



Legally compliant through a cyber incident

OWASP, 26.02.2025

“Global Digital Law Experts”

Olga Stepanova

Lawyer | Partner

LL.M. (Berkeley), CIPP/E

Specialist lawyer for information technology law

Specialist lawyer for intellectual property law

Fields of activity

- International data protection consulting
- AI Regulation, DORA and NIS-2
- Representation in administrative court and official proceedings in data protection law
- Contract law with a focus on IT law
- External data protection officer

bytelaw



Dirk Koch

Lawyer | Partner

CEHv11 – Certified Ethical Hacker /
Data Protection Risk Manager / CIPP/E

Fields of activity

- Breach Counselor / Crisis Preparation
- IT-Security / ISMS
- NIS-2 / BSI basic protection consulting
- Advice on IT-related offenses
- Corporate governance
- IT and data protection compliance
- External data protection officer



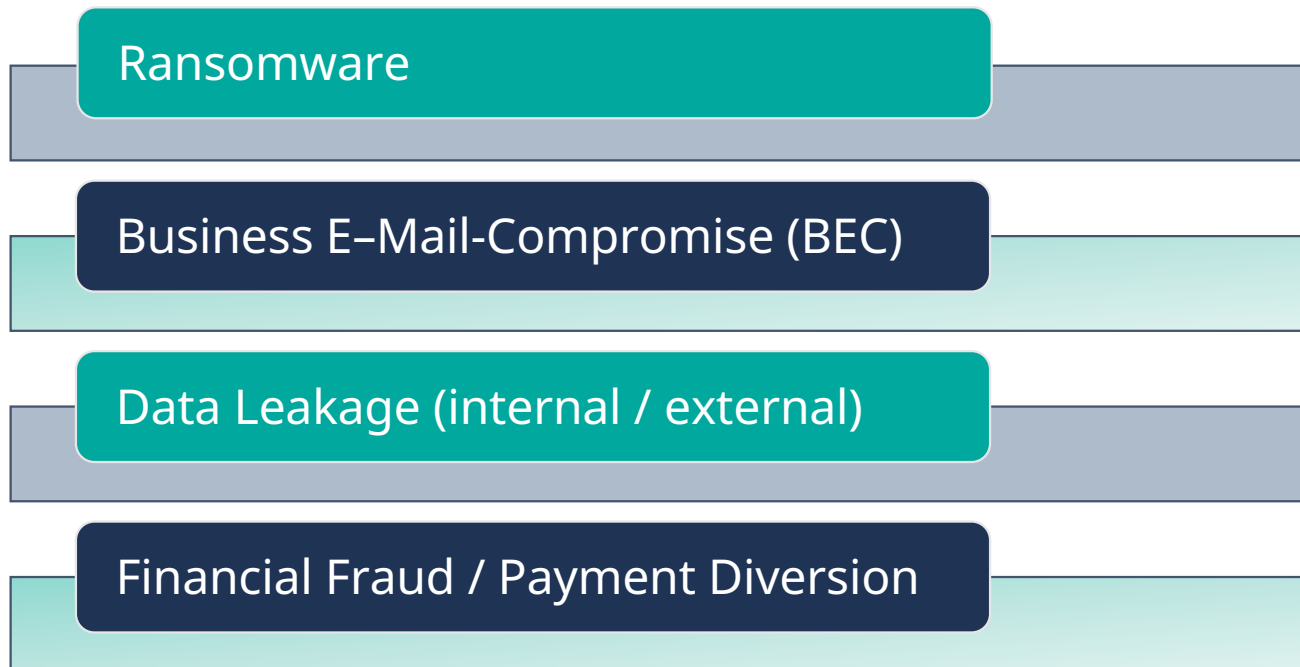
What do we need to protect against?



- Loss of ability to work (provision of the service)
- Claims for damages (partners / suppliers / customers)
- Claims for damages - GDPR
- Sanctions - legal



Current **threat** situation



> Overview– legally secure



1

Decisions in times of crisis

2

Dealing with the
perpetrators

3

Dealing with the authorities

4

Dealing with insurance
companies

5

Dealing with employees,
suppliers, etc.

Decisions in times of crisis



01

Making documented decisions

- a) Obtain knowledge
- b) Weigh up / obtain expertise
- c) Make and document decision

02

Define decision-making competencies in advance

- a) Guidelines for preparation
- b) Clear communication - **Who is the decision-maker in the incident?**

03

Establishment of a crisis team to maintain the flow of information

04

Documented decisions from the group are difficult to legally define as "wrong"

➤ Dealing with the perpetrators



1

Define goals of communication
with offenders

2

Weighing up goals against
risks

3

„Support for criminal
organizations”

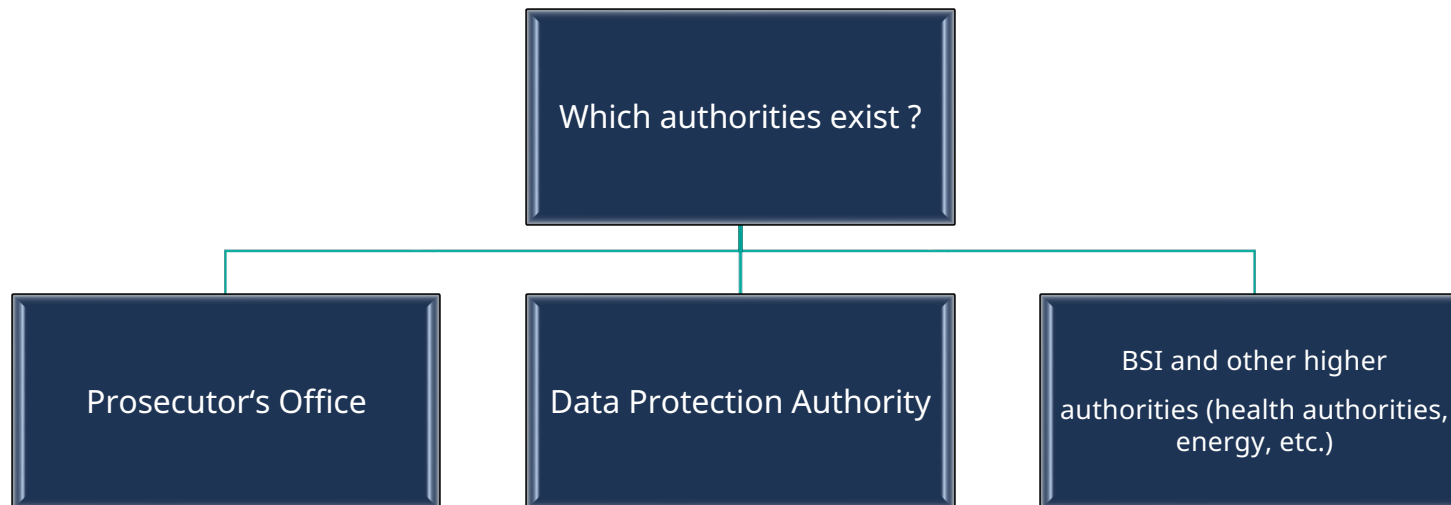
4

Consultation with the authorities
on communication

5

Consultation with the insurer about
communication

Dealing with the **authorities**



When do I contact the authorities?



Who and how do I communicate with the authorities?

Dealing with insurance companies



- Before the incident:
Know what the insurance company expects from you
- Familiarize yourself with the emergency plan



- Get to know insurance conditions quickly



- Close contact with the insurance company if desired

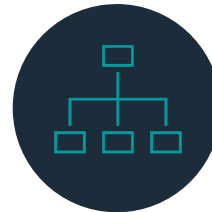


- Business interests take precedence over insurance interests

Dealing with employees, suppliers, etc.



Communication must be clear and consistent



Build up strategically / information in stages



Greatest possibility of damage



Transparent within the legal framework

- What contracts exist?
- Have obligations been dealt with?
- Do you know your contact persons?

Preparation of an incident

1. Guidelines on the cyber incident procedure

- Competencies
- Determining the thresholds for incidents
- Minimum measures for the individual parts of the organization

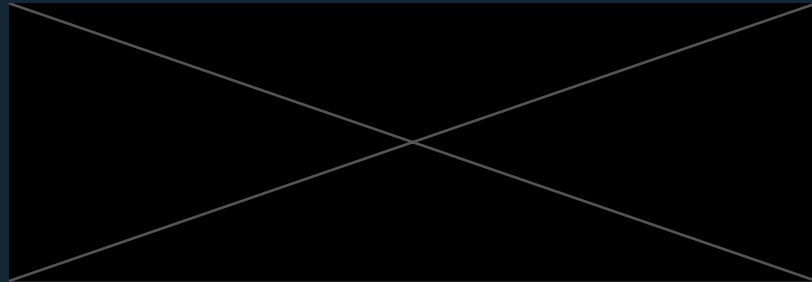
2. Know your contracts

- Contact IT security
- Special regulations (fixed contractual penalties / short deadlines / special features)
 - Data protection contact

➤ Service provider in the incident




- ➔ Bring neutrality to the incident (not involved in set-up or operation)
- ➔ Expert analysis and assessment of the incident
- ➔ Mediation between the parties involved and support in finding a solution
- ➔ Documentation of the incident and preparation of an objective report
- ➔ Recommendation of measures for damage limitation and future prevention




100101001010101
1010101010101**DATENSCHUTZ**100101
10100**DATENSICHERHEIT**1001010
01010101**DIGITALES**100101
0010101010110100

bytelaw Attorneys

Koch • Stepanova • Veeck Part mbB
Bockenheimer Landstraße 51-53
60325 Frankfurt am Main
Germany

 +49 69 153 91 91 90

 Info@byte.law

 +49 69 153 91 91 91

 www.byte.law

Reg: PR3036 Amtsgericht Frankfurt am Main