Fiche-conseils

D'UNE CYBERATTAQUE À LA SAISIE DES DONNÉES

Les incidents et attaques liés à la sécurité informatique, appelés cyberattaques, sont de plus en plus fréquents. Leurs natures ainsi que leurs conséquences peuvent être très diversifiées. Du simple message non-sollicité (spam) au piratage virulent et complexe (virus, cheval de Troie, etc.), les conséquences peuvent se révéler sévères et coûteuses, avec parmi les plus importantes pour une institution, l'indisponibilité de tout un système et la perte de données sensibles.

Procédures et instruction judiciaire

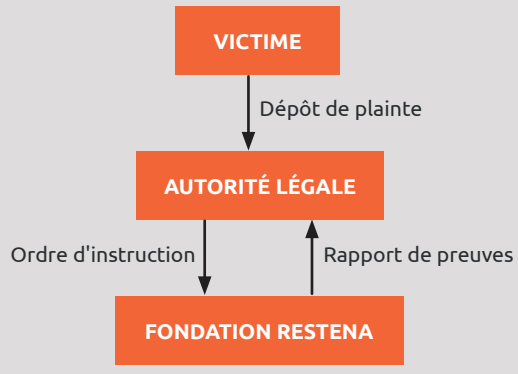
Dépôt de plainte auprès d'une autorité légale

Toute personne ou institution victime d'une cyberattaque est invitée à rapporter l'attaque auprès d'une autorité légale et à déposer plainte dans les meilleurs délais. Cette rapidité d'action permet tant la sauvegarde des traces que la recherche de preuves.

Conformément à la loi luxembourgeoise, une autorité légale comme la police de proximité, la police judiciaire ou le parquet luxembourgeois, peut, dans le cadre d'une enquête, saisir des données et autres preuves auprès des opérateurs et fournisseurs de services électroniques.

Dès le dépôt d'une plainte par la victime, une instruction pour la perquisition des données est ouverte. Celle-ci est remise à l'opérateur ou au fournisseur de services électroniques concerné.

Procédure pour une saisie de données



Support à l'enquête

En tant que fournisseur d'accès au réseau de la recherche et de l'éducation, la Fondation Restena peut être sollicitée par une autorité légale. Dans ce cas, la Fondation Restena supporte techniquement l'enquête et se charge de la recherche de preuves.

Les données requises par une enquête incluent des données relatives au trafic, telles que les données de transition composées des adresses IP, ports, date et heure, durée de la communication, protocoles utilisés, etc. Les données relatives au trafic peuvent en général être retracées jusqu'au compte de l'utilisateur de l'entité concernée.

La loi luxembourgeoise de juillet 2010* prévoit que les fournisseurs de services électroniques et les opérateurs conservent les données relatives au trafic pour une durée d'au moins six mois à compter de la date à laquelle la communication a eu lieu. Il est donc vivement conseillé aux victimes de déposer plainte au plus vite pour éviter l'effacement des données, donc des preuves, si la période de six mois est dépassée.

Les autorités légales au Luxembourg

- Police Grand-ducale du Luxembourg
- Parquet du Luxembourg (Parquet du Tribunal d'Arrondissement du Luxembourg et Parquet du Tribunal d'Arrondissement de Diekirch)
- Service de la Police Judiciaire, Section Nouvelles Technologies, Luxembourg

** Loi du 24 juillet 2010 portant modification des articles 5 et 9 de la loi modifiée du 30 mai 2005 concernant la protection de la vie privée dans le secteur des communications électroniques et de l'article 67-1 du Code d'instruction criminelle.*

restena
réseau · sécurité · .lu

Contribuer efficacement à une enquête

Aucune institution n'est à l'abri d'une cyberattaque, alors autant se préparer à cette éventualité afin de pouvoir contribuer au bon déroulement d'une enquête. Pour cela, nous vous conseillons de suivre quelques recommandations simples.

Gardez à jour vos coordonnées institutionnelles et/ou celles de votre contact de sécurité.

Des coordonnées à jour facilitent la prise de contact lors d'une cyberattaque sur votre réseau. Si vous avez besoin d'aide pour mettre à jour les détails de vos coordonnées signalétiques, contactez la Fondation Restena.

Mettez en place un système de journalisation.

En archivant des données relatives au trafic du réseau informatique, un système de journalisation facilite la réponse technique aux requêtes lors d'une enquête. La loi luxembourgeoise exige d'ailleurs, pour certaines institutions, selon leur activité, de disposer d'un tel système.

Mettez en place une procédure décrivant les démarches à suivre lors d'une enquête.

Grâce à des procédures définissant clairement les responsabilités et rôles de chacun, vous ne freinez pas l'enquête en cours.

Portez immédiatement plainte, si vous êtes victime d'une cyberattaque.

Si vous disposez d'un système de journalisation des données relatives au trafic sur votre réseau, conservez toutes les évidences possibles sur toute la durée de l'attaque et joignez-les à votre plainte.

Confidentialité des données

De manière générale et en se référant au règlement relatif à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données (loi GDPR en cours **), la Fondation Restena ne communique en aucun cas les données relatives au trafic sur sa communauté à une partie tierce. Ces données sensibles sauvegardées ne sont utilisées ni à des fins commerciales ni à des fins de surveillance.

Exception : Dans le cadre d'une enquête officielle menée par une autorité légale, seules les données relatives à l'incident sont communiquées.

→ Votre institution est victime d'une cyberattaque ?
N'attendez-plus, réagissez immédiatement !

Offre de services

Grâce à son équipe de réponse aux incidents de sécurité informatique (Restena-CSIRT), la Fondation Restena aide la communauté luxembourgeoise de la recherche et de l'éducation confrontée à des incidents de sécurité informatique.

Pour plus d'informations sur ce service, rendez-vous sur www.restena.lu/csirt

*** Règlement 2016/679 du 27 avril 2016 relatif à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données, et abrogeant la directive 95/46/CE (règlement général sur la protection des données).*

restena
réseau · sécurité · .lu