CNPD
COMMISSION NATIONALE POUR LA PROTECTION DES DONNÉES

Protection des données

GARANTIR LA RÉSILIENCE CONTRE LES ATTAQUES INFORMATIQUES

Dans un paysage numérique en constante évolution, la protection des données est un enjeu vital pour garantir la sécurité des individus, des entreprises et des institutions contre les attaques informatiques. Les cybercriminels exploitent sans relâche les vulnérabilités des systèmes pour accéder aux données personnelles, ce qui peut entraîner des conséquences majeures allant de la perte financière à la violation de la vie privée.

La cybersécurité est une composante essentielle de la protection des données, car elle a notamment pour objectif de prévenir, détecter et répondre aux menaces potentielles qui pourraient compromettre l'intégrité, la confidentialité et la disponibilité des données.

Récemment, le Grand-Duché a été victime d'une attaque DDOS de grande ampleur. L'attaque, qui a pour objectif de saturer de requêtes différents sites internet, a abouti et se faisant, rendu plusieurs sites gouvernementaux inutilisables entrainant une indisponibilité des données.

Les données personnelles sont une cible de choix pour les cybercriminels, car elles peuvent être exploitées ou revendues à des fins de fraude, d'usurpation d'identité ou de chantage. En protégeant ces informations, conformément à l'article 32 du Règlement Général sur la Protection des Données (RGPD) , les organisations peuvent préserver la confidentialité des données, la confiance de leurs clients et limiter l'impact de la cyberattaque.

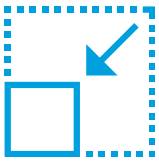
Quelques bonnes pratiques en protection des données pour renforcer la cybersécurité :

Privacy by Design et Privacy by Default :

Le RGPD encourage l'intégration de la protection des données dès la conception des systèmes et des services. Par ce biais, les responsables de traitements sont invités à déployer des mesures de cybersécurité qui garantissent l'intégrité, la confidentialité et la disponibilité des données. Une attention plus particulière doit être accordée aux données sensibles des personnes concernées. En planifiant la manière dont les données seront protégées avant même le commencement du traitement, les responsables de traitement réduisent drastiquement le risque de violation de données.

Analyse d'impact relative à la protection des données :

Lorsqu'un traitement de données présente un risque élevé pour les droits et libertés des personnes concernées, une analyse d'impact sur la protection des données (AIPD) doit être réalisée. En absence présumée de risque élevé il est malgré tout recommandé de mener une analyse au moins sommaire mais systématique afin d'avoir une vue d'ensemble du traitement. Cela inclut l'évaluation des risques liés à la cybersécurité et la mise en place de mesures pour atténuer ces risques et parfois un plan d'atténuation en cas de réalisation du risque.



Réduction de la surface d'attaque :

En limitant la collecte de données au strict nécessaire (principe de minimisation), les entreprises réduisent la quantité de données pouvant être exposée lors d'une attaque. De la même manière, s'assurer de respecter une durée de conservation des données préétablie, de supprimer, archiver, ou anonymiser les données en temps voulu permet de réduire l'efficacité des différentes attaques.

Anonymisation, pseudonymisation et principe du « besoin d'en connaitre » (need to know) :

S'assurer que les données personnelles ne sont pas utilisées ou accessibles par des employés ou agents qui n'en ont aucune nécessité ou utilité permet de limiter fortement l'impact d'une cyberattaque. Le responsable de traitement doit donc strictement limiter les accès aux données personnelles aux services qui sont responsables des finalités prédéterminées liées à ces données. L'anonymisation et la pseudonymisation permettent d'offrir une résistance supplémentaire au regard de la confidentialité contre une attaque visant les données personnelles.

Limitation de l'usurpation d'identité :

L'usurpation d'identité se produit lorsque que l'attaquant s'empare de données personnelles et peut reconstituer l'identité numérique d'un individu. Ce faisant il lui est possible de contracter au nom d'une autre personne. Une telle situation peut engendrer une longue période de difficultés sérieuses pour les victimes.

Accompagnement des personnes concernées :

Lors d'une violation de données personnelles présentant un risque important pour les personnes concernées le responsable de traitement est tenu d'accompagner la personne concernée et de lui indiquer la manière de minimiser au mieux les risques entrainés par la violation. Le respect de cette obligation pour le responsable de traitement permet de garantir la confiance des personnes concernées et de limiter grandement les résultats de la cyberattaque pour les attaquants. Cet accompagnement peut se caractériser de différentes façons comme en se tenant à disposition des personnes concernées, leur proposer un suivi individualisé ou encore une assistance juridique.

Préservation de la bonne réputation :

Un respect du RGPD et une communication publique sincère et pragmatique permet de renforcer la confiance en l'organisation des utilisateurs, clients, patients, partenaires et consommateurs et autres personnes concernées, qu'il s'agisse d'une communication quant à une violation de données personnelles ou du respect des exigences de transparence de la réglementation. Afin de consolider sa réputation et de s'assurer la confiance des personnes concernées, les organisations peuvent recourir à la certification de leur processus de traitement de données.

Dans ce contexte la CNPD tient à préciser qu'en cas de violation de données personnelles présentant un risque pour les personnes concernées, il est impératif pour les responsables de traitement de signaler cette violation à la CNPD dès que celle-ci présente un risque pour les personnes concernées et ce, indépendamment de la gravité dudit risque.

La Commission nationale rappelle qu'une violation de données à caractère personnel se caractérise par un défaut dans la sécurité de celles-ci et résulte en une perte de confidentialité, d'intégrité ou de disponibilité des données que ce soit de manière illicite ou accidentelle.

En cas de déclaration de violation, la CNPD, met son expertise technique et légale à disposition du responsable de traitement afin de le guider au mieux. (Plus d'information sur le site de la CNPD dans la partie violations de données.)

L'Union européenne, depuis 2022, s'est saisie plus en profondeur des questions relatives à la cybersécurité. Les Etats membres, dont le Grand-Duché du Luxembourg, œuvrent en ce moment même à l'implémentation technique et légale de la directive NIS 2 qui vise à assurer la sécurité de systèmes garantissant le fonctionnement des principales infrastructures du pays. Ces systèmes sont désignés comme « critiques » par la directive et doivent faire l'objet d'une cybersécurité renforcée. Dans ce contexte, la conformité à la règlementation sur la protection des données nécessite une attention d'autant plus importante.

CNPD
COMMISSION NATIONALE POUR LA PROTECTION DES DONNÉES

Commission nationale pour la protection des données
15, Boulevard du Jazz I L-4370 Belvaux
Tél. : (+352) 26 10 60 - 1
www.cnpd.lu

Mai 2024