LE RGPD COMME OUTIL DE LA CYBERSÉCURITÉ

Nathalie Ragheno

Premier conseiller FEB

Board member dpo pro

Board member Cyber Security Coalition

Membre du Centre de connaissances APD

PLAN DE L'EXPOSÉ

1. Quelques chiffres sur la cybercriminalité
2. RGPD & cybersécurité
3. Obligations légales de cybersécurité dans le RGPD
4. Notification d'incidents
5. Responsabilités de la cybersécurité
6. Sanctions
7. Outils en matière de cybersécurité et sites utiles

CHAQUE JOUR DE NOUVELLES ENTREPRISES VICTIMES…

Politie gehackt: PV's en gevoelige foto's gelekt

Pechverhelper Touring slachtoffer van cyberaanval

rtbf.be VIDÉO AUDIO MON CHOIX CHAÎNES

…TU INFO SPORT ACTUALITÉS LOCALES CULTURE ET MUSIQUE ENVIRONNEMENT ET NATU

Plusieurs milliers de clients de banques belges victimes de hackers

LIÈGE

Le site du CHC a été piraté

Libre ECO

…t-up Décideurs & chroniqueurs Placements & marchés Mes finances Immobilier

Economie › Digital

Le nombre de cyberattaques en Belgique a été multiplié par trois depuis l'arrivée de la crise sanitaire

Les banques belges sont pourtant moins vulnérables que celles d'autres pays et obtiennent un score bien supérieur à la moyenne mondiale ou à la moyenne européenne.

Gerecht start onderzoek naar massale cyberaanval bij stadsdiensten en politie in Antwerpen

ANTWERPEN **Onbekenden hebben in de nacht van 5 op 6 december de computers van de stad Antwerpen gehackt. Afspraken maken bij de dienst bevolking, in het containerpark of bij de politie is voorlopig onmogelijk. Ook reserveren in de stedelijke musea gaat niet meer. Het Antwerpse parket is een opsporingsonderzoek gestart naar de nooit eerder geziene cyberaanval.**

Lien Verlinden 06-12-22, 09:37 **Laatste update:** 14:15

ACCUEIL • ÉCONOMIE • ENTREPRISES

Fuite de données chez Degroof Petercam, plusieurs centaines d'entreprises concernées

Un employé de la banque privée et d'affaires a abusé de ses droits d'autorisation et téléchargé illégalement des fichiers clients. Des collaborateurs de plusieurs centaines d'entreprises sont concernés.

7sur7 ACTU SHOW SPORT LIFESTYLE VIDEO

Belgique Monde Faits divers Insolite Ecologie Tech Santé Economie Sciences

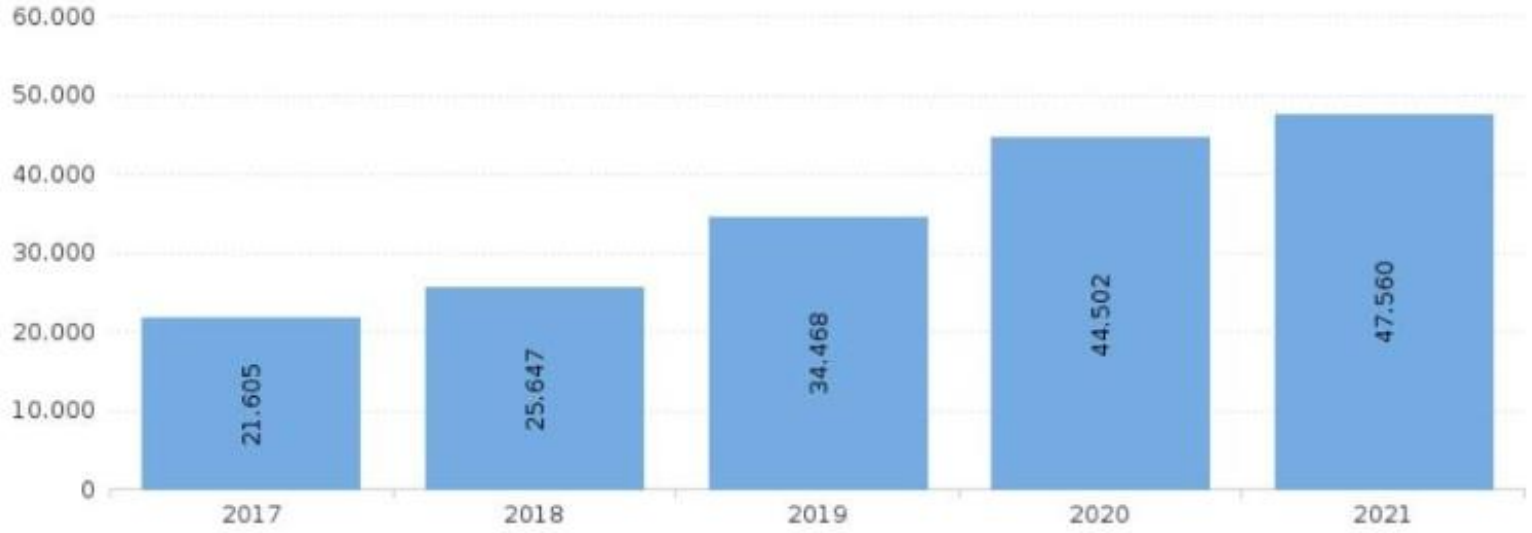
un logiciel malveillant

Un logiciel malveillant, appelé Xenomorph, s'attaque aux smartphones des utilisateurs européens, et plus précisément à leur application bancaire. En Belgique, neuf banques au moins seraient concernées.

MOUSCRON

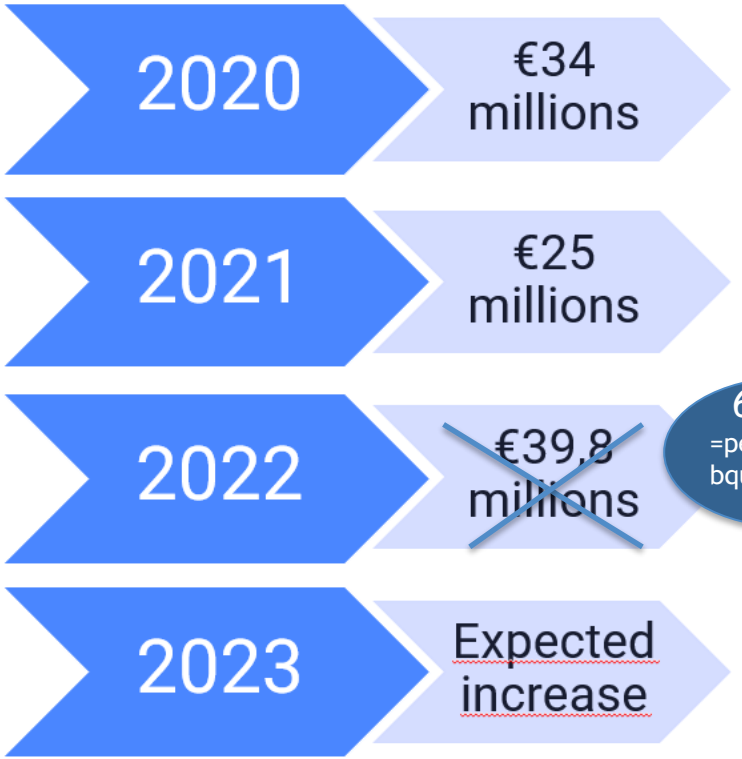
Tout le CPAS bloqué par une cyberattaque

1. QUELQUES CHIFFRES



Nombre de faits enregistrés en matière de criminalité informatique, par année
Source : Police fédérale

Online fraud in Belgium



60 MIO
=pertes des bques et clients

FSMA Figures about fake investments

FEBELFIN Figures about phishing

1. QUELQUES CHIFFRES

2022

- 1 entreprise sur 3 confrontée à un ou plusieurs incidents de cybersécurité
- 1/2 de ces incidents →conséquences financières
- 1/3 a empêché les collaborateurs d'effectuer leur travail.

Dans 90% des cyberattaques, le coupable est l'e-mail

Environ 30 000 sites sont piratés chaque jour dans le monde

5.500 milliards d'euros : c'est le coût annuel dans le monde de la cybercriminalité

Les principales cibles sont les institutions gouvernementales (fédérales et régionales), le secteur hospitalier, les institutions financières mais également les PME

4 entreprises sur 10 manquent de sensibilisation à la cybersécurité

L'APD a ouvert 1426 dossiers de fuite de données en 2022 .
Ce qui est stable par rapport à 2021.

Experienced a cyber attack (%)

	2021	2022	+/-
Belgium	42	**43**	+1
France	49	**52**	+3
Germany	46	**46**	–
Ireland	39	**49**	+10
The Netherlands	41	**57**	+16
Spain	53	**51**	-2
United Kingdom	36	**42**	+6
United States	40	**47**	+7

Median cost of all cyber attack ($000)

	2021	2022	+/-
Belgium	12	**10**	+2
France	18	**17**	-1
Germany	24	**21**	-3
Ireland	8	**17**	+9
The Netherlands	12	**18**	+6
Spain	12	**12**	–
United Kingdom	14	**28**	+14
United States	10	**19**	+9

Experienced a ransomware attack (%)

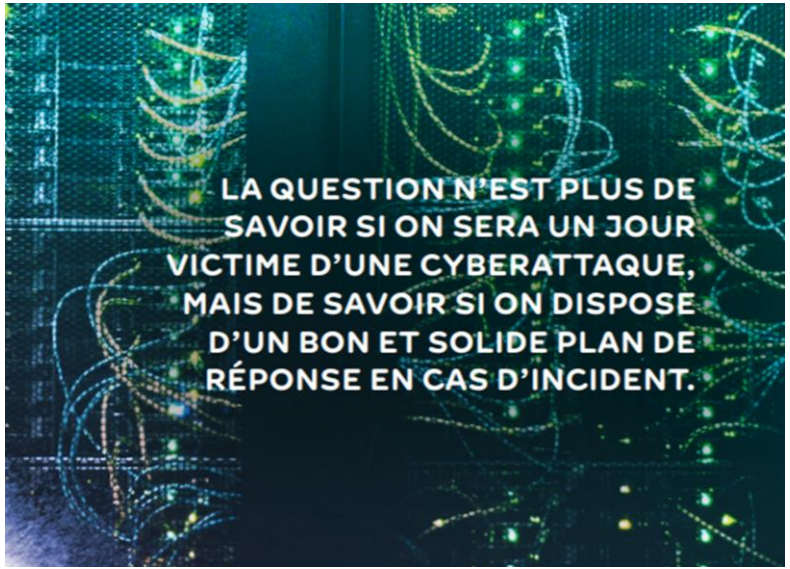
	2021	2022	+/-
Belgium	19	**15**	-4
France	14	**19**	+5
Germany	19	**21**	+2
Ireland	16	**19**	+3
The Netherlands	13	**26**	+13
Spain	14	**22**	+8
United Kingdom	13	**16**	+3
United States	17	**17**	–

Victims of ransomware that paid (%)

	2021	2022	+/-
Belgium	49	**74**	+25
France	65	**62**	-3
Germany	54	**48**	-6
Ireland	75	**80**	+5
The Netherlands	48	**79**	+31
Spain	44	**64**	+20
United Kingdom	58	**63**	+5
United States	71	**84**	+13

Importance de la prévention des cyber incidents

… et surtout disposer d’un plan d’organisation en cas d’incident!



2. RGPD & CYBERSÉCURITÉ

RGPD ≠ texte sur la sécurité des réseaux et systèmes d'information (NIS)

Cependant → sécurité est condition *sine qua non* de la protection des données

→ obligations RGPD et NIS **compatibles et complémentaires**

Objectifs communs : protéger accès, disponibilité, modification, suppression non autorisée de données (y compris à caractère personnel)

Obligations de sécurité = obligation de moyen → prouver que tout a été mis en oeuvre pour appliquer les mesures de sécurité adaptées aux risques

Approche globale = fondée sur une évaluation préalable des risques

2. RGPD & CYBERSÉCURITÉ

RGPD contient des dispositions relatives à la **sécurité des traitements**

RGPD met en place le **principe d'intégrité et de confidentialité** des données à caratère personnel (+ licéité, loyauté, transparence, finalité, minimisation, exactitude, conservation)

→ Les données doivent être traitées de façon à garantir une sécurité appropriée "***y compris*** *la protection contre le traitement non autorisé ou illicite et contre la perte, la destruction ou les dégâts d'origine accidentelle, à l'aide de mesures techniques ou organisationnelles appropriées*" (RGPD, art. 5,§1er, f))

- Intégrité des données : données authentiques et non modifiées par mégarde ou malveillance (WP 29) + s'étend à l'intégrité des systèmes informatiques
- Confidentialité : prévenir l'accès non autorisé aux données et à l'équipement utilisé pour le traitement des données (considérant 39 RGPD)

2. RGPD & CYBERSÉCURITÉ

Art 32, §1er RGPD énumère de manière non exhaustive les moyens mis en place pour garantir la confidentialité, l'intégrité, **la disponibilité et la résilience des systèmes et services de traitement** et les moyens permettant de rétablir la disponibilité des données.

→ **Continuité des traitements**

→ **Disponibilité des données**

Considérant 49 : "… *garantir la sécurité du réseau et des informations càd la capacité d'un réseau ou d'un système d'information de résister à des événements accidentels ou à des actions illegales ou malveillantes qui compromettent la disponibilité, l'authenticité, l'intégrité et la confidentialité de données…*"

2. RGPD & CYBERSÉCURITÉ

Champ d'application différent

RGPD peut avoir un champ d'application plus large

Exemple : tout détournement de finalité résultant d'un traitement "non autorisé" n'est pas une infraction de criminalité informatique

2. RGPD & CYBERSÉCURITÉ

CENTRE FOR CYBER SECURITY BELGIUM

Autorité de protection des données

- Notifications d'incidents dans RGPD et NIS
- Obligations de notification différentes pour RGPD et NIS
- Autorités de contrôle distinctes

3. OBLIGATIONS LÉGALES DE CYBERSÉCURITÉ DANS LE RGPD

a) Obligations du responsable de traitement et du sous-traitant
b) Analyse du risque
c) Analyse de impact si risque élevé
d) Types de mesures à prendre
e) Caractère approprié des mesures de sécurité

3. OBLIGATIONS LÉGALES DE CYBERSÉCURITÉ DANS LE RGPD

a) Responsables de traitement et sous-traitants doivent mettre en oeuvre des mesures de sécurité appropriées pour garantir un *niveau de sécurité adapté aux risques, dont le degré de probabilité et de gravité varie, pour les droits et libertés des personnes physiques*. (art. 32, §1er)

Examen → de la nature des données
→ des circonstances qui entourent le traitement
→ des risques pour les personnes concernées

= Obligation de moyen

3. OBLIGATIONS LÉGALES DE CYBERSÉCURITÉ DANS LE RGPD

b) Analyse du risque selon le RGPD

- évaluer la **probabilité d'un risque potentiel** qui n'est pas encore intervenu = complexe
- **gravité du risque** : considérant 75 donne des exemples de conséquences négatives pour les droits et libertés des personnes (réputation, usurpation d'identité, perte de confidentialité, …) = préjudice moral et même dommages physiques et matériels

Recommandation APD (01/2018) : évaluation des risques inhérents et risques résiduels

Art 32 RGPD impose d'évaluer les risques inhérents au traitement pour mettre en oeuvre les mesures adéquates pour les atténuer (considérant 83)
→ impliquer DPO, concepteurs des applications, personnel ,…

→ contrôle périodique

3. OBLIGATIONS LÉGALES DE CYBERSÉCURITÉ DANS LE RGPD

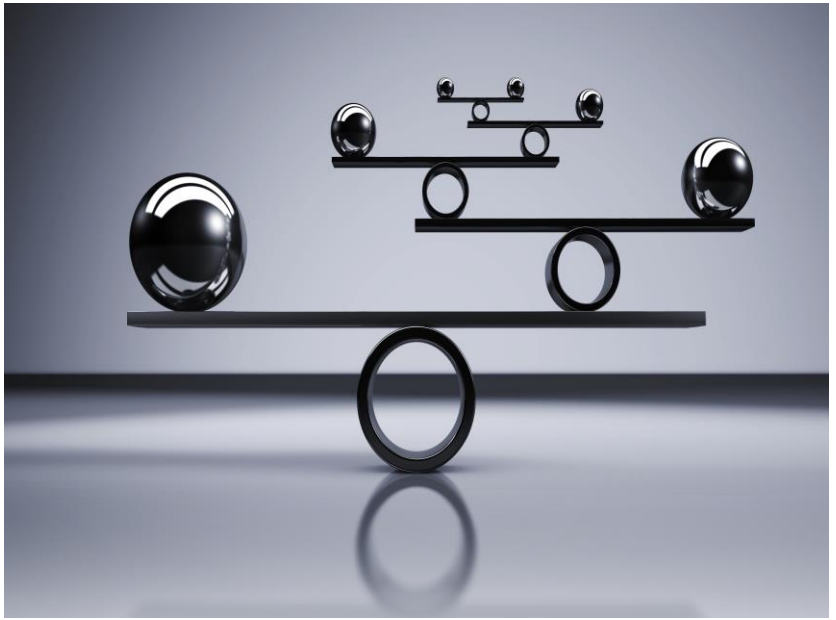
c) Analyse d'impact *avant le traitement* si risque élevé

Notion de risqué élevé : pas définie en détail dans RGPD (= notion liée à d'autres gestions de risques)

Traitements de données qui sont ou pourront être *susceptibles* (= probable) d'avoir des *incidences négatives sensibles* pour les droits et libertés des personnes physiques .

Exemples :

- ✓ Utilisation de données biométriques pour identification
- ✓ Décision automatisée avec refus d'un service
- ✓ Collecte à grande échelle de données



3. OBLIGATIONS LÉGALES DE CYBERSÉCURITÉ DANS LE RGPD

d) 2 types de mesures en matière de sécurité prévues par le RGPD :

- **mesures techniques**: limitations techniques à la collecte et/ou à la communication des données, anonymisation, pseudonymisation, cryptage des données personnelles, sauvegardes supplémentaires, …

- **mesures organisationnelles** : conscientisation, formation, contrôles périodiques, séparation des fonctions, …

+ **mesures juridiques (APD)** : garanties contractuelles, BCR,…

3. OBLIGATIONS LÉGALES DE CYBERSÉCURITÉ DANS LE RGPD

e) Caractère approprié des mesures de sécurité (art. 24, §2 RGPD)

I. *Politique de sécurité de l'information*

→ document écrit reprenant la démarche d'évaluation des risques, priorités, mécanismes mis en place, politique gestion des incidents, sensibilisation de l'entreprise, …

→ politique approuvée par le plus haut niveau de la hiérarchie

II. *État des connaissances* (art 32,§1er RGPD)

doc. ENISA → assistance pour interpréter l'état des connaissances au sens du RGPD

→ s'informer des diverses techniques de sécurité sur le marché (techniques de pointe ?) et les évaluer en fonction des risques décelés.

3. OBLIGATIONS LÉGALES DE CYBERSÉCURITÉ DANS LE RGPD

Caractère approprié des mesures de sécurité (art. 24, §2 RGPD)

III. Coût de la mise en oeuvre

Frais suffisants et raisonnables.
Les ressources financières du responsable de traitement ne sont pas un critère pris en compte

IV. Codes de conduite, certifications, labels,..

Peu développés mais à comparer avec les certifications des entreprises essentielles dans NIS 2

4. NOTIFICATION D'INCIDENTS

Dans le cadre du RGPD, en cas de violation des données , notification obligatoire (article 33, § 1er) lorsque violation susceptible d'engendrer un risque pour les droits et libertés des personnes physiques

Qui notifie?

- Responsable de traitement
- Sous-traitant doit notifier au responsable de traitement dans les meilleurs délais après prise de connaissance

4. NOTIFICATION D'INCIDENTS

A qui notifier ?

- APD compétente
- Si risqué élevé : notification aux personnes concernées elles-mêmes dans les meilleurs délais

Si l'entreprise relève du champ d'application de NIS 1 (OSE ou FSN) et bientôt de NIS 2 (18 secteurs – entreprises essentielles et importantes)
→ notification obligatoire au CCB (https://nis-incident.be)

→ notification *sans retard (le + rapidement possible)*

→ **ou notification volontaire** (https://cert.be/fr/signaler-un-incident)

Si entreprise est OSE supervisée par BNB
→ notification directe à la BNB

4. NOTIFICATION D'INCIDENTS

Délai de notification ?

- 72 heures au plus tard après prise de connaissance
- Point de départ du délai de notification: degré raisonnable de certitude qu'un incident a eu lieu et que des données personnelles sont compromises
- Importance de disposer d'un plan de gestion des incidents adéquat

4. NOTIFICATION D'INCIDENTS

Que notifier?

- Description de la nature de la violation des données
- Coordonnées DPO
- Description des conséquences
- Description des mesures prises
- Notification de l'indisponibilité des données ?
- Pas de notification si
  - Mesures techniques ou organisationnelles rendant lecture des données impossible (cryptage par exemple)
  - exige des efforts disproportionnés

Comment notifier ?

Autorité de protection des données

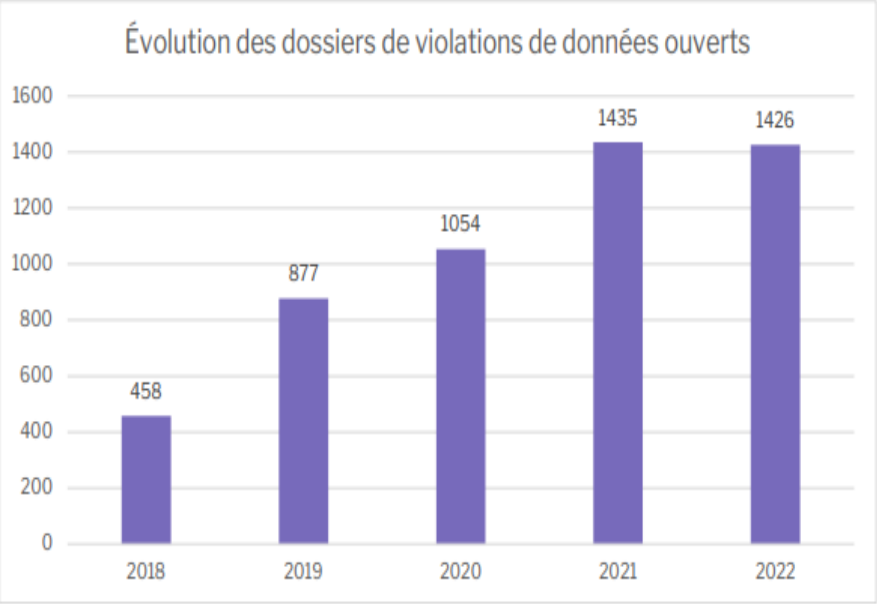
https://www.autoriteprotectiondonnees.be/professionnel/actions/fuites-de-donnees-personnelles

4. NOTIFICATION D'INCIDENTS (EN CHIFFRES)

En 2022, l'APD a reçu

- 1.420 notifications concernant des violations de données et

- elle a elle-même initié 6 dossiers suite à une suspicion de violation de données avec un impact social important pour laquelle aucune notification n'a été introduite



https://www.autoriteprotectiondonnees.be/publications/rapport-annuel-2022.pdf

4. NOTIFICATION D'INCIDENTS

Causes les plus fréquentes de violations de données	Nombre
Erreur humaine	47 %
Hacking, phishing & malware	25 %
Usage impropre des droits d'accès	9 %

5. RESPONSABILITÉS DE LA CYBERSÉCURITÉ

RESPONSABILITÉS AU SENS DU RGPD

RESPONSABILITÉS DE DROIT COMMUN

RESPONSABILITÉS NIS (1 ET 2)

5. RESPONSABILITÉS DE LA CYBERSÉCURITÉ

Responsabilités au sens du RGPD (art. 24 et svt RGPD)

→ Entreprises publiques & privées

→ agissant comme responsable de traitement ou sous-traitant

Principe d'accountability : resp. de traitement doit pouvoir démontrer que le principe de sécurité est respecté en ce compris l'efficacité des mesures + analyse d'impact

Avec aide sous-traitants (contrat de sous-traitance doit mentioner cette collaboration compte tenu de la nature du traitement et des informations à la disposition du ST)

Le contrat de sous-traitance peut prévoir des obligations additionnelles de résultat en matière de sécurité informationnelle (ex : contrôle des accès, techniques cryptographiques spécifiques, …)

→ ST ne pourra se dégager de sa responsabilité qu'en prouvant la force majeure, faute du RT ou d'1/3

5. RESPONSABILITÉS DE LA CYBERSÉCURITÉ

Responsabilité de droit commun

- Indisponibilité des services
- Contrats non exécutés
- Dommages causés à des personnes physiques

Responsabilités de la cybersécurité (NIS)

Alourdissement des responsabiltés des dirigeants

Sanctions : RGPD – loi 2018 – NIS 2 - …

5. RESPONSABILITÉS DE LA CYBERSÉCURITÉ

Un plan de gouvernance d'entreprise propre à la cybersécurité doit être mis en place au sein des entreprises (tout comme cela existe pour le RGPD)

Il est également important pour les dirigeants de savoir auprès de qui ils peuvent déléguer les obligations qui pèsent sur eux dans ce cadre

Les administrateurs doivent comprendre et aborder la protection des données et la cybersécurité comme une question de stratégie à l'échelle de l'entreprise et ne pas considérer qu'il s'agit d'une simple question informatique de la responsabilité du service IT et du DPO/CISO

6. SANCTIONS & JURISPRUDENCE

En Belgique

Remarque luminaire:

Les amendes administratives, tant en application de la loi vie privée de 2018 que de la future loi de transposition de NIS 2 ne s'appliquent pas au secteur public.

Décisions de la Chambre contentieuse en 2022:

Nature des dossiers traités ayant donné lieu aux décisions :

- 174 dossiers de plaintes (nationaux)
- 1 dossier de violation de données
- 12 dossiers d'inspection d'initiative
- 3 dossiers d'initiative
- 5 plaintes internationales pour lesquelles l'APD est compétente

6. SANCTIONS & JURISPRUDENCE

En Belgique

Quelques exemples récents:

- Décision 110/2023 du 9 août 2023 : Plainte à l'encontre d'une école secondaire municipale en raison de la publication de rapports disciplinaires et d'une enquête sur les élèves.
- Décision 78/2023 du 19 juin 2023: Plainte relative à la divulgation de données personnelles d'un employé par son employeur à des tiers – fin de la relation de travail
- Décision 33/2022 : du 10 mars 2022 : absence de réaction de la part du responsable du traitement à une demande d'accès et à l'insuffisance de mesures de sécurité, suite à un hacking informatique
- CdP 21 août 2019 : Fuite de 2000 empreintes digitales : l'Autorité de protection des données suit l'affaire Adecco

6. SANCTIONS & JURISPRUDENCE

En Europe : quelques exemples

- **Pays-Bas : Autoriteit Persoonsgegevens (AP)**
  - 04.10.2023 : 300 EUR à l'encontre d'une école supérieure en dédommagement d'un étudiant dont les données ont été hackées
  - 13 avril 2023 : 150.000 EUR à l'encontre de SVK pour manque de controle d'identité dans un helpdesk téléphonique (données sensibles)
  - 7 juillet 2021 : 450.000 EUR à l'encontre de UWV pour absence de mesures de sécurité suffisantes dans l'envoi de données de santé de 15.000 personnes
- **France – CNIL** : 21 avril 2022 : sanction de 1,5 million EUR à l'encontre de la société DEDALUS BIOLOGIE pour une fuite de données de santé
- **Pologne :** 12 juillet 2023: La DPA polonaise a infligé une amende de 2 640 EUR à un responsable du traitement pour ne pas avoir notifié une violation aux personnes concernées et pour ne pas avoir informé l'autorité de protection des données dans le délai de 72 heures, en violation des articles 33 et 34 du règlement GDPR.

6. SANCTIONS & JURISPRUDENCE

En Europe : quelques exemples

- **The Danish DPA :** 28 sept. 2023 **:** La DPA a réprimandé un sous-traitant, une plateforme tout-en-un pour l'industrie immobilière, pour avoir enfreint l'article 32, paragraphe 1, du GDPR. Le sous-traitant avait mis en place une sécurité insuffisante sur sa plateforme puisque les utilisateurs pouvaient voir des données confidentielles dans le code source simplement en accédant aux outils de développement du navigateur.
- **Norvège -** Datatilsynet : 4 mars 2019 : 170 000 EUR à l'encontre de la commune de Bergen pour insuffisance de mesures de sécurité pour des données sensibles (comptes d'élèves d'écoles primaires)
- **Grèce :** 24 juillet 2023 : La DPA a ordonné à un conseil municipal en Grèce de cesser ses activités de traitement, en vertu de l'article 58, paragraphe 2, du GDPR en raison d'une violation de données non résolue, qui a permis à des utilisateurs non autorisés d'accéder aux données personnelles des citoyens par le biais de la manipulation d'URL.
- **Roumanie:**
  - 23 nov. 2023 : Rompetrol Downstream SRL, un opérateur de gaz a été condamné à une amende de 110 000 EUR pour une violation de données affectant les données personnelles des clients, où les données ont été consultées de manière non autorisée et utilisées pour obtenir frauduleusement des prêts
  - 28 juin 2019 : 130 000 EUR à l'encontre d'une banque pour absence de mise en oeuvre de mesures techniques et organisationnelles

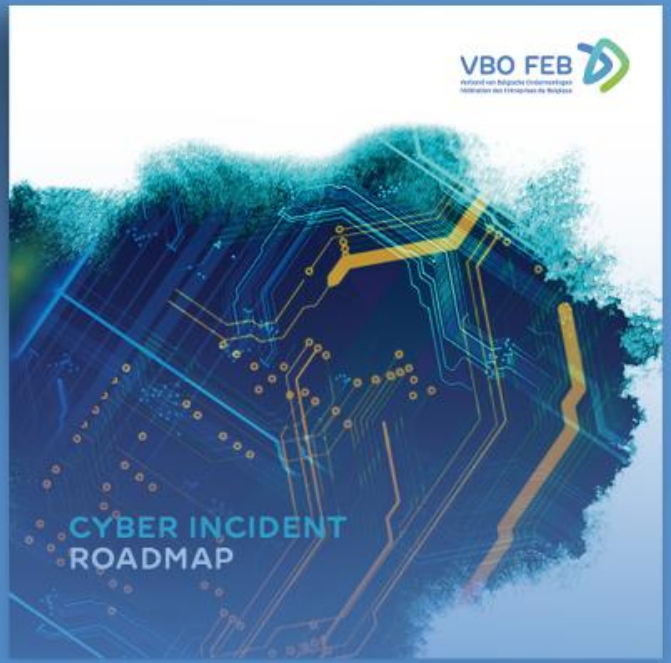
7. OUTILS

https://www.autoriteprotectiondonnees.be/professionnel/actions/fuites-de-donnees-personnelles

CENTRE FOR
CYBER SECURITY
BELGIUM

CYBER SECURITY
COALITION.be

CYBER SECURITY
INCIDENT MANAGEMENT GUIDE



CYBER INCIDENT ROADMAP

CYBER INCIDENT ROADMAP

Témoignages d'entreprises victimes de cyberattaques

- Point de départ du projet

Objectifs

- Sensibiliser les administrations publiques
- Définir un **point de contact précis** auprès de chaque administration pour les victimes

Résultats

- Roadmap
- Collaboration des administrations publiques à la mise en place de points de contact et de procedures spécifiques pour les victimes

Next steps

- Mise à jour régulière de cette roadmap en **collaboration avec les administrations** concernées

febelfin

www.febelfin.be/fr/themes/fraude-et-securite

CERT.be
The Federal Cyber Emergency Team

www.cert.be/fr/signaler-un-incident

CENTRE FOR CYBER SECURITY BELGIUM

www.ccb.belgium.be/fr

CYBER SECURITY COALITION

www.cybersecuritycoalition.be/tools/

Safeonweb.be

www.safeonweb.be/fr/home

Safeonweb.be a pour ambition d'informer rapidement et efficacement les citoyens belges en matière de sécurité informatique

VBO FEB
Verbond van Belgische Ondernemingen
Fédération des Entreprises de Belgique

CONTACT

Nathalie Ragheno

Premier Conseiller
Eerste Adviseur
Centre de compétence Droit & Entreprise
Competentiecentrum Recht & Onderneming

T +32 2 515 09 52 • M + 32 477 45 82 38
nr@vbo-feb.be

VBO FEB
Verbond van Belgische Ondernemingen
Fédération des Entreprises de Belgique

Creating value for society

Verbond van Belgische Ondernemingen vzw
Fédération des Entreprises de Belgique asbl

Rue Ravensteinstraat 4, 1000 Brussel/Bruxelles
BE476 519 923 – RPR Brussel/Bruxelles
www.vbo-feb.be – avh@vbo-feb.be