Resilience Under Fire: Incident Response and Continuity in Critical Infrastructure

Michaela Uhríková

cloudfield

cloudfield

comma_0

What’s New with NIS2?

- §28 „Zabezpečení průmyslových, řídicích a obdobných specifických technických aktiv“
  - Policy Implementation vs. Real Business Security
- Efficient Use of Budget for NIS2 Implementation

What will I cover today?

- The role of Incident Response Plans in business
- How to build up effective Disaster Recovery Plans
- Creating supporting documentation not only for compliance purposes

Incidents that we can learn from

- Stuxnet Worm (Discovered in 2010)
- Ukraine Power Grid Attack (2015 & 2016)
- Rye Brook Dam (NY, 2013–2015)
- Florida Water Treatment Plant Attack (2021)

Lessons learned

- Delayed incident reporting worsens the impact.
- Poor cross-functional coordination between relevant depts.
- Failure to notify national authorities.
- Lack of tested recovery procedures.

Incident response plan

- Clearly defined roles and responsibilities – adjust it to your business needs.
- Ensure coordination between the depts. (IT, Legal, PR,..)
- Escalation paths are documented and rehearsed. (TTX)

Test your IRP by TTX

- **Simulates real-world attack scenarios** in a controlled, discussion-based setting.
- Helps **identify gaps in roles, communication, and procedures before** a real incident occurs.
- Promotes **team coordination** and sharpens decision-making under pressure.

IRP: Dos & Don´ts

Don'ts

- ✗ A state-of-the-art doc written by an external firm
- ✗ 20 pages long
- ✗ No one from the SOC/CSIRT team knows how to carry out half of the steps

Dos

- ✓ Clearly written with only essential steps to restore services
- ✓ Regularly tested, with team members personally executing the steps
- ✓ New employees with assigned roles are trained and have practiced their tasks

Disaster recovery plans

- **Critical systems and data recovery priorities** with clear RTO/RPO objectives.
- **Roles and responsibilities** for internal teams and external partners.
- **Step-by-step recovery procedures** for various disaster scenarios.
- **Regular testing and updates** to ensure plan remains effective and current.

DR: Dos & Don´ts

Don'ts

- ✗ A DRP that relies on having two live instances and simply turning one off and on — more like load balancing than true DR
- ✗ A formally written plan that looks functional on paper, but no one has ever dared to test it

Dos

- ✓ A DRP that is executed at least once a year, involving a full restoration of production data from backups to the live system
- ✓ DR plan that spins up a replica of the production system and restores all data from backup

Assume the breach

- Shift mindset: **Breaches are inevitable**, not just possible.
- Focus on **detection, response, and containment** over pure prevention.
- Build infrastructure with **zero trust principles** and **segmentation**

Key Takeaways

- **Compliance is not enough** — real resilience requires readiness.
- **Test your plans** before reality does.
- **Learn from past incidents** to strengthen future response.
- **Adopt an "Assume the Breach" mindset** to stay one step ahead.

THANK YOU!

Contact us

Michaela Uhríková

michaela.uhrikova@comma0.io

www.comma0.io