CYBER SECURITY AND BUSINESS CONTINUITY

INDUSTRIENS FOND

SDU

ROYAL DANISH DEFENCE COLLEGE

Assume Breach

www.cyber-smv.dk

The tool has been developed as part of the project **Cybersecurity and Business Continuity** (www.cyber-smv.dk), supported by the Danish Industry Foundation. Published on May 12, 2026.

Assume breach

Purpose

→To create a realistic understanding of risk and focus on consequence reduction rather than perfection.

Mental model

→*The question is not if something goes wrong, but when.*

Participants

→All employees.

→No technical prerequisites required.

Input

→A realistic case (e.g., phishing email, incorrect recipient, lost device) (see the following pages).

→A brief introduction to the “Assume Breach” principle.

Case: Background

→A Danish manufacturing company with approximately 90 employees produces components for the machinery industry. The company has both:
  → **Information Technology (IT)** (email, ERP, CRM, etc.).
  → **Operational Technology (OT)** (MES, SCADA, etc.).
→IT and OT are partially interconnected to support efficient operations and reporting.
→The company has basic IT security measures in place but is not a large enterprise with its own dedicated security team.
→Management has decided to adopt the “Assume Breach” principle - meaning that the company plans its security as if an attack has already occurred.

Case: The incident

→An employee in procurement receives an email that appears to come from a known supplier. The email contains an attached document with an updated price list. The employee opens the document and subsequently logs into the ERP system as usual.

→Without the employee's knowledge, the login credentials have been intercepted by an attacker, who now has access to the employee's account.

→The attacker then attempts to:

- →Gain access to the administrative functions of the ERP system.
- →Move further into the production systems.
- →Retrieve information about orders and suppliers.

Case: Discussion questions

1. **Identification**
   → Where in the case has the company already been compromised?
   → What signs could indicate that a security breach has occurred?
2. **Assume Breach mindset**
   → How does “Assume Breach” differ from focusing on preventing all attacks?
   → Which specific measures in the case support the “Assume Breach” approach?
3. **Consequence limitation**
   → What could the consequences have been without segmentation and role-based access control?
   → Which business risks were reduced?
4. **Transfer to your own daily work**
   → Where in your own company could a similar breach occur?
   → What can employees concretely do to support “Assume Breach” in practice?

Case: Possible solutions for Identification

→**Where in the case has the company already been compromised?**
- →The company is compromised the moment the employee opens the attached document and the attacker gains access to the employee's login credentials.
- →The breach therefore occurs before any visible problems arise.

→**What signs could indicate that a security breach has occurred?**
- →Login from an unusual location or at an unusual time.
- →Attempts to access functions that the employee does not normally use.
- →Multiple failed login attempts or repeated requests.
- →Alerts from monitoring and logging systems.

👉 **Important learning point:** A breach is rarely detected at the moment the incident occurs, but rather through abnormal behavior.

Case: Possible solutions for the Assume Breach mindset

→How does "Assume Breach" differ from focusing on preventing all attacks?

→Instead of believing that all attacks can be prevented, "Assume Breach" is based on the assumption that the attacker is already inside the system. The focus shifts from perfection to resilience and damage limitation.

→Which measures in the case support "Assume Breach"?

→Role-based access rights (the attacker only gains the same limited access as the employee).
→Network segmentation (office IT cannot freely access production IT).
→Multi-factor authentication (prevents escalation of access privileges).
→Logging and monitoring (the breach is detected quickly).

👉 The **key point** is that the systems do not blindly trust that a user is legitimate.

Case: Possible solutions for Consequence limitation

→What could the consequences have been without segmentation and role-based access control?

- → Access to production systems and risk of production downtime.
- → Manipulation or deletion of orders and bills of materials.
- → Theft of supplier and customer information.
- → Financial losses and delivery disruptions.

→Which business risks were reduced?

- → Risk of production downtime.
- → Risk of loss of customer trust.
- → Risk of financial losses and breach of contracts.
- → Risk of regulatory consequences (e.g., related to NIS2).

👉 **Assume Breach** - protect the business - not just IT.

Case: Possible solutions for Transfer to your own daily work

→Where in the company could a similar breach occur?

- → Typically, in functions with:
  - → Extensive email communication (e.g., procurement, sales, finance).
  - → Access to central systems.
  - → Collaboration with external suppliers.

→What can employees concretely do to support Assume Breach?

- → Respond quickly to suspicious behavior and report it.
- → Accept security measures such as multi-factor authentication.
- → Follow the principle of least privilege.
- → Be aware that “normal” actions can be exploited by attackers.

→ 👉 **Message:** Employees are an active part of security, not just a risk.