc.admin.ch/ncsc/fr/home/aktuell/im-fokus/ransomware-8.html

- Le lien vers l'application mobile du canton de Vaud en matière de cybersécurité, qui recense en particulier 10 bonnes pratiques essentielles de sécurité : https://vd.ch/cybersecurite
- Les conseils de votre police pour se prémunir des risques de rançongiciel : https://votrepolice.ch/entreprises/rancongiciels/

Nous espérons que ces quelques recommandations pourront vous être utiles et restons bien entendu volontiers à votre disposition.

A cette occasion, nous vous adressons, Mesdames les Syndiques, Messieurs les Syndics, Mesdames les Municipales, Messieurs les Municipaux, chères Mesdames, chers Messieurs, l'expression de nos salutations distinguées.

Jean-Luc Schwaar

Directeur général des affaires institutionnelles et des communes (DGAIC)

Marc Barbezat

Directeur de la sécurité numérique
Direction générale du numérique et des systèmes d'information (DGNSI)

Annexe : Récapitulatif « Conseils en cas de cyberattaque », DGNSI