RÉSILIENCE NUMÉRIQUE DES FONDATIONS SUISSES

Aperçu des Menaces et Recommandations

CyberPeace Institute

With the support of:

REPUBLIC AND STATE OF GENEVA

POST TENEBRAS LUX

Résumé

Les fondations suisses jouent un rôle essentiel dans la poursuite de missions philanthropiques, mais elles sont confrontées à des menaces croissantes en matière de cybersécurité face à un monde de plus en plus numérique. Ce rapport du CyberPeace Institute, soutenu par la République et Canton de Genève, évalue la résilience numérique des fondations suisses et révèle un aperçu fragmenté en matière de cybersécurité. Bien que les grandes fondations disposent souvent de ressources dédiées, les plus petites fonctionnent avec une protection limitée, ce qui les rend plus vulnérables à des menaces complexes.

Le rapport identifie six défis majeurs: un manque de sensibilisation et de formation, des budgets limités, un manque d'expertise au niveau du conseil de fondation, une incohérence des pratiques de sécurité, une fragmentation des efforts et un accès restreint aux ressources partagées. Pour y remédier, il recommande de dispenser des formations ciblées au personnel et aux conseils de fondation, d'intégrer la cybersécurité dans la structure organisationnelle au moyen de budgets et de politiques spécifiques, et de mutualiser les ressources par le biais de services partagés et de réseaux d'experts. Il préconise également de favoriser l'innovation par des programmes pilotes et des certifications, d'encourager la collaboration par le partage de bonnes pratiques et les partenariats, et de tirer parti d'un soutien externe, notamment d'initiatives telles que le programme CyberPeace Builders.

Ce rapport est un appel à l'action: la résilience numérique doit devenir une priorité stratégique pour les fondations suisses.

Avant-propos

Stéphane Duguin

Chief Executive Officer, CyberPeace Institute

L'ère numérique a apporté des opportunités et des défis sans précédent pour les organisations du monde entier, y compris les fondations suisses. En tant que CEO du CyberPeace Institute, je suis pleinement conscient de l'importance cruciale de la cybersécurité pour protéger le travail précieux de notre communauté philanthropique. Ce rapport est le résultat de notre étude de 2023 sur les menaces cyber impactant la Genève Internationale, d'un séminaire organisé sur le sujet avec des fondations suisses le 19 mars 2024, et d'une enquête subséquente - il souligne les vulnérabilités numériques et la résilience des fondations suisses.

Les résultats révèlent effectivement un paysage où la sensibilisation et la préparation varient considérablement d'une organisation à l'autre. Alors que certaines fondations ont adopté des mesures de sécurité avancées, nombreuses sont celles qui s'appuient encore sur des protections de base, les rendant vulnérables aux menaces cyber sophistiquées. Les défis identifiés, allant des contraintes de ressources au manque d'expertise et de gouvernance adaptée sur le sujet, mettent en évidence l'urgence d'adopter une approche stratégique et collective de la cybersécurité.

Cette situation est préoccupante non seulement pour les fondations suisses elles-mêmes, mais aussi pour leurs bénéficiaires. De nouvelles données issues de la plateforme CyberPeace Tracer, lancée en 2025, mettent en lumière le paysage des menaces auquel sont confrontés ces bénéficiaires, y compris ceux qui sont basés en Suisse. Ces derniers ont connu de nombreux incidents cyber au cours des dernières années, notamment des attaques par ransomware, des attaques DDoS et des opérations de piratage et de divulgation. Plus de 500 vulnérabilités techniques affectant 73 bénéficiaires que mon équipe surveille soulignent l'urgence croissante de renforcer leur protection, à commencer par les donateurs qui les soutiennent.

Avant-propos (suite et fin)

Stéphane Duguin

Chief Executive Officer, CyberPeace Institute

Le présent rapport fournit des recommandations concrètes pour relever ces défis. En les adoptant, les fondations suisses peuvent renforcer considérablement leur position en matière de cybersécurité. Le CyberPeace Institute s'engage à soutenir ces efforts. J'invite toutes les parties prenantes à se joindre à nous pour construire un environnement numérique plus sûr pour toutes et tous.

Cordialement,

Stéphane Duguin, CEO, CyberPeace Institute

Appel à la Mobilisation

Pour relever ces défis et exploiter les opportunités identifiées dans le rapport, les fondations suisses doivent adopter une approche proactive et collective de la cybersécurité. Les actions suivantes sont essentielles:

1. **Améliorer la sensibilisation et la formation:** Mettre en place des programmes de formation ciblés et des initiatives d'éducation continue pour réduire les lacunes en matière de cybersécurité. Exploiter les événements et les plateformes existants pour maximiser la portée et l'impact.
2. **Mutualisation des ressources:** Mettre en place des plateformes et des mécanismes pour partager les ressources, les outils et les bonnes pratiques en matière de cybersécurité. Encourager la mise en commun des moyens pour l'acquisition de solutions de cybersécurité et créer des réseaux d'experts en cybersécurité pour soutenir les fondations et leurs bénéficiaires.
3. **Intégration de la cybersécurité dans la gouvernance:** Plaider en faveur d'allocations budgétaires dédiées à la cybersécurité et intégrer l'expertise en cybersécurité au niveau du conseil d'administration. Élaborer et mettre régulièrement à jour des politiques globales de cybersécurité. Mettre à jour en conséquence le Swiss Foundation Code.
4. **Favoriser l'innovation et l'adaptation:** Promouvoir les certifications en cybersécurité, piloter des solutions innovantes et mettre en place des programmes de reconnaissance pour encourager les fondations à améliorer leurs mesures de sécurité.
5. **Encourager la collaboration et le partage d'expériences:** Mettre en place des forums et des réseaux pour le partage d'expériences, documenter et diffuser les bonnes pratiques, et favoriser les partenariats avec des organisations actives dans le domaine de la cybersécurité et des établissements universitaires.
6. **Utilisation du soutien externe:** Tirer parti d'initiatives telles que CyberPeace Builders et favoriser les partenariats public-privé afin d'accéder à des ressources, des compétences et des financements supplémentaires pour les initiatives en matière de cybersécurité.

Résilience numérique des fondations suisses: aperçu des menaces et recommandations

Objectif du Rapport

Ce rapport vise à fournir une vue d'ensemble complète de l'état actuel de la cybersécurité parmi les fondations suisses, fondée sur les informations recueillies lors d'un atelier organisé en mars 2024 et d'une enquête menée auprès des participants. Les objectifs principaux de ce projet, soutenu par la République et l'État de Genève, étaient d'identifier les défis majeurs auxquels ces fondations sont confrontées en matière de cybersécurité, d'analyser l'efficacité des pratiques actuelles et de proposer des recommandations concrètes pour renforcer leur niveau de sécurité et celui de leurs bénéficiaires. En abordant ces problématiques, le rapport cherche à créer un environnement plus résilient et sécurisé pour les fondations suisses, leur permettant de continuer leurs missions philanthropiques avec une confiance accrue.

Contexte

Le 19 mars 2024, le CyberPeace Institute a organisé un séminaire au Campus Biotech de Genève afin d'aborder la question urgente de la cybersécurité au sein des fondations suisses. Cet événement a réuni des représentants du secteur public, des membres de la communauté philanthropique ainsi que des experts en cybersécurité. L'objectif principal était de favoriser un dialogue ouvert sur les défis auxquels ces fondations sont confrontées et d'explorer ensemble des pistes de solutions concrètes.

Dans le cadre du séminaire, une enquête a été menée auprès des participants afin de recueillir des informations complémentaires et des retours d'expérience. Dix réponses ont été reçues (cinq en français et cinq en anglais) offrant un regard précis sur les pratiques actuelles, les obstacles identifiés et les besoins exprimés par les fondations suisses en matière de cybersécurité. Ce rapport s'appuie sur les éléments recueillis lors du séminaire ainsi que sur les résultats de l'enquête pour formuler ses constats et recommandations.

Le rapport débute par un résumé des échanges tenus lors de la rencontre, suivi d'une analyse des résultats de l'enquête. La section principale est consacrée aux recommandations et aux prochaines étapes, proposant un cadre d'action concret pour permettre aux fondations suisses de renforcer leurs dispositifs de cybersécurité.

En adoptant une approche collective et stratégique, ces fondations peuvent accroître significativement leur résilience face aux menaces numériques, tout en assurant la pérennité et la sécurité de leurs actions philanthropiques.

1. Résumé du Séminaire

a. Principaux défis identifiés

Au cours du séminaire, un certain nombre de défis critiques ont été soulignés:

- Gestion des risques financiers et de la fraude

La fraude financière est une des préoccupations majeures de nombreuses fondations. Les mécanismes existants de vérification des paiements et des bénéficiaires témoignent d'une certaine prise de conscience des risques, en particulier à la suite d'attaques réussies. Toutefois, ces mesures sont souvent limitées et ne sont pas appliquées de manière systématique à l'échelle de l'écosystème philanthropique. Les témoignages recueillis lors du séminaire ont également mis en évidence la sophistication croissante des attaques, notamment avec le recours à l'intelligence artificielle, rendant indispensable l'adoption de stratégies plus robustes de détection et de prévention des fraudes.

Études de cas

Étude de cas 1: Usurpation vocale du PDG par deepfake audio dans une fondation suisse

Contexte

Une éminente fondation suisse a récemment été victime d'une cyber-attaque sophistiquée impliquant un deepfake audio. Les attaquants ont imité la voix et les expressions du directeur de la fondation afin d'orchestrer un système de fraude à la direction générale visant l'équipe financière.

Aperçu de l'incident

La tentative de fraude s'est déroulée lorsque l'équipe financière de la fondation a reçu un appel téléphonique qui ressemblait à s'y méprendre à celui de son directeur. L'imitation de la voix était si convaincante qu'elle a réussi à tromper deux membres de l'équipe sur trois. L'appelant, qui se faisait passer pour le directeur, a donné des instructions pour autoriser un décaissement important.

La vigilance du troisième membre de l'équipe a permis à la fondation d'éviter une perte financière. Sentant que quelque chose n'allait pas, cette personne a décidé d'utiliser un canal de communication secondaire pour vérifier la demande directement auprès du directeur. Cette étape a permis de confirmer la fraude et de déjouer l'attaque.

Techniques d'attaque

Plusieurs éléments ont mis en évidence le degré de préparation et la complexité de cette attaque:

- **Imitation vocale:** La technologie de deepfake a reproduit de manière convaincante la voix du directeur, y compris certaines expressions et nuances spécifiques.
- **Ciblage du personnel:** Les attaquants ont su identifier avec précision les membres clés de l'équipe financière et les contacter directement, témoignant d'une compréhension approfondie des processus internes de la fondation.
- **Recherche préalable:** Les cybercriminels avaient manifestement mené une enquête approfondie en amont, collectant des coordonnées et se familiarisant avec les procédures de décaissement de la fondation. Ce niveau de préparation laisse penser à l'implication d'acteurs organisés et déterminés, plutôt qu'à celle d'arnaqueurs amateurs.

Implications en matière de cybersécurité

Ce cas met en lumière la menace croissante que représente la technologie des deepfakes dans les fraudes numériques. Avec les avancées rapides de l'intelligence artificielle générative et des deepfakes vidéo, ce type d'attaque risque de devenir de plus en plus courant et difficile à détecter. Les fondations et organisations similaires, qui ne se considèrent pas toujours comme des cibles prioritaires, doivent faire preuve d'une vigilance accrue.

Constats et recommandations

- **Canaux de vérification secondaires:** Toujours recourir à un canal de communication secondaire pour confirmer toute demande sensible, en particulier lorsqu'elle concerne des transactions financières.
- **Sensibilisation et formation:** Organiser régulièrement des sessions de formation pour l'ensemble des collaborateurs afin de leur permettre d'identifier les menaces liées aux deepfakes et de comprendre l'importance des procédures de vérification.
- **Surveillance et contrôles internes:** Mettre en place des systèmes de surveillance efficaces et des contrôles internes robustes, tels que des autorisations basées sur les rôles ou des systèmes de double validation, afin de détecter et prévenir les transactions non autorisées.
- **Maîtrise de l'exposition en ligne:** Limiter la diffusion en ligne de contenus audiovisuels des cadres dirigeants pour réduire le risque de création de deepfakes.
- **Collaboration avec des experts:** S'associer à des experts en cybersécurité pour rester informé des menaces émergentes et mettre en œuvre des dispositifs de protection avancés.

Conclusion

La tentative de fraude au président visant cette fondation suisse constitue un rappel essentiel de l'évolution constante des menaces cyber. Les deepfakes, développés à partir de l'intelligence artificielle générative, posent de nouveaux défis en matière de cybersécurité. En restant informées et proactives, les organisations peuvent renforcer leur capacité de défense face à ces attaques complexes et garantir la sécurité de leurs activités.

Études de Cas

Étude de Cas 2: Escroqueries par usurpation ciblant une fondation suisse

Contexte

Une fondation importante a récemment été la cible de cybercriminels ayant recours à une arnaque par usurpation d'identité particulièrement élaborée. Ce cas illustre la menace croissante que représentent les escroqueries par e-mail et via les réseaux sociaux, qui cherchent à exploiter la réputation et la confiance dont bénéficient les organisations philanthropiques.

Aperçu de l'incident

L'arnaque a débuté par la création de faux profils sur les réseaux sociaux et de fausses adresses e-mail usurpant l'identité d'un philanthrope bien connu, associé à la fondation. Ces profils frauduleux ont interagi avec des victimes potentielles sur des plateformes comme Instagram, établissant progressivement un lien de confiance à travers des échanges en apparence authentiques.

L'une des personnes ciblées a été approchée par un individu se faisant passer pour le philanthrope. Après quelques échanges cordiaux initiaux, l'escroc poursuit les échanges par courrier électronique, en utilisant une adresse imitant de très près le nom du philanthrope. Il a alors promis un don important de 800 000 dollars, à condition que les fonds soient utilisés pour des projets entrepreneuriaux et des actions caritatives. Pour enclencher le processus de versement, il a demandé des informations personnelles telles que le nom complet, l'adresse du domicile et le numéro de téléphone. Ces données peuvent ensuite être exploitées à des fins d'usurpation d'identité, ou utilisées dans les étapes suivantes de l'escroquerie, qui consistent à inciter la victime à effectuer un transfert d'argent au profit de l'escroc, ce dernier prétendant que ce versement est nécessaire pour libérer la prétendue donation.

L'approche de l'escroc incluait des détails précis sur le fonctionnement de la fondation et ses modalités de versement, ce qui témoigne d'un haut niveau de préparation et de compréhension.

Heureusement, la personne ciblée a pris contact avec la fondation par d'autres canaux, ce qui a permis d'éviter toute perte financière. La fondation avait recommandé aux bénéficiaires potentiels de vérifier toute offre directement via ses canaux officiels, une consigne que la cible a suivie, permettant ainsi de révéler l'escroquerie.

Techniques d'attaque

Tactiques utilisées par les usurpateurs:

- **Usurpation d'identité:** utilisation du nom et de l'image d'un philanthrope reconnu pour gagner la confiance des victimes potentielles.
- **Engagement via les réseaux sociaux:** prise de contact et création d'un lien de confiance à travers de faux profils sur les réseaux sociaux.
- **Fraude par courrier électronique:** poursuite des échanges par e-mail à l'aide d'adresses très similaires à celles de personnes légitimes.
- **Prétexte détaillé:** présentation d'informations précises et crédibles sur les dons et les conditions de paiement afin de renforcer la crédibilité de la demande.
- **Collecte d'informations personnelles:** demande de données sensibles (nom, adresse, téléphone) sous couvert de traiter la prétendue donation.

Implications en matière de cybersécurité

Ce cas illustre la fréquence croissante et la complexité grandissante des arnaques par usurpation d'identité visant les fondations. À mesure que les fraudeurs affinent leurs méthodes en construisant des scénarios convaincants et des communications réalistes, il devient essentiel pour les fondations de mettre en place des mesures robustes afin de protéger leurs activités et les bénéficiaires de leur soutien.

Constats et recommandations

- **Protocoles de vérification:** Mettre en place et appliquer des protocoles stricts de vérification pour toute transaction financière ou toute offre reçue. Encourager les bénéficiaires à confirmer la légitimité des propositions via les canaux officiels de la fondation.
- **Sensibilisation et formation:** Organiser régulièrement des sessions de formation à l'intention du personnel et des bénéficiaires afin de leur permettre d'identifier et de réagir face aux arnaques par usurpation d'identité.
- **Surveillance proactive:** Assurer une veille active sur les réseaux sociaux et sur la présence en ligne de la fondation afin de détecter les faux profils et les activités frauduleuses impliquant des personnes associées à l'organisation.
- **Communication claire:** Assurer la transparence sur les procédures de subvention et les escroqueries connues via le site internet de la fondation. Y intégrer une section dédiée à l'information du public sur les menaces potentielles.
- **Mécanismes de signalement:** Mettre en place et promouvoir des dispositifs simples et accessibles pour signaler les tentatives d'escroquerie. Collaborer avec les plateformes de réseaux sociaux et les autorités compétentes pour faire retirer rapidement les comptes frauduleux.

Conclusion

L'arnaque par usurpation d'identité visant cette fondation constitue un rappel essentiel de l'évolution constante des menaces cyber. En adoptant des mesures de cybersécurité proactives et globales, les fondations peuvent protéger leurs activités et prémunir leur communauté contre des escroqueries de plus en plus élaborées. Les enseignements tirés de cet incident soulignent l'importance de la vigilance, de la sensibilisation et de protocoles de vérification rigoureux pour préserver l'intégrité et la confiance qui entourent les organisations philanthropiques.

Sensibilisation et formation

Un problème majeur identifié concerne le manque de sensibilisation et de connaissances en cybersécurité parmi le personnel des fondations, en particulier dans les structures de petite taille et au sein des conseils d'administration. De nombreuses fondations notamment celles dont la transformation numérique reste limitée pensent à tort être à l'abri des cyberattaques. Bien que certaines initiatives de formation existent, elles restent souvent limitées dans leur portée et leur impact. Cela souligne l'importance de mettre en place des programmes de sensibilisation continus, ciblés et adaptés à l'ensemble des niveaux de l'organisation.

Contraintes budgétaires et organisationnelles

L'un des problèmes centraux abordés concerne l'absence d'allocations budgétaires spécifiques à la cybersécurité. Faute de conscience suffisante des menaces, les fondations investissent peu dans leur propre cybersécurité. Par conséquent, leurs bénéficiaires ne formulent que rarement des demandes de soutien en cybersécurité, contribuant ainsi à entretenir un cycle de sous-investissement.

Nos recherches précédentes sur les menaces pesant sur la Genève Internationale ont mis en évidence un défi similaire du côté des bénéficiaires des fondations. Le manque de sensibilisation des membres des conseils d'administration empêche la cybersécurité d'être considérée comme une priorité lors de la planification budgétaire. En conséquence, les Organisations Non Gouvernementales (ONG) ne recherchent pas activement de ressources en cybersécurité, et les fondations ne leur en proposent pas.

Disparités et manque de cohésion

Le séminaire a mis en évidence d'importantes différences au sein de l'écosystème des fondations suisses. Les grandes organisations disposent généralement de plus de ressources et de mesures de cybersécurité, tandis que les structures petites et moyennes restent plus vulnérables. Ce déséquilibre est accentué par un manque de partage de ressources et de connaissances. Une approche cohérente de la cybersécurité, reposant sur le partage des ressources et la mise en commun des efforts, est essentielle pour réduire ces écarts.

2. Analyse de l'enquête

a. Méthodologie

L'enquête menée auprès des participants au séminaire du 19 mars 2024 visait à recueillir des informations complémentaires sur les pratiques, les défis et les besoins des fondations suisses en matière de cybersécurité. Le séminaire a réuni environ 40 fondations, issues à la fois de la Suisse romande et d'autres régions du pays. Afin de garantir la confidentialité, les noms des fondations ne seront pas divulgués. Environ 25% des participants ont répondu à l'enquête, avec cinq réponses en français et cinq en anglais. Le présent rapport, ainsi que les recommandations qui en découlent, s'appuient sur ces contributions. Les questions posées visaient à recueillir des données sur le niveau de sensibilisation des participants aux enjeux de cybersécurité, leurs pratiques actuelles, les difficultés spécifiques rencontrées, ainsi que leur retour sur l'utilité du séminaire. Les résultats complets de l'enquête figurent dans la section suivante du rapport.

b. Résultats

Les résultats de l'enquête ont fourni des informations précieuses sur l'état de la cybersécurité au sein des fondations, mettant en évidence à la fois les points forts et les axes d'amélioration.

Degré de sensibilisation

L'enquête a révélé des niveaux de sensibilisation et de connaissances en cybersécurité variables parmi les répondants. Si certains participants ont témoigné d'une bonne maîtrise des principes et des pratiques en cybersécurité, d'autres ont révélé des lacunes importantes, bien qu'ils aient exprimé un vif intérêt pour le sujet. Cette hétérogénéité souligne la nécessité de mettre en place des programmes de sensibilisation ciblés afin de combler les écarts, en particulier auprès des petites fondations et des membres de conseils d'administration dont la compréhension des exigences en cybersécurité reste limitée.

Données principales:

- Sensibilisation élevée: 40 % des répondants estiment avoir un niveau élevé de sensibilisation à la cybersécurité.
- Sensibilisation modérée: 30 % des répondants évaluent leur niveau de sensibilisation comme modéré.
- Faible sensibilisation: 30 % des répondants considèrent avoir un faible niveau de sensibilisation à la cybersécurité.

Principales pratiques identifiées

- Audits de sécurité réguliers: 50 % des répondants réalisent des audits de sécurité de manière régulière.
- Systèmes de détection avancée des menaces: 30 % des répondants utilisent des systèmes de détection avancée.
- Mesures de sécurité de base: 70 % des répondants s'appuient sur des mesures de base telles qu'un antivirus ou la protection par mot de passe.

Enjeux et besoins prioritaires

Les répondants ont identifié plusieurs obstacles qui limitent leur capacité à gérer efficacement la cybersécurité:

- Contraintes de ressources: ressources financières et humaines limitées allouées à la cybersécurité.
- Manque d'expertise: difficulté à accéder à des professionnels qualifiés dans ce domaine.
- Déficit de sensibilisation: sensibilisation et formation insuffisantes du personnel et des membres des conseils d'administration.
- Efforts dispersés: manque de coordination et de partage des connaissances entre fondations.

En matière de soutien et de ressources, les participants ont exprimé un besoin de formations plus accessibles, de ressources partagées et d'un accompagnement par des experts pour les aider à faire face à la complexité des enjeux liés à la cybersécurité.

Principaux besoins identifiés:

- Programmes de formation: 80% des répondants ont exprimé le besoin de disposer de davantage de programmes de formation.
- Accompagnement par des experts: 70% des répondants ont souligné l'importance de bénéficier de conseils et de soutien d'experts.
- Ressources partagées: 60% des répondants ont mis en avant la nécessité d'avoir accès à des ressources partagées en matière de cybersécurité.

c. Conclusion

Les résultats de l'enquête confirment les constats formulés lors du séminaire, en mettant en évidence des défis importants liés à la sensibilisation à la cybersécurité, à l'allocation des ressources et à l'accès à l'expertise au sein des fondations suisses. Il ressort clairement un besoin de programmes de formation ciblés, d'un meilleur partage des ressources, ainsi que d'un accompagnement par des experts pour renforcer les capacités en cybersécurité des fondations. Les retours positifs concernant le séminaire soulignent l'utilité de ce type d'événement pour favoriser la collaboration et le partage de connaissances entre fondations. À l'avenir, répondre à ces besoins identifiés sera essentiel pour améliorer la résilience globale du secteur face aux menaces cyber.

3. Recommandations

À partir des éléments relevés lors du séminaire et des résultats de l'enquête, les recommandations suivantes sont proposées afin de renforcer la cybersécurité au sein des fondations suisses. Ces recommandations visent à répondre aux principaux défis identifiés, tout en s'appuyant sur les forces existantes au sein de la communauté philanthropique.

a. Renforcer la sensibilisation et la formation

Des lacunes notables en matière de sensibilisation et de connaissances en cybersécurité ont été relevées parmi le personnel et les membres des conseils d'administration des fondations, en particulier dans les structures de petite taille. Pour y remédier, les stratégies suivantes sont recommandées:

- **Programmes de formation ciblés:** Élaborer et mettre en œuvre des programmes de formation complets, adaptés aux besoins spécifiques du personnel et des membres des conseils d'administration des fondations. Ces programmes devraient couvrir les principes fondamentaux de la cybersécurité, la gestion des risques, ainsi que les bonnes pratiques pour la protection des actifs numériques.

- **Utilisation des plateformes existantes:** S'appuyer sur des événements et plateformes déjà en place, pour proposer des sessions de sensibilisation à la cybersécurité et des ateliers de formation. Cette approche permet de toucher un public plus large et d'intégrer la cybersécurité dans les discussions plus générales sur la gestion des fondations.

- **Formation continue:** Instaurer une culture de l'apprentissage continu en proposant des mises à jour régulières et des formations de mise à jour sur les menaces émergentes en cybersécurité et les solutions disponibles. Des cours en ligne, des webinaires et des ateliers interactifs peuvent être utilisés pour maintenir le personnel et les membres des conseils d'administration informés et préparés.

b. Partage des ressources

Les contraintes de ressources, en particulier au sein des petites fondations, constituent un obstacle majeur à la mise en place de mesures de cybersécurité solides. Pour y remédier, les actions suivantes sont recommandées:

- **Plateforme de services partagés:** Créer une plateforme dédiée au partage de ressources, d'outils et de bonnes pratiques en matière de cybersécurité entre fondations. Elle pourrait inclure un accès à des informations sur les menaces, des modèles de politiques de sécurité, ainsi que des guides de réponse aux incidents.

- **Achats mutualisés:** Encourager l'achat collectif de solutions et de services de cybersécurité. En regroupant leurs besoins, les fondations peuvent bénéficier d'économies d'échelle, réduire les coûts et accéder à des services de meilleure qualité.

- **Réseaux d'experts**: Développer des réseaux d'experts en cybersécurité pouvant fournir des services de conseil pro bono ou à tarif préférentiel aux fondations. Des initiatives telles que CyberPeace Builders pourraient être étendues afin d'offrir un soutien plus structuré et accessible à un plus grand nombre de fondations.

c. Intégrer la cybersécurité dans la structure organisationnelle

Pour garantir une attention durable et des ressources suffisantes en matière de cybersécurité, il est essentiel d'intégrer cette dimension dans les mécanismes décisionnels des fondations, tels que le Swiss Foundation Code. Les recommandations suivantes peuvent contribuer à cet objectif:

- **Financement dédié:** Promouvoir l'inclusion de budgets spécifiquement alloués à la cybersécurité dans les plans financiers des fondations et dans les subventions octroyées. Cela peut être encouragé par des campagnes de sensibilisation ciblant les instances dirigeantes, en soulignant l'importance de la cybersécurité comme priorité stratégique.

- **Expertise au sein du conseil:** Intégrer une expertise en cybersécurité au niveau du conseil d'administration, soit en nommant des membres disposant de compétences spécifiques, soit en proposant une formation en cybersécurité aux membres en place. Cette intégration permet d'ancrer la cybersécurité dans les processus décisionnels et les pratiques de pilotage de la fondation.

- **Élaboration de politiques:** Concevoir et mettre en œuvre des politiques et procédures de cybersécurité complètes, alignées sur les bonnes pratiques et les exigences réglementaires. Ces politiques doivent faire l'objet de révisions régulières afin de rester adaptées à l'évolution des menaces et des vulnérabilités.

Le Swiss Foundation Code est disponible ici.

d. Promouvoir l'innovation et la capacité d'adaptation

Encourager l'innovation et la capacité d'adaptation en matière de pratiques de cybersécurité peut aider les fondations à anticiper les menaces émergentes. Les stratégies suivantes sont recommandées:

- **Certifications en cybersécurité:** Développer et promouvoir des certifications ou labels en cybersécurité pour les fondations respectant des normes de sécurité spécifiques. Ces certifications peuvent servir de référence en matière de bonnes pratiques et inciter les fondations à renforcer leurs dispositifs de cybersécurité.

- **Programmes pilotes**: Lancer des programmes pilotes pour tester et évaluer des solutions innovantes en cybersécurité, telles que des systèmes avancés de détection des menaces, l'utilisation de la blockchain pour des transactions sécurisées, ou encore l'intelligence artificielle pour l'analyse des risques. Les initiatives concluantes pourront être élargies et partagées avec l'ensemble de la communauté des fondations.

- **Reconnaissance et incitations:** Mettre en place des programmes de reconnaissance et des mécanismes d'incitation pour les fondations adoptant des pratiques exemplaires en matière de cybersécurité. Des distinctions, des reconnaissances publiques ou des subventions dédiées à des initiatives en cybersécurité peuvent encourager les fondations à accorder une priorité accrue à la sécurité et à améliorer leurs dispositifs.

e. Encourager la collaboration et le partage d'expérience

La collaboration et le partage d'expériences entre fondations peuvent contribuer de manière significative à renforcer la résilience collective face aux menaces cyber. Les actions suivantes sont recommandées:

- **Forums et réseaux:** Créer des forums et des réseaux dédiés permettant aux fondations de partager leurs expériences, leurs défis et leurs solutions en matière de cybersécurité. Des réunions régulières, des conférences et des groupes de discussion en ligne peuvent faciliter les échanges de connaissances et encourager une approche collaborative de la cybersécurité.

- **Études de cas et bonnes pratiques:** Documenter et diffuser des études de cas ainsi que des exemples de bonnes pratiques issus de fondations ayant mis en place avec succès des mesures de cybersécurité. Ces ressources peuvent servir de guides pratiques et constituer une source d'inspiration pour d'autres fondations souhaitant renforcer leur posture de sécurité.

- **Partenariats:** Encourager les partenariats entre fondations, organisations spécialisées en cybersécurité et institutions académiques. Ces collaborations peuvent offrir un accès à des recherches de pointe, à des conseils d'experts et à des ressources supplémentaires pour soutenir les initiatives en cybersécurité.

Des études de cas provenant d'organisations de la société civile internationales sont disponibles ici.

f. Mobiliser les soutiens externes

Le soutien externe peut jouer un rôle déterminant dans le renforcement des mesures de cybersécurité au sein des fondations. Les recommandations suivantes peuvent aider les fondations à tirer pleinement parti des ressources disponibles:

- **Les CyberPeace Builders**: Étendre le programme CyberPeace Builders afin d'offrir un accompagnement plus complet à un plus grand nombre de fondations. Ce soutien peut inclure des formations de sensibilisation, une assistance en cas d'incident, ainsi qu'un accompagnement continu en matière de cybersécurité.

Vous trouverez plus d'informations sur le programme CyberPeace Builders - basé à Genève - ici.

- **Partenariats public-privé:** Encourager les partenariats entre les secteurs public et privé afin d'accéder à des ressources, des expertises et des financements supplémentaires pour soutenir les initiatives en cybersécurité. Les agences gouvernementales, les entreprises du secteur privé et les organisations philanthropiques peuvent collaborer pour répondre aux besoins des fondations en matière de sécurité numérique.

- **Programmes de subvention:** Mettre en place des programmes de subvention spécifiquement dédiés au renforcement de la cybersécurité au sein des fondations. Ces financements peuvent couvrir des formations, des mises à niveau technologiques et d'autres actions visant à améliorer la résilience face aux menaces cyber.

g. Conclusion

La mise en œuvre de ces recommandations nécessite un engagement collectif de l'ensemble des acteurs de la communauté philanthropique. En renforçant la sensibilisation et la formation, en mutualisant les ressources, en intégrant la cybersécurité dans les structures organisationnelles, en favorisant l'innovation, en encourageant la collaboration et en mobilisant les soutiens externes, les fondations suisses peuvent améliorer significativement leur posture en matière de cybersécurité. Ces mesures permettront non seulement de protéger les fondations elles-mêmes, mais aussi de garantir la sécurité et la pérennité de leurs missions philanthropiques. Face à l'évolution constante des menaces numériques, une approche proactive et collective de la cybersécurité est indispensable pour préserver l'impact et la valeur du travail mené par les fondations suisses.

4. Conclusions

L'urgence de traiter la question de la cybersécurité au sein de l'écosystème des fondations suisses est plus que jamais d'actualité. À mesure que les menaces numériques évoluent, il est essentiel que les fondations reconnaissent que la cybersécurité ne relève pas uniquement d'un enjeu technique, mais constitue un pilier fondamental de la bonne gouvernance et de la résilience organisationnelle. En agissant de manière collective et stratégique, les fondations peuvent protéger leurs activités, sécuriser leurs actifs numériques et garantir la pérennité de leurs missions philanthropiques.

Les recommandations et prochaines étapes présentées dans ce rapport offrent une feuille de route permettant aux fondations suisses de renforcer efficacement leur posture en matière de cybersécurité. En collaborant et en s'engageant dans une démarche d'amélioration continue, les fondations suisses peuvent construire un avenir plus sûr et plus résilient pour les communautés qu'elles soutiennent.

Les points clés mis en évidence dans ce rapport sont les suivants:

1. Déficit de sensibilisation et de formation: Un manque notable de sensibilisation et de formation en cybersécurité a été observé, en particulier au sein des petites fondations et parmi les membres plus agés des conseils d'administration. Cette lacune représente un risque important dans un contexte où les menaces numériques deviennent de plus en plus sophistiquées.

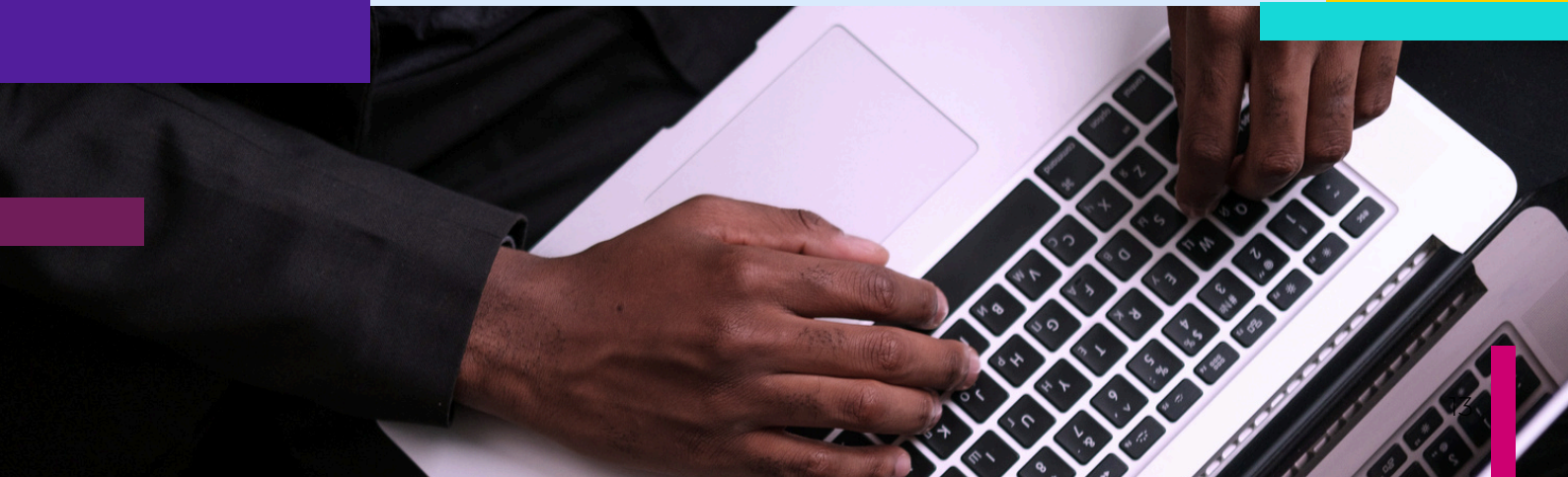
2. Contraintes de ressources: De nombreuses fondations, en particulier les plus petites, sont confrontées à des contraintes financières et humaines qui limitent leur capacité à mettre en place des mesures de cybersécurité robustes. Cela inclut un manque d'allocation budgétaire suffisante ainsi qu'un accès limité à des professionnels qualifiés en cybersécurité.

3. Lacunes en matière de gouvernance et de politiques: La cybersécurité n'est souvent pas intégrée aux cadres de gouvernance des fondations, tels que le Swiss Foundation Code, ce qui entraîne un manque d'attention stratégique et une allocation insuffisante des ressources. Ce problème est aggravé par l'absence d'expertise en cybersécurité au sein des conseils d'administration.

4. Inégalités dans les pratiques de cybersécurité: Des écarts significatifs existent entre les pratiques de cybersécurité des grandes fondations et celles des plus petites. Alors que les grandes structures disposent souvent de dispositifs de sécurité complets, les plus petites se contentent de protections de base, ce qui les rend plus vulnérables aux attaques.

5. Nécessité de collaboration et de mutualisation: Le manque d'actions coordonnées et les efforts fragmentés entre les fondations mettent en évidence l'importance de renforcer la collaboration et la mutualisation des ressources afin d'améliorer la résilience collective en matière de cybersécurité.

6. Retours positifs sur le séminaire: Les retours des participants au séminaire ont été largement positifs, soulignant la valeur de ce type d'événement pour favoriser les échanges de connaissances et la collaboration. Une demande claire s'est exprimée en faveur de sessions plus interactives et concrètes lors des prochains rendez-vous.



À Propos de Nous

Offre du CyberPeace Institute

L'Institut a développé un large éventail d'outils et de services pouvant aider les fondations suisses à surmonter les défis identifiés dans ce rapport. Ces ressources visent à renforcer leurs missions en répondant aux enjeux essentiels en matière de cybersécurité.

1. Évaluation: Les fondations, ainsi que les organisations qu'elles soutiennent, peuvent réaliser une Évaluation Générale de la Cybersécurité (GCSA) afin d'identifier leurs vulnérabilités et de recevoir des recommandations alignées sur des cadres de référence tels que le NIST et Cyber Essentials. Cette évaluation porte sur les domaines clés suivants en matière de cybersécurité:

- Gestion des actifs et des utilisateurs
- Sécurité des terminaux et des réseaux
- Accès à distance et services Cloud
- Sauvegardes
- Sécurité du périmètre numérique exposé au public
- Authentification multifacteur (MFA) et gestion des mots de passe
- Sensibilisation à la cybersécurité
- Surveillance du dark web et des journaux d'activité
- Gouvernance (politiques internes)

Vous trouverez plus d'informations sur notre évaluation GCSA ici.

2. Alertes et rapports personnalisés: Les fondations, ainsi que les organisations qu'elles soutiennent, peuvent accéder à des renseignements détaillés sur les menaces qui les concernent, issus de données commerciales agrégées. Elles reçoivent également des alertes en cas de menaces immédiates, accompagnées de plans d'action spécifiques. Ces plans privilégient des solutions efficaces en termes de ressources et proposent une feuille de route pour une amélioration continue.

Vous trouverez plus d'informations sur nos services de veille sur les menaces ici.

3. Soutien par des bénévoles: Pour remédier aux vulnérabilités identifiées par nos analystes internes et combler les lacunes révélées par l'évaluation GCSA, les fondations et leurs bénéficiaires peuvent bénéficier de l'expertise des bénévoles du réseau CyberPeace Builders. Ce réseau compte plus de 1300 professionnels de la cybersécurité issus d'entreprises partenaires, mobilisables pour des missions ciblées telles que la sensibilisation à la cybersécurité, les simulations de phishing, les évaluations de vulnérabilités, l'élaboration de politiques de sécurité, et bien plus encore. Il est également possible pour les ONG de demander un accompagnement personnalisé selon leurs besoins spécifiques. À ce jour, nos bénévoles ont déjà fourni plus de 2 500 heures de soutien dans le cadre de plus de 1 000 missions, au bénéfice de plus de 500 fondations et bénéficiaires à travers le monde.

Vous trouverez plus d'informations sur notre programme CyberPeace Builders ici.

4. Formation: Nous proposons des formations, des analyses assistées par l'IA et des exercices de simulation pour aider les fondations et les ONG à renforcer leur cybersécurité. Nos programmes permettent de développer les compétences, d'améliorer la détection des menaces et de renforcer les capacités de réponse, afin que les fondations et leurs bénéficiaires puissent protéger leur mission ainsi que les communautés qu'ils soutiennent.

Vous trouverez plus d'informations sur la CyberPeace Academy ici.

5. Outils: Accès à des outils et guides de cybersécurité gratuits, négociés avec nos partenaires, incluant des solutions de protection contre le phishing, de détection des menaces, d'analyse des vulnérabilités, et bien plus encore. En tant que membre fondateur de Nonprofit Cyber, nous disposons d'une connaissance approfondie des outils mis gratuitement à disposition par d'autres acteurs, que nous pouvons recommander en toute confiance.

Vous trouverez plus d'informations sur ces outils ici.

6. Renforcement de la communauté: Les fondations et leurs bénéficiaires feront partie d'une communauté croissante dédiée à la cybersécurité dans le secteur non lucratif, favorisant l'apprentissage entre pairs, le partage de bonnes pratiques, la défense d'intérêts communs et la diffusion d'alertes communautaires.

Vous trouverez plus d'informations sur notre communauté dédiée à la cybersécurité et nos campagnes de sensibilisation et d'engagement ici.