Guide to Managing IT Security Incidents

Incident Response: Respond with speed and precision.

Rapid and appropriate response to IT security incidents

IT security incidents can affect any company or organization. A well-thought-out Incident Response Plan helps effectively minimize the impact of IT security incidents.

An efficient emergency plan is especially important for small businesses, enabling them to respond effectively to incidents even with limited resources, without delays or uncertainties. This helps minimize operational disruptions, protects sensitive data, strengthens the security culture, and ensures compliance with legal requirements.

The key to responding to security incidents is to act quickly. Targeted countermeasures can substantially mitigate the technical and financial impacts of cyberattacks, expediting the return to normal business operations. As such, implementing an effective Incident Response Plan is essential for every organization, irrespective of size or industry.

Defining IT Security Incidents

Clear guidelines and examples make it easier for users to recognize security-related incidents. Some examples include:

- **CEO fraud attacks**: Attempts to obtain confidential information or force bank transactions through fake emails or websites typically result in significant financial losses. Awareness helps clarify such phishing campaigns.

- **Ransomware infection**: Malware that encrypts files or the entire computer and demands ransom for restoration should be reported immediately to prevent potential spread in the system and document any data theft.

- **Loss or theft of devices**: Physical losses of computers, laptops, or mobile devices with access to company resources must be reported to IT immediately to be able to lock devices or user accounts and remotely erase data.

- **Unauthorized access to systems**: Suspected unauthorized access to systems or networks, including unusual logins, should be reported to IT immediately to detect intruders in the system and close security gaps.

Blechturmgasse 11 | 1050 Vienna | Austria | Phone: +43 1 589 95-0 | office@ikarus.at | www.IKARUSsecurity.com

User Perspective: Reporting a Cybersecurity Incident

Incident reporting is the initial step in an Incident Response process. Therefore, continuously educate and encourage your employees to recognize signs of security breaches and anomalies and report them promptly.

Appropriate behaviour during an IT security incident is crucial to minimize its impact. Clear communication of behavioural guidelines, efficient communication channels, relevant points of contact, and essential information needed by IT or security personnel for incident handling promotes effective collaboration.

- → Raise awareness of the dangers and potential entry points.
- → Inform about current threats such as ransomware and phishing campaigns.
- → Share knowledge about common attack vectors and suitable countermeasures.
- → Position your IT department as the first point of contact for all questions and incidents.

User Tips for Behaviour

- ✓ Stay calm.
- ✓ Contact your IT hotline by phone.
- ✓ Immediately stop working on the IT system.
- ✓ Document what you see.
- ✓ Do not try to solve the problem yourself.
- ✓ Do not shut down the system ("pull the plug") to preserve evidence.
- ✓ Follow the instructions provided by your IT department.

Prepare for the following questions:

- → Who is reporting the incident?
- → Which IT system is affected?
- → What were you doing on the IT system?
- → What did you observe?
- → When did the event occur?
- → Where is the affected IT system located?

Time is the most crucial factor during a security incident. Do not hesitate to reach out to IT - it's better to make one call too many and quickly than to make one call too few!!

Tip: Like the familiar signs for "Behaviour in Case of Fire," it is advisable to equip all offices with an "**IT Emergency Card**". This card should include the correct contact person(s) for IT emergencies and their contact information, what information should be relayed, and guidelines for appropriate behaviour.

Blechturmgasse 11 | 1050 Vienna | Austria | Phone: +43 1 589 95-0 | office@ikarus.at | www.IKARUSsecurity.com

IT Perspective: Handling Cybersecurity Incidents

IT personnel play a key role in managing security incidents. The principle of "keeping calm" is crucial here as well, to act thoughtfully and minimize the spread of damages.

Organizational and technical measures are equally important.

Organizational Measures for IT Emergencies

From an organizational perspective, it is important to know which authorities to inform and when.

- ✓ Immediately inform IT security officers, data protection officers, and IT operations.
- ✓ Follow the agreed responsibilities for communication, escalation, and reporting obligations.
- ✓ Keep all information from the IT Security Incident report at hand:
  - Affected systems
  - Affected users
  - Identified anomalies
  - Point of entry
  - Path of spread

Existing emergency plans (Incident Response Plans) should be practiced regularly or developed now if not already in place. Contact lists with key contacts, contact information, and responsibilities should always be up-to-date and readily available.

Tip: Establish an alternative communication channel far from your own IT infrastructure. Existing communication channels may already be monitored by the attacker.

Technical Measures for IT Emergencies

When dealing with computers affected by a security incident, extra caution is warranted. Several general considerations should be taken into account:

- → What user accounts exist on the system?
- → Are there user accounts with unnecessary elevated privileges?
- → If so, was this change to the user account made recently?
- → Who made the changes to the user account? When did this occur?
- → Don't just analyse the affected system - look for other computers that may be affected.
- → Disconnect the affected system from the production network - either through EDR solutions that support this or by unplugging the network cable, but never by turning it off!
- → If multiple systems are affected, disconnect them from the network simultaneously if possible.
- → Secure forensic data (memory dump, processes).
- → Consider systems as completely compromised.

Blechturmgasse 11 | 1050 Vienna | Austria | Phone: +43 1 589 95-0 | office@ikarus.at | www.IKARUSsecurity.com

- → If a user account is affected, consider the network as compromised as well.
- → Consider all access credentials stored on or entered into the affected systems after the infection as compromised.
- → Ensure the completeness and functionality of log files, especially firewall logs.
- → Log network traffic using appropriate systems. If such systems are not in use, set up a computer to receive analysable network traffic via SPAN ports.
- → Block malicious access on suitable systems (e.g., firewall).
- → Check for the presence of current backups - and whether they could be compromised.

Caution: An administrator account must never log in to a compromised system! This should only be done, if necessary, when the system is disconnected from the network!

Examining Log Data

Next, log data is examined, with logs from the firewall, proxy, mail server, and Active Directory being of particular interest. Unauthorized access attempts, IP addresses of attackers, suspicious URLs or downloads, phishing, or spam emails, failed or suspicious authentication or login attempts, changes to user accounts, or unusual access activities can be identified in this way.

Interpreting this data requires experienced personnel familiar with normal operations to detect malicious changes post-infection.

Rebuilding and Securing the System

The affected system should be rebuilt to ensure that no remnants or traces of malware remain. Afterward, it is crucial to learn from the incident: How did the malware infiltrate the system? The newly rebuilt systems must be hardened, and the entry vector closed.

When restarting IT systems, a specific sequence should be followed, with critical systems being brought back online or put into operation first. Checklists assist in implementation.

Resources:

- → IKARUS Incident Response Checklist for SMEs
- → IKARUS Emergency Plan for Ransomware
- → IT Emergency Card “Behaviour during IT Emergencies” (external)

Services:

- → IKARUS 24/7 incident.response: Emergency Service for Cybersecurity Incidents

Blechturmgasse 11 | 1050 Vienna | Austria | Phone: +43 1 589 95-0 | office@ikarus.at | www.IKARUSsecurity.com

Disclaimer

This guide is provided for informational purposes only and does not constitute legal, financial, or technical advice. The user assumes full responsibility for any actions or decisions made based on this guide. IKARUS accepts no liability for any technical or financial consequences arising directly or indirectly from the application or non-application of the information contained in this guide. It is the user's responsibility to consult appropriate professionals or advisors to address specific legal, financial, or technical questions.

About IKARUS Security Software GmbH

Since 1986, IKARUS Security Software has been at the forefront of cyber security development and implementation. Their proprietary Malware Scan Engine, user-friendly cloud solutions, and securing critical infrastructures are the focal points.

In collaboration with global leaders, IKARUS offers comprehensive cyber security services for organizations of all sizes and critical infrastructures - from Incident Response Services to Advanced Threat Protection and OT-Security Sensors, as well as the modular IKARUS Threat Intelligence Platform. The integration of partner technologies into the IKARUS data center in Austria/EU ensures full transparency and security in data processing.

Blechturmgasse 11 | 1050 Vienna | Austria | Phone: +43 1 589 95-0 | office@ikarus.at | www.IKARUSsecurity.com