Your World First

C/M/S/
Law.Tax

De juridische aspecten van cybersecurity

IRO-bijeenkomst: Cyber Risk

Utrecht, 14 februari 2019

Leonard Böhmer & Erik Jonkman


European Commission
DIGITAL CONTRACTS
Creating a
#DigitalSingleMarke
European Commission
Commission européenne
Commission européenne
European Commission


EU Cyber Security Strategy
European Commission
Commission européenne

GDPR


Location service
Offline
Device name: S-K-O
S-K-O
History
Tracking
Geofence
Setting

CONSUMERS

European Commission

European Commission > Safety Gate: Rapid Alert System for dangerous non-food products

Safety Gate home | Back to report listings | Search alerts | IPSW 2018

The Rapid Alert System for Non-Food Products (RAPEX)

Share on

Alert number: A12/0157/19

Product: Smart watch for children

Category: Other

Name: Safe-KID-One

Brand: ENOX

Batch number / Barcode: 4260088860947

Type / number of model: Unknown

Type of alert: Serious

Risk type: Other

The mobile application accompanying the watch has unencrypted communications with its backend server and the server enables unauthenticated access to data. As a consequence, the data such as location history, phone numbers, serial number can easily be retrieved and changed.
A malicious user can send commands to any watch making it call another number of his choosing, can communicate with the child wearing the device or locate the child through GPS.

The product does not comply with the Radio Equipment Directive.

Measures ordered by public authorities (to: Distributor): Recall of the product from end users

Description: Smart watch for children in a cardboard box 12x15x8cm. the product was sold online.

Country of origin: Germany

Alert submitted by: Iceland

Cybersecurity in onze dagelijkse praktijk

– *First response team* (24/7) voor cyberincidenten

– Advisering over cybersecuritybeleid

Bijvoorbeeld:

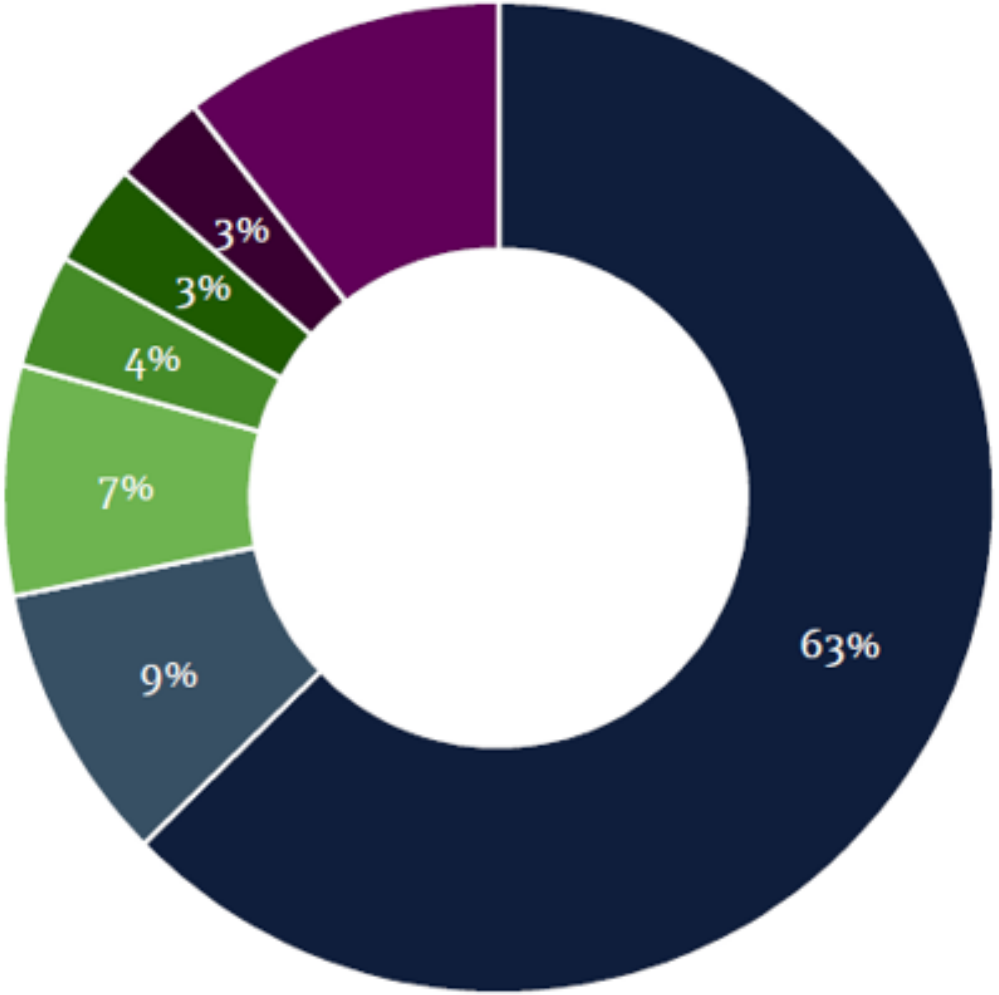
- Incidentprotocollen
- Inzet van camera's
- Monitoren van werknemers

– Adviseren en procederen over aansprakelijkheid en verzekeringen

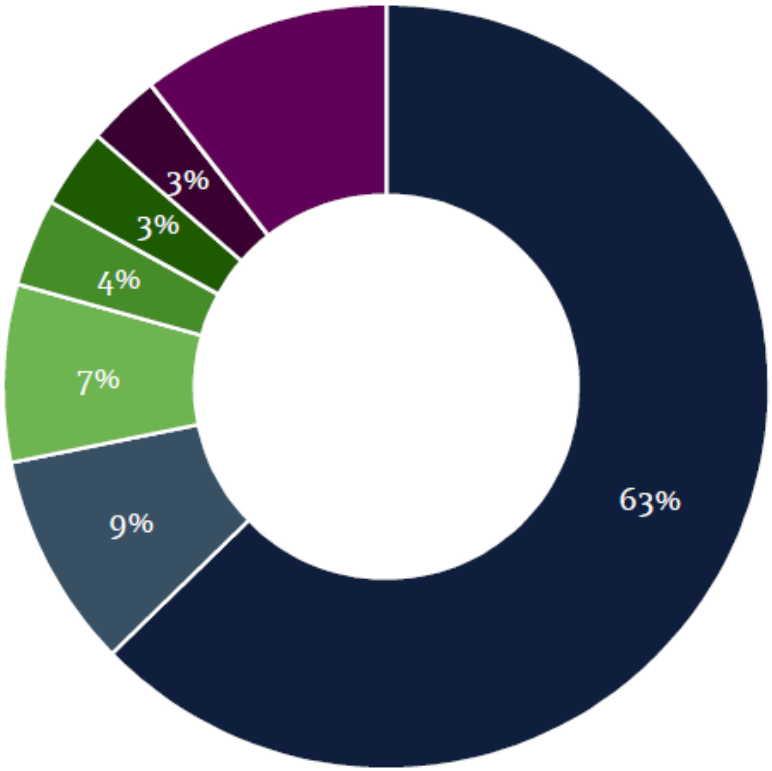
Vandaag op het menu: 3 hot topics

- De meldplicht datalekken in de praktijk
- Contracteren over informatiebeveiliging (i.h.b. verwerkersovereenkomsten)
- Cyberverzekeringen en aansprakelijkheid

I. De meldplicht datalekken in de praktijk


63%
9%
7%
4%
3%
3%

Meldingen in 2018:



- Persoonsgegevens verstuurd of afgegeven aan verkeerde ontvanger 63%
- Brief of postpakket kwijtgeraakt of geopend retour ontvangen 9%
- Apparaat, gegevensdrager en/of papier kwijtgeraakt of gestolen 7%
- Hacking, malware en/of phishing 4%
- Persoonsgegevens per ongeluk gepubliceerd 3%
- Persoonsgegevens van verkeerde klant getoond in klantportaal 3%
- Overig 11%

ENISA aanbevelingen voor impactbeoordelingen

Recommendations for a methodology of the assessment of severity of personal data breaches

Working Document, v1.0, December 2013

European Union Agency for Network and Information Security www.enisa.europa.eu

3.2 Definition of severity level

As introduced in the Section 2.2, the overall severity (SE) is calculated by the following formula:

$$SE = DPC \times EI + CB$$

The final score shows the level of severity of a certain breach, taking into account the impact to the individuals[8].

Severity of a data breach		
SE < 2	Low	Individuals either will not be affected or may encounter a few inconveniences, which they will overcome without any problem (time spent re-entering information, annoyances, irritations, etc.).
2 ≤ SE < 3	Medium	Individuals may encounter significant inconveniences, which they will be able to overcome despite a few difficulties (extra costs, denial of access to business services, fear, lack of understanding, stress, minor physical ailments, etc.).
3 ≤ SE< 4	High	Individuals may encounter significant consequences, which they should be able to overcome albeit with serious difficulties (misappropriation of funds, blacklisting by banks, property damage, loss of employment, subpoena, worsening of health, etc.).
4 ≤ SE	Very High	Individuals may encounter significant, or even irreversible, consequences, which they may not overcome (financial distress such as substantial debt or inability to work, long-term psychological or physical ailments, death, etc.).

3.3 Flags

Once the severity level has been defined, it can be accompanied by flags indicating certain elements of the breach that, although they do not affect a priori the scoring, they are important for the final assessment. For the purpose of the methodology, two flags have been considered:

Number of individuals breached exceeds 100. Data of an individual, breached in the context of a bigger incident, can potentially be more easily disclosed, whereas at the same time a high number of affected individuals influences the overall scale of the breach.

Data unintelligible. Unintelligibility (e.g. in the form of strong encryption and without key compromise) can substantially decrease the impact to individuals, since it highly decreases the possibility of unauthorized parties accessing the data.

[8] Table setting the levels of severity of a data breach was first introduced in the "Recommendations on technical implementation guidelines of Article 4", page 24, but has been made more precise in this document.

Het online meldloket van de AP

2. Tijdlijn

Exacte datum waarop de inbreuk was, indien bekend

Startdatum van de periode waarbinnen de inbreuk was

Einddatum van de periode waarbinnen de inbreuk was

Duurt de inbreuk op dit moment nog voort? Kies er een

Wanneer werd de inbreuk ontdekt?

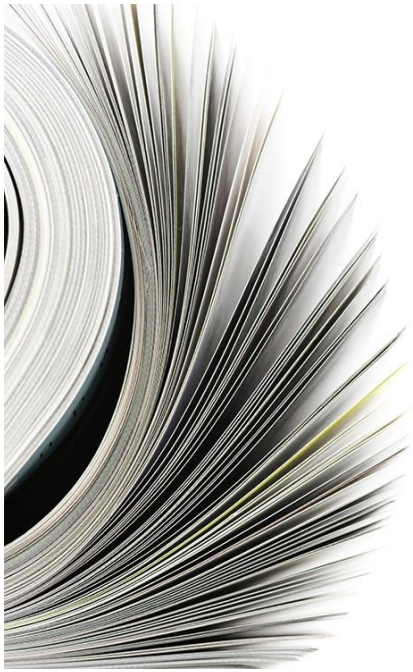
Als u de inbreuk later meldt dan 72 uur na de ontdekking, wat is daarvan dan de reden?

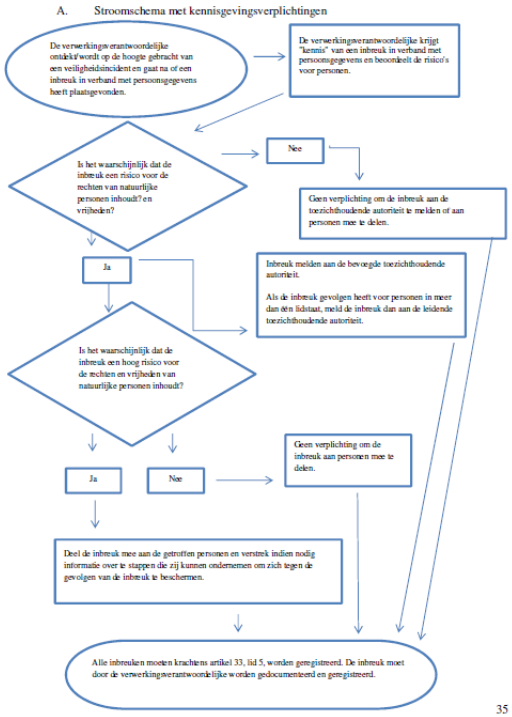
3. Gegevens over het datalek

3.1 Aard van de inbreuk

Inbreuk op de vertrouwelijkheid van de gegevens Kies er een

1. <u>Implementeer</u> een incidentprotocol.





2. Bewaak de communicatie tussen verschillende disciplines

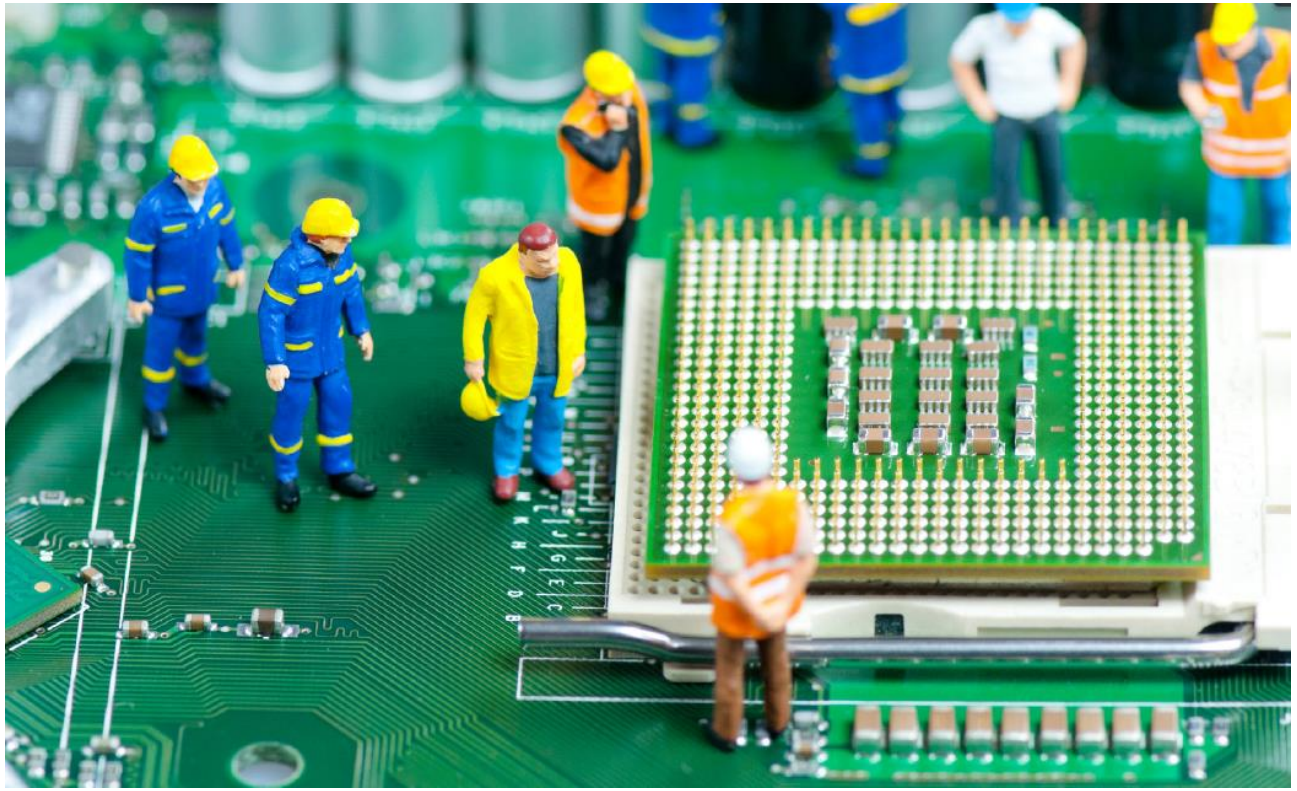
3. Ga verstandig om met 72 uur

4. Benut kansen op aanvulling en intrekking

5. Kies bewust wie je wel/niet informeert

AUTORITEIT
PERSOONSGEGEVENS

6. Ga verstandig om met IT-dienstverleners



De Autoriteit Persoonsgegevens in 2018

- 14.489 datalekmeldingen beoordeeld

- In 298 gevallen “actie ondernomen”, d.w.z.:
  - 39%: aanvullende informatie opgevraagd
  - 35%: het sturen van een normuitleggende brief
  - 23%: normoverdragend gesprek gevoerd

- In vier gevallen is een onderzoek gestart

- In nog eens drie gevallen is een kortlopend onderzoek gestart

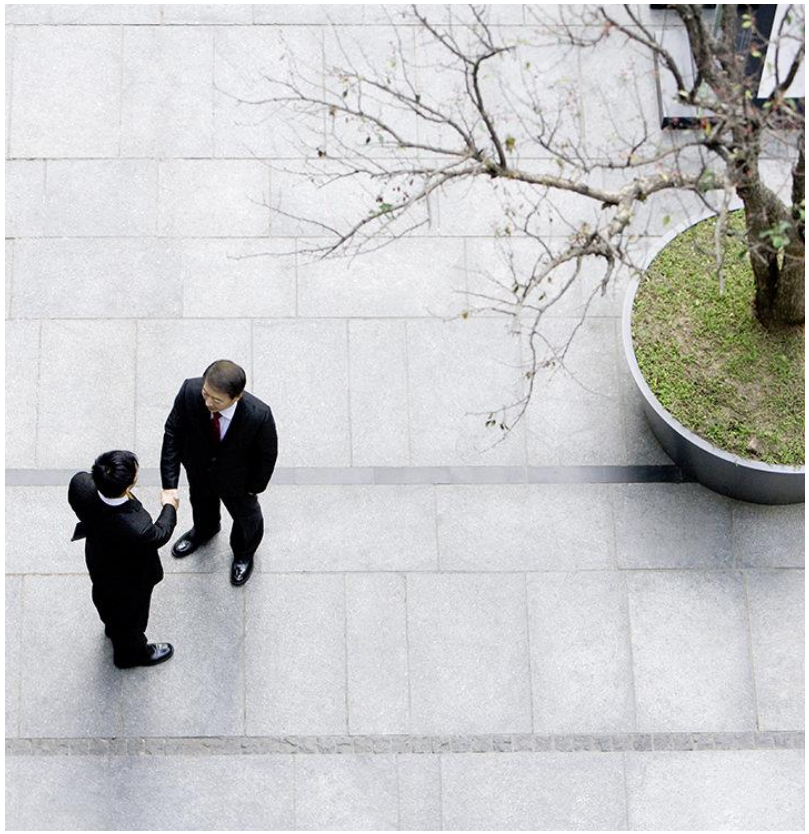
II. Contracteren over informatiebeveiliging: verwerkersovereenkomsten in de praktijk

De “hot spots” bij de onderhandeling

- Notificatietermijnen bij incidenten

- Informatiebeveiligingsnormen

- Beperking van aansprakelijkheid



III. Cyberverzekeringen en aansprakelijkheid

Vragen?

C/M/S/ Law-Now™

Your free online legal information service.

A subscription service for legal articles
on a variety of topics delivered by email.
www.cms-lawnow.com

C/M/S/ e-guides

Your expert legal publications online.

In-depth international legal research
and insights that can be personalised.
eguides.cmslegal.com

CMS locations:
Aberdeen, Algiers, Amsterdam, Antwerp, Barcelona, Beijing, Belgrade, Berlin, Bratislava, Bristol, Brussels, Bucharest, Budapest, Casablanca, Cologne, Dubai, Duesseldorf, Edinburgh, Frankfurt, Geneva, Glasgow, Hamburg, Istanbul, Kyiv, Leipzig, Lisbon, Ljubljana, London, Luxembourg, Lyon, Madrid, Mexico City, Milan, Moscow, Munich, Muscat, Paris, Podgorica, Prague, Rio de Janeiro, Rome, Sarajevo, Seville, Shanghai, Sofia, Strasbourg, Stuttgart, Tirana, Utrecht, Vienna, Warsaw, Zagreb and Zurich.

---

www.cmslegal.com