Associations, cibles des cyberattaques Conseils d'un expert en cybersécurité (Octobre 2021)

En moyenne, dans le monde, toutes les 10 secondes, une structure est victime d'un ransomware (rançongiciels en français), une attaque informatique suivie d'une demande de rançon pour résoudre le problème. Les pirates, profitant de la pandémie ont visé tous types de secteur d'activité. Malheureusement, les associations sont très souvent victimes. Comment se protéger ?

Conseils d'Arnaud Deschavanne, responsable de l'activité évaluation « Cybersécurité » de Magellan Consulting.

Les associations/ONG sont aussi la cible des attaques informatiques. Pourquoi ?

Il y a un grand écart entre les petites associations qui ont peu de moyens et pourtant des données à protéger (fichier adhérents, par exemple) et des grosses associations/ONG qui, sachant qu'elles sont ciblées, ont développé un niveau de protection bon, voire très bon.

Il faut comprendre la logique des pirates. Ils ratissent généralement large. Tout le monde est visé, les entreprises comme les associations. Mais pour éviter d'être pris dans les mailles de leur filet, il faut avoir un système plus sécurisé que les autres. Si les associations sont souvent victimes, c'est parce que leur niveau de sécurisation est moins bon que la moyenne. On pourrait dire la même chose des PME/TPE.

Quelles bonnes pratiques mettre en place ?

Impossible d'assurer une sécurité parfaite. Ceci dit voici quelques conseils de base.
Du côté des infrastructures, si le cœur de métier n'est pas technologique (ce qui est le cas de la grosse majorité des associations), il faut privilégier des solutions de type Cloud. Elles permettent d'externaliser la gestion d'outils collaboratifs (traitement de texte en ligne, espace de partage...). La sécurisation est assurée par le prestataire.

J'attire aussi l'attention sur la sécurisation des terminaux des utilisateurs (ordinateurs ET smartphones). D'autant que, depuis les confinements, l'utilisation d'ordinateur personnel pour télétravailler s'est développée, particulièrement dans les petites structures et ce sont des portes ouvertes aux cyberattaques.

Donc, il faut :
1/ mettre à jour les systèmes d'exploitation, les logiciels, les applications logiciels ;
2/ installer des antivirus ;
3/ mettre en place le principe du moindre privilège : compartimentez bien les droits d'accès et réservez les droits d'administration à des personnes sensibilisées, voire formées à la sécurité ;
4/ protéger les accès sensibles avec de la double authentification (via une application sur smartphone, par exemple).

Il est crucial de former vos publics : salariés, contrats aidés, bénévoles… à la sécurité informatique. Entraînez-les à détecter des e-mails frauduleux, des applications corrompues…
Pour les comptes e-mail et des réseaux sociaux, je le répète, il faut systématiquement activer la double authentification. Car si une personne donne par erreur son mot de passe à un cybercriminel, il ne pourra pas, pour autant, accéder facilement à vos systèmes.

Autre point de vigilance : les sauvegardes.
Le récent incendie d'un data center a montré que les sauvegardes d'un site Internet ne sont pas systématiques. C'est un service qui ne fait pas forcément partie de l'offre de service et pour lequel un complément payant est parfois à prévoir.
Par ailleurs, en cas de compromission par ransomware, les attaquants essayent de plus en plus d'effacer les sauvegardes existantes pour augmenter leur chance d'obtenir le paiement de la rançon. Il est donc nécessaire de mettre en place des sauvegardes distantes et déconnectées pour pouvoir reconstruire et restaurer les services essentiels après une attaque.
Vous avez le choix du support : clé USB, disque dur ou bien NAS.
Couplez cette sauvegarde sur un espace en ligne différent du premier.
Et mettez en place des routines régulières.

>> Pour creuser le sujet, lisez le « Guide d'hygiène informatique » de l'ANSSI qui répertorie 42 mesures.

Que faire si l'on est victime d'un rançongiciel, une pratique en plein boom ?

Il faut avoir lu un autre guide incontournable de l'ANSSI « Attaques par rançongiciels, tous concernés. Comment les anticiper et réagir en cas d'incident » (télécharger le guide, PDF).
Si le mal est fait : débranchez les équipements concernés du réseau, priorisez la protection des sauvegardes et ne payez pas.
Vous n'avez aucune garantie que les pirates respectent leur parole et vous entretenez cette cybercriminalité. Très souvent, le coût de la reconstruction est énorme par rapport au prix de la rançon demandée par les pirates informatiques. Pour des grosses entreprises, il peut se chiffrer en dizaine de millions d'euros. Même assuré (car des contrats d'assurance couvrent partiellement ce risque désormais), ce sera insuffisant.

Avoir un petit problème qui va sensibiliser l'ensemble de l'association ou mener un exercice de simulation serait l'idéal. Mais qui va piloter cette opération ? S'il n'y a pas de personne compétente en sécurité informatique, en interne, on peut demander à un prestataire.
Certaines associations mènent des tests d'intrusion, mais ce type de prestation est coûteuse car elle nécessite des profils experts.
Certains prestataires spécialisés peuvent avoir une politique de mécénat pour effectuer des prestations (pro bono par exemple). Une autre solution peut être également de se rapprocher d'écoles d'ingénieur ayant des masters spécialisés en Cybersécurité et qui sont en quête de cas pratiques.

Mes conseils
- Prendre le temps de lire et de se positionner par rapport au guide d'hygiène de l'ANSSI qui présente les mesures minimums à respecter pour protéger les informations de votre association ou de votre organisation.
- Se faire accompagner si les compétences n'existent pas en interne, déléguer les sujets pour lesquels il n'y a pas de valeur ajoutée en interne par exemple en utilisant des applications SaaS ou des services Clouds qui offriront un niveau de sécurité par défaut et par design.

Propos recueillis par Évelyne Jardin, Juris associations pour le Crédit Mutuel

➢ *Pour en savoir plus :*

- *Créer un site associatif en 6 étapes*
- *Les réseaux sociaux*
- *Déclarer une attaque sur la plateforme du gouvernement*
- *Suivre le cours en ligne gratuit de l'ANSSI*
- *Organiser un exercice de gestion de crise*
- *Guide attaque par rançongiciels - ANSSI*
- *Anticiper les attaques par rançongiciels*