INCIDENT RESPONSE

Identification, containment, eradication, and recovery of security incidents in computer networks

When a security incident occurs, effective and efficient incident response is required. Security incidents can take many different forms and be anything from an active threat, an attempted intrusion, a successful compromise of the security perimeter, or even a data breach.
Improsec offers deployment of an internationally accredited Computer Security Incident Response Team (CSIRT) to assess the scope of the incident and the potential damages caused, and to work with the impacted business to develop a mitigation plan until the incident is resolved.
The incident response team works through a controlled and highly documented process to contain, eradicate, and recover from the incident - and to answer important questions like "how it happened" and "how to avoid similar incidents in the future".
Our team of incident responders have broad experience in responding and handling incidents of all sizes, ranging from simple security breaches to advanced and complex cyber-attacks.

Value

- Precise and accurate identification of damages and events leading to the security incident
- Understand the true impact and severity of a security incident to enable the appropriate level of response
- Enable fast and effective mitigation without compromising or destroying relevant artifacts needed for the investigation
- Identify impact caused by malicious attackers, compromised insiders, or even insiders unknowingly participating in the security incident
- Controlled containment, eradication, and recovery from the security incident
- Advise on how to avoid re-occurring security incidents
- Supports the Data Protection Officer (DPO) in delivering timely and accurate information to DPA (National Data Protection Authority) in case of a data breach of personal data
- Skilled advice to C-level crises management and in the dialogue with authorities e.g. police

Product

The deliverables of the incident response team will vary depending on the nature of the incident. The typical deliverables during an incident are:

- Frequent management and/or board information updates for executive overview and informed decision enabling
- Frequent technical feedback on results and conclusions during the response phase
- A post-incident report in detail describing the actions performed by the CSIRT team and the results achieved
- Recommendations and next steps (if applicable)

Method

The incident response process is delivered in different stages – inspired by the ISO/IEC Standard 27035 supported by various industry best practice:

- Plan and prepare for handling security incidents
- Identify detection mechanisms and assess detection capabilities
- Triage security events and decide on incident handling response
- Deploy the CSIRT team to analyze, investigate, contain, and recover from the incident
- Assess learning and update risks based on the incident and implement systematic improvements to the security management process

Improsec A/S
www.improsec.com
Telephone: (+45) 5337 5337
Email: info@improsec.com