Associations : conseils pour mieux se protéger des cyberattaques
(Décembre 2023)

En 2022, 43 % des organisations auraient subi au moins une cyberattaque au cours des douze derniers mois. L'hameçonnage tient le haut du pavé des actes de cybermalveillance, devant l'exploitation d'une faille[1]. Les associations ne sont pas épargnées. Comment mieux se protéger ? Recueil des conseils de Christophe Gueguen, expert Cybersécurité de Magellan Sécurité.

Pourquoi des associations/ONG sont-elles la cible de cyberattaques?

Il ne faut pas confondre victime et cible. Dans la majorité des cas, les associations sont victimes comme toutes les autres organisations. Généralement, les pirates ratissent large. Tout le monde peut être visé : les entreprises, collectivités territoriales, établissements de santé et… les associations.
La question est : qui sera pris dans les mailles de leur filet ? Réponse : les organisations ayant des systèmes moins sécurisés que ceux des autres et des humains moins informés/formés. Et c'est malheureusement le cas de nombreuses associations. Donc, si elles sont souvent victimes (et non pas cibles), c'est parce que leur niveau de sécurisation technique et humaine est moins bon que la moyenne. On pourrait dresser le même constat chez les PME/TPE qui représentent 40 % des victimes.

Deuxième cas de figure, il y a des associations/ONG qui, de par leur activité de lobbying, de défense de droits divers et variés s'attirent des opposants. Dans ce cas, elles peuvent être véritablement ciblées. Certaines ONG ayant des moyens ont développé des procédures de défense et un niveau de protection supérieur en s'entourant d'experts en cybersécurité.

Quelles bonnes pratiques mettre en place ?

Gardez en tête que la sécurité parfaite n'existe pas. Ceci dit voici quelques conseils élémentaires.

Du côté des infrastructures informatiques, si le cœur de métier n'est pas technologique (ce qui est le cas de la grosse majorité des associations), privilégiez des solutions de type *Cloud*. Elles permettent d'externaliser la gestion d'outils collaboratifs (traitement de texte en ligne, espace de partage…), voire d'héberger des fichiers d'adhérents, d'usagers, de bénévoles hors des ordinateurs de l'association. La sécurisation technique est assurée par le prestataire. Toutefois, veillez à sécuriser l'accès à ces espaces en ligne avec des mots de passe robustes et des processus de double authentification. Veillez aussi à ce que vos prestataires respectent le RGPD (Règlement général de protection des données personnelles) s'ils stockent vos données. Par ailleurs, si des données à caractère personnel ont été piratées, il faut porter plainte et déclarer la violation à la CNIL sous 72h.

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

1 *Source : https://www.blogdumoderateur.com/bilan-cyberattaques-pme-les-plus-exposees/*

>> Pour creuser ce sujet, lisez « Recommandations sur le nomadisme numérique »; Guide de l'ANSSI (Agence nationale de la sécurité des systèmes d'information), mis à jour en novembre 2023.

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 une 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 vérolées... Pensez aux exemples d'attaques avec des QR Codes corrompus qui ont explosé ces derniers temps.

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 du site Internet.
De nombreuses associations ont vu leur site tomber en panne et leur base de données disparaître totalement. Cela faisait suite à l'incendie d'un gros *data center* en mars 2021. Donc, les sauvegardes d'un site Internet ne sont pas systématiques. C'est un service qui ne fait pas forcément partie de la prestation et pour lequel un complément payant est parfois à prévoir. Il faut le vérifier et mettre en place des sauvegardes en parallèle.

>> Ce ne sont que quelques bonnes pratiques basiques. 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 ?

En cas de compromission par *ransomware (ou rançongiciel)*, disposer de sauvegardes de qualité est clé. Si elles sont compromises par l'attaque, redémarrer l'activité sera très compliquée voire impossible. 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 (*Network Attached Storage* ou serveur de stockage en réseau, en français).
Couplez cette sauvegarde avec un espace en ligne différent du premier.
Et mettez en place des routines régulières pour tester que les sauvegardes peuvent être restaurées.

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 ».

Si le mal est fait : déconnectez les équipements concernés du réseau mais n'éteignez pas les machines, 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.

Est-ce pertinent de simuler une attaque ?

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.

Dernier conseil : avant d'être victime, il faut absolument savoir si l'association, une fois attaquée, pourrait poursuivre ses activités en mode dégradé car la gestion de crise peut s'étendre. Il faut éviter le blocage complet.

Mes conseils
- Prendre le temps de lire et de se positionner par rapport au guide d'hygiène informatique de l'ANSSI qui présente les mesures minimums à respecter pour protéger les informations de votre association ou de votre organisation.
- Monter en compétence en suivant le cours en ligne *SecNumacadémie* de l'ANSSI. Il est gratuit et accessible à tous jusqu'au 30 juin 2024.

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

Lexique

- *Ransomware* ou rançongiciel : logiciel malveillant qui bloque l'accès aux utilisateurs et leur réclame le paiement d'une rançon pour rétablir l'accès
- *Phishing* ou hameçonnage : technique de cyberattaque qui vise à obtenir l'accès à des comptes : réseaux sociaux, banques, administrations…

➢ *Pour aller plus loin :*

- *Avis d'expert - Cyberattaques, les associations victimes*
- *Anticiper les attaques par rançongiciels*
- *Déclarer une attaque sur la plateforme du gouvernement*
- *Contacter son CSIRT (Computer Security Incident Response Team) régional*
- *Être accompagné par le programme gratuit Cyber for Good*
- *Le webinaire organisé par Solidatech, 23/11/2023*