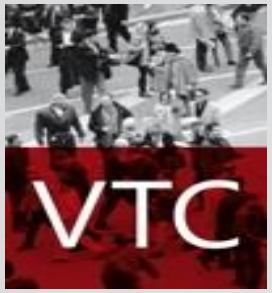


Gegevenslekken

Een analyse van meldingen
Periode : 2020 – 2022

Marc Nyssen, Anne Teughels
Vlaamse Toezichtcommissie

Deze sessie :

Doel : informeren en interageren (*dit is een workshop!*)

1) Presentatie VTC activiteiten
2) Hoofdonderwerp : focus op de gegevenslekken
3) Uw ervaringen
4) Opinies
5) Raadgevingen aan VTC

VTC werkschema

1) Adviezen wetgeving
2) Diverse adviezen en aanbevelingen
3) Datalekken
4) Klachten
5) Inspecties
6) Contact met het werkveld
7)===> ***Slechts enkele actiemiddelen :***

VTC werkschema

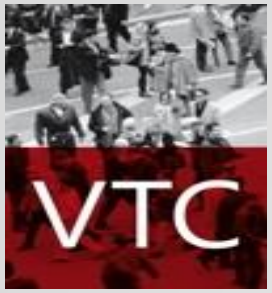
Actiemiddelen (maatregel artikel 58,2,AVG) :

- ☒ waarschuwing (a)
- ☐ berispt (b)
- ☐ gelast de verzoeken van de betrokkene tot uitoefening van zijn rechten in te willigen (c)
- ☒ gelast de verwerking in overeenstemming te brengen met de AVG (d)
- ☐ gelast de inbreuk aan de betrokkenen mee te delen (e)
- ☐ legt een tijdelijke verwerkingsbeperking op (f)
- ☐ legt een tijdelijk verbod op (f)
- ☐ legt een definitieve verwerkingsbeperking op (f)
- ☐ legt een definitief verwerkingsverbod op (f)
- ☐ gelast de persoonsgegevens te rectificeren(g)
- ☐ gelast de persoonsgegevens te wissen (g)
- ☐ gelast de verwerking te beperken (g)

VTC werkschema

Opgelegde maatregelen :
(vooral onderwijs en lokale besturen)

- in 2019 werden 185 instanties berispt
- Uitzonderlijk wordt een verwerking stopgelegd



DataNews

5 jaar GDPR: 5.815 gegevenslekken

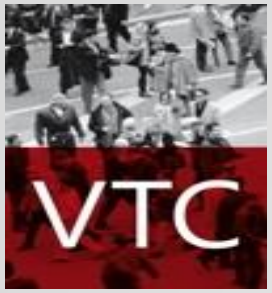
De bekendste datawetgeving van Europa, de GDPR of AVG, bestaat vandaag vijf jaar. In die periode werden er in België heel wat datalekken gemeld, en werden er ook heel wat adviezen, inspecties en uitspraken gedaan.

Toezicht op gegevensinbreuken

In 2022 ontving de GBA **1.420 meldingen met betrekking tot gegevensinbreuken** en startte ze zelf ook 6 dossiers op naar aanleiding van een vermoedelijke gegevensinbreuk met grote maatschappelijke impact waarvoor nog geen melding bij de GBA werd gedaan.

Onderstaande tabel geeft inzicht in de meest voorkomende oorzaken van de gegevensinbreuken. Bijna de helft van de gegevensinbreuken werd veroorzaakt door een menselijke vergissing.

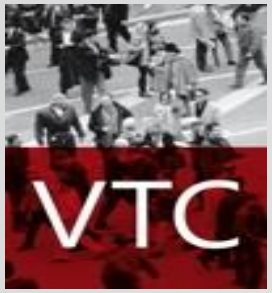
Meest voorkomende oorzaken gegevensinbreuken	Aantal
Menselijke vergissing	47%
Hacking, phishing en malware	25%
Oneigenlijk gebruik toegangsrechten	9%



Ter info: uit jaarverslag GBA:

Behandeling van gegevensinbreuken
2022 leek het jaar waarin vooral Belgische steden en gemeenten het slachtoffer werden van ransomware-aanvallen. Dit beeld dient evenwel enigszins genuanceerd te worden. Van de 1.426 nieuwe geopende gegevensinbreukdossiers in 2022, kunnen 361 onder hacking, phishing en malware worden geplaatst. Van deze 361 dossiers konden **135 (of 37%)** gekwalificeerd worden als **ransomware-aanvallen** en binnen deze groep had **8 % (noot secr: 10**) betrekking op Belgische steden en/of gemeenten (noot secr: Vlaamse steden en gemeenten hebben waarschijnlijk dubbel gemeld bij GBA en VTC). Een gelijkaardig percentage had betrekking op Belgische ziekenhuizen en/of woonzorgcentra. Het overgrote deel van de gemelde ransomware-incidenten vindt dus plaats bij private spelers.

In 2022 heeft het Algemeen Secretariaat **1.378 dossiers in verband met gegevensinbreuken** in staat gesteld. Naar aanleiding van 101 meldingen nam het Algemeen Secretariaat contact op met de verwerkingsverantwoordelijke en zorgde voor de opvolging hiervan. In een aantal gevallen werden deze dossiers op het Directiecomité geagendeerd en naar aanleiding hiervan werden 2 dossiers aan de Inspectiedienst van de GBA overgemaakt.



Analyses datalekken 2020-2022

1. Jaaroverzichten 2020, 2021, 2022
2. Analyse versus VTC aanbevelingen
3. Specifiek « onderwijs »
4. Maatregelen genomen door de « slachtoffers »
5. Aanbevelingen VTC

Overzicht per jaar

	2020	2021	2022
Phishing/hacking	68	70	68
Ransomware – cryptolocker	5	1	3
Diefstal	12	12	7
Misbruik toegangsrechten	16	8	
Publicatie soc-med-pers	3	4	1
Fysiek verlies-onbeschikbaarheid	14	3	10
Ongewild verkeerde bestemmeling	14	10	53
Verkeerde bestemmeling/teveel info	6	8	25
Onachtzaamheid/brieven/documenten	53	62	38
Ongewild doorgave door fout in toepassing	5		
Gebruikers- en toegangsbeheer	13	19	4
	209	**197**	**209**

Minimale aanbevelingen (o.a. VTC)

1) Zorg voor een business continuity and recovery plan met een getest back-up-systeem.

2) Bij back-ups wordt de 3-2-2 regel aanbevolen: voorzie 3 back-ups waarvan er 2 lokaal bewaard worden op 2 verschillende dragers en waarvan er 2 elders bewaard worden (1 op een andere locatie en 1 in de cloud*).

3) Zorg voor MFA/2FA op alle externe toegangen.

4) Voorzie netwerksegmentatie.

5) Voorzie een plan voor logging en monitoring en back-ups van de log servers.

6) Voorzie regelmatige updates om kwetsbaarheden snel te verhelpen.

Minimale aanbevelingen (2)

7) Voor grote bedrijven en organisaties is een gespecialiseerde business anti-ransomware oplossing aanbevolen.

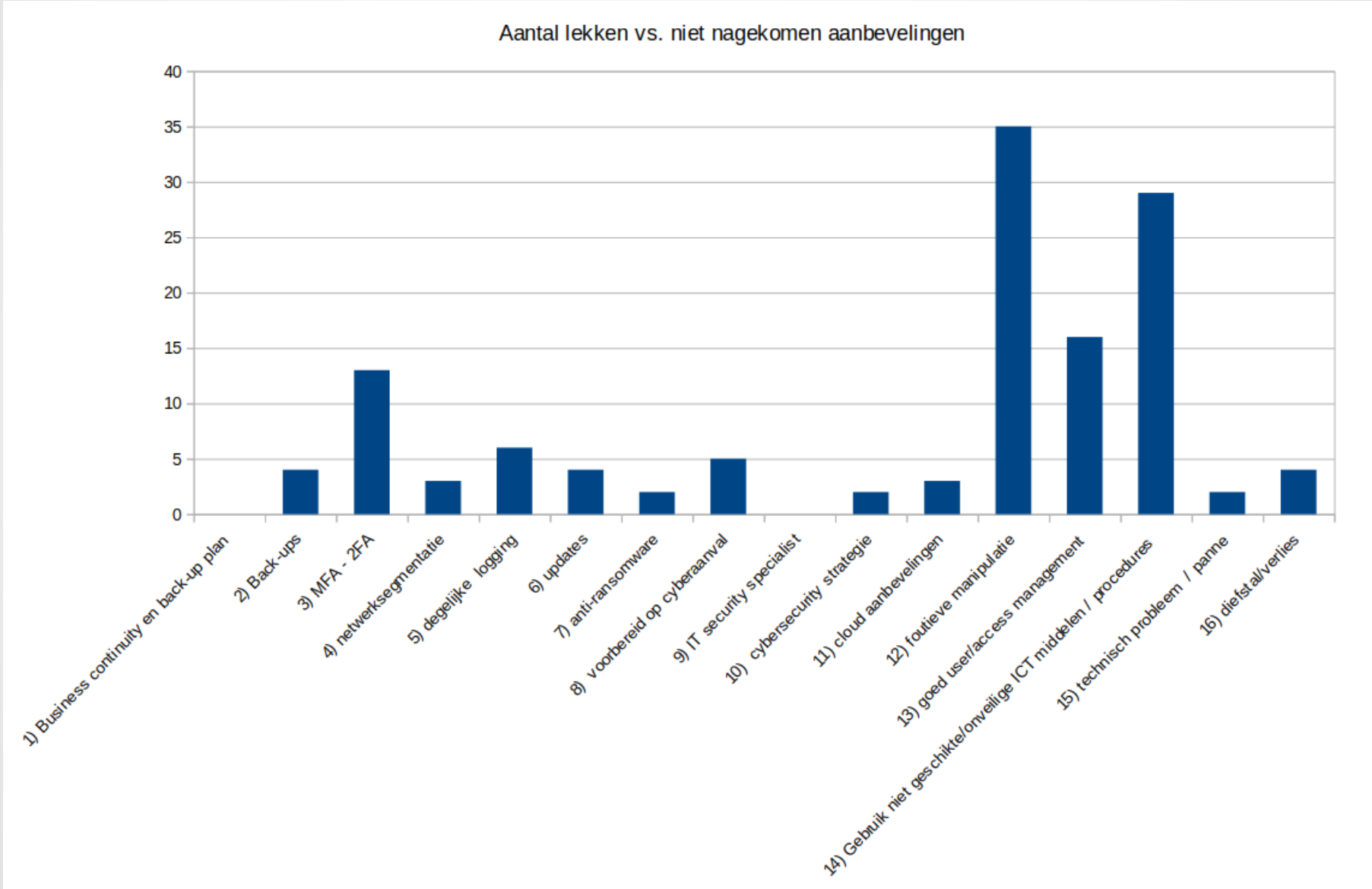
8) Zorg dat je organisatie voorbereid is op een cyberaanval.

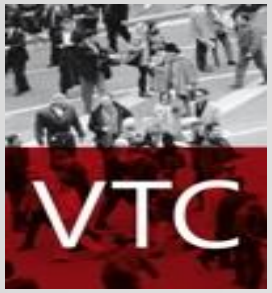
9) Laat je IT security architecture & policy nakijken door een specialist.

10) Maak werk van een cybersecurity strategie

11) * mits naleving van de richtlijnen van de VTC i.v.m. cloud

100 meldingen vs. aanbevelingen





Maatregelen genomen door de « slachtoffers »

- Technische analyses – via log-bestanden, historieken
- Updates / gebruik van beter aangepaste systemen / platformen
- Installatie anti-virus software
- Multi-factor-authenticatie wordt ingesteld
- Firewall-optimisatie
- Encrypterende bestandensystemen op de computers
- Aanpassing van procedures / nakijken van toegangsrechten
- Sensibilisering personeel / tuchtmaatregelen / opleiding
- Geheimhoudingsverklaringen / juridische stappen
- ...*(zie ook komende jaarverslagen met daarin meer informatie)*

Het is niet steeds « ICT »

gegevenslek	maatregel
Enveloppe met facturen is ergens open gegaan en inhoud is er uitgevallen. De enveloppe kwam leeg aan op de boekhouding	Contact opgenomen met Bpost Afspraak om grote enveloppen extra dicht te plakken met plakband

Maar meestal wel

gegevenslek	maatregel
op website gemeente kunnen onderwijsinstanties een bezoek aan de bib of één vd buurtfilialen aanvragen. Door het aan/afvinken ve optie id ontwerpmodule vh formulier in Drupal waren de ingevulde aanvraagformulieren leesbaar online+gecachet door Google	• Procedure bij Google om gegevens uit cache te halen • Melding ad auteur vh betrokken formulier met aandachtspunt rond het belang van aan/afvinken vd betrokken optie • Melding gegevensverwerker die webplatform beheert ifv mogelijke aanpassing beheersmodule

Specifiek onderwijs (1)

	2020	2021
Hacking (kwaadwillig)	4	5
Ongewilde/onterechte publicatie	1	1
Verkeerde bestemmeling, teveel/ verkeerde info	6	8
Niet respecteren van procedures		7

Specifiek onderwijs (2)

gegevenslek	maatregel
een leerling heeft zich via een keylogger toegang kunnen verschaffen tot het wachtwoord en de smartschoolacount van een personeelslid.	beslissing genomen om meteen multi-factor-authenticatie in te schakelen

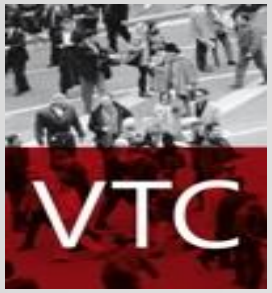
Ook talrijk: slordig nazicht van bestemmelingen

Vlaamse Overheid (1)

gegevenslek	maatregel
Personeelslid agentschap : gestolen laptop namen en adressen (privé en standplaats) van medewerkers; 700 personen	• Office 365 account werd verwijderd • aanmelden werd onmogelijk gemaakt • sensibilisering personeel • installeren Bitlocker encryptie

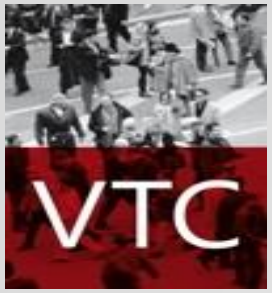
Vlaamse Overheid (2)

gegevenslek	maatregel
gestolen laptop - dief bekend = familielid, maar geen teruggave zeer gevoelige gegevens - beperkt aantal personen slechts gedeeltelijke disk encryptie	verhoogde beveiliging van verwerker gevraagd



Conclusies

- Bij de controle van meldingen van gegevenslekken stelt de VTC vast dat incidenten zeer **vaak integraal vermeden hadden kunnen worden** of dat minstens de impact ervan sterk gereduceerd had kunnen worden, door de implementatie van relatief rudimentaire en gangbare veiligheidsmaatregelen.
- Er blijkt vaak onvoldoende besef te zijn van de enorme risico-reducerende rol die dergelijke maatregelen kunnen spelen om de burgers te beschermen, en om het functioneren van overheidsdiensten te verzekeren.
- Om die reden zal de VTC toekomstige meldingen van gegevenslekken mede beoordelen aan de hand van de beschermingsmaatregelen die gepubliceerd werden door CERT.be en die intussen in het meldingsformulier zijn opgenomen.
- Met name voor het voorkomen en bestrijden van phishing- en ransomware-aanvallen zijn deze maatregelen cruciaal.



Vragen (workshop)

1. Weerstand tot melden … waarom ?

2. Ransomware : voorstel : algemene (uitgesproken) politiek : *de overheid betaalt nooit ! Budgetair verbod* . Zou dit volgens u impact hebben ?

3. Relatie met toeleveranciers van ICT systemen en middelen ? (er komt een vragenlijst)

4. Hoe kan VTC beter steun bieden ?
   - DPO’s
   - steden en gemeenten
   - scholen / schoolgemeenschappen
   - andere instanties

Rapportage sessies 1 + 2 (1)

1. Weerstand tot melden … waarom ?

graag: richtlijnen wat wel en niet hoeft gemeld te worden
lokale besturen: leidingevenden betrekken
melden zelf positief maken niet alleen « berispen »

2. Ransomware : voorstel : algemene (uitgesproken) politiek : *de overheid betaalt nooit ! Budgetair verbod*. Zou dit volgens u impact hebben ?

– goed idee maar: effectief tegenover de misdaadorganisaties
– dit zal niet alles oplossen
– cyberdivisie bij de politie beter ondersteunen → einde straffeloosheid

Rapportage sessies 1 + 2 (2)

3. Relatie met toeleveranciers van ICT systemen en middelen ? (er komt een vragenlijst)

– voorstel de CIO's van de voornaamste leveranciers aan te spreken/event

– verantwoordelijken bij de Vlaamse Overheid betrekken bij dit onderwerp

4. Hoe kan VTC beter steun bieden ?

- DPO's: steun om « oude lopende projecten » te bekijken qua gegevensbescherming

– er komt een VTC bevraging naar de DPO's betreffende de conformiteit van de leveranciers

– een netwerkplatform voor DPO's

– steun voor kleine entiteiten: scholen en VZW's