Rapport Analytique

Les ONG au service de l'humanité en danger : les cybermenaces qui pèsent sur la "Genève internationale"

Résumé

Introduction

Au cœur de la Genève internationale prospère un vibrant écosystème abritant 38 organisations internationales (OI) et 432 organisations non gouvernementales (ONG), auxquelles s'ajoutent plusieurs centaines d'associations actives au plan international, toutes unies par une mission commune : faire du monde un lieu de paix et de justice. Les ONG sont les héros méconnus de cette mission, intervenant en cas de conflit armé, de catastrophe naturelle et de crise humanitaire, défendant les droits de l'homme et contribuant à la réalisation des objectifs du développement durable (ODD). Comme de nombreuses organisations, les ONG sont utilisatrices de technologies numériques, essentielles à projeter leurs opérations à l'international en temps réel. Cette accélération technologique est une chance, mais crée également de nouveaux défis.

Et de nouvelles menaces.

En effet, alors qu'elles se battent pour notre bien commun, les ONG doivent aussi lutter contre toutes les formes de cyberattaques. Espionnage, rançongiciel, fraude, désinformation, dans le cyberespace, les ONG sont les variables d'ajustement de la pire des équations.

D'un côté, elles sont ciblées par tous les types d'acteurs malveillants - groupes criminels, acteurs étatiques, groupes terroristes ou hacktivistes, motivés tour à tour par l'appât du gain, le vol de données ou la destruction des systèmes - de l'autre, elles n'ont pas les moyens humains ou financiers de se protéger.

À Genève, le CyberPeace Institute participe à la protection de ces héros. Nos services de cybersécurité pour les ONG comprennent une cartographie des menaces, de la main d'œuvre qualifiée, des

notifications d'alerte, une aide à la collaboration avec les services de police et, enfin et surtout, des recommandations stratégiques aux donateurs et aux décideurs publics et privés. Tout cela est gratuit et adapté à la réalité opérationnelle des ONG.

Ce rapport propose des recommandations concrètes à l'intention des ONG, des donateurs et des États. Il donne un aperçu de la maturité des ONG pour ce qui est de prévenir, de détecter et de répondre aux cyberattaques. S'appuyant sur des données jamais exploitées jusqu'à ce jour, y compris le résultat d'entrevues avec des professionnels de terrain, ce rapport a pour ambition d'aider les ONG à renforcer leur résilience de façon pérenne et de devenir les acteurs principaux de leur cybersécurité.

Conclusions

Conclusion 1

Les ONG de la Genève internationale sont la cible de cyberattaques.

- **41 % des ONG** déclarent avoir été victimes d'une cyberattaque dans les trois dernières années.
- **Toutes les ONG** qui ont été victimes d'attaques déclarent qu'il ne s'agissait pas d'incidents isolés. La fréquence de ces incidents varie, certaines ONG y étant confrontées quotidiennement, tandis que d'autres y font face une fois par mois ou par an.
- **70 % des ONG** ne pensent pas être suffisamment résilientes ou ne savent pas si elles sont suffisamment résilientes pour se remettre d'une cyberattaque.

Conclusion 2

Les ONG de la Genève internationale se savent exposées, mais ne bénéficient pas du soutien nécessaire pour mettre en œuvre des stratégies pérennes de cybersécurité.

- Contrairement à des entités reconnues comme infrastructures essentielles, les ONG n'ont pas de désignation sectorielle précise qui leur vaudrait des protections particulières dans le cyberespace.
- Le financement des ONG est généralement fléché par projets et ne

prévoit souvent pas de budget pour la cybersécurité.

- **33 % des ONG** déclarent ne pas disposer de compétences informatiques en interne, et **56 % des ONG** déclarent ne pas affecter de budget à leurs besoins en matière de cybersécurité.
- Les ONG ont conscience de la diversité de la menace, comme la fraude en ligne, l'ingénierie sociale ayant pour but la manipulation, les rançongiciels ou les logiciels espions, mais seulement **4 %** ont une politique concrète de cybersécurité.
- **85 % des ONG** savent combien il est important de sensibiliser leurs employés à la cybersécurité, mais seulement **52 %** leur font suivre régulièrement la formation nécessaire.

Conclusion 3

Les ONG de la Genève internationale ont du mal à concilier leurs modèles de fonctionnement avec l'évolution rapide du contexte numérique et les besoins en matière de cybersécurité.

- Les ONG doivent composer avec l'évolution rapide de la réglementation, des normes et des lois relatives à l'utilisation de la technologie et des obligations en cas de cyberattaques, comme par exemple, les obligations de protection des données en cas d'atteinte à la sécurité des données.
- Les outils de cybersécurité en libre accès ne sont pas adaptés aux modèles de fonctionnement et de gestion particuliers des ONG. Il ne suffit pas aux ONG d'avoir connaissance de ces outils et d'y avoir accès pour assurer durablement leur cybersécurité.
- Il faut aux ONG plus que des outils gratuits et des connaissances générales de sécurité: Il leur faut surtout des moyens humains pour penser une stratégie de cybersécurité et assurer son suivi opérationnel.

Même si les ONG ont encore beaucoup de progrès à faire en ce qui concerne leurs capacités en matière de cybersécurité, le fait de reconnaître les menaces très réelles qui pèsent sur elles et de développer des pratiques de cybersécurité montre qu'il est possible de prendre des mesures concrètes et, donc, d'être plus optimiste pour l'avenir.

Contrer les menaces - Recommandations stratégiques et techniques

Les principales constatations éclairent sur les défis majeurs que doivent relever les organisations non gouvernementales (ONG) de la Genève internationale en matière de cybersécurité, et les recommandations suivantes proposent une feuille de route concrète.

Les recommandations stratégiques et techniques portent sur les catégories suivantes en matière de cybersécurité:

- Processus et structures
- Partenariats et réseaux
- Personnes et compétences
- Technologie
- Documents officiels relatifs aux questions de cybersécurité

Il est également recommandé aux ONG de se joindre au programme des CyberPeace Builders de l'Institut, ou autre programme similaire, afin de bénéficier d'une assistance concrete en matière de cybersécurité.

Le programme des CyberPeace Builders fournit aux ONG des conseils et des renseignements sur les cybermenaces afin qu'elles puissent détecter les cyberattaques à venir; il renforce les capacités des ONG pour empêcher qu'elles ou leurs bénéficiaires soient victimes de cyberattaques; et il collabore avec des experts en cybersécurité et des ONG au moyen d'une plateforme de bénévolat, également pour encourager l'engagement communautaire.

Le CyberPeace Institute remercie les ONG qui ont participé à ce projet pour leurs contributions importantes. L'analyse, les constatations et les conclusions de ce rapport sont le fruit du travail des analystes et experts du CyberPeace Institute. Elles ont été communiquées aux ONG qui ont participé à la recherche, mais il ne leur a pas été demandé de les approuver.

CyberPeace Institute
Campus Biotech Innovation
Park Avenue de Sécheron 15
1202 Geneva, Switzerland

cyberpeaceinstitute.org
@CyberPeace Institute
@CyberpeaceInst