

20/20

Hindsight

A retrospective view of a security incident
at the University of Akureyri

Gunnar Ingi Ómarsson
Project Manager of IT
University of Akureyri

The problem with hindsight

Afterwards, everything looks obvious. During the incident, very little is.

Decisions come before certainty
Confidence is easy after the fact
Humility is harder, but more useful

“How do we make useful decisions when the situation is incomplete, uncertain and moving?”

Before the call

We were not careless. But we had assumptions.

Assumptions we carried

- We are a small university
- We are not an obvious financial target
- We are reasonably secure
- We will probably notice if something serious happens
- Other organisations should share more after their incidents

I used to ask:

“Why don’t they just tell us?”

Public statements often felt vague
Requests for details rarely helped
Rumours filled the gap
People read between the lines
I thought more openness was always better

**Then we became
the organisation with
the carefully worded
public statement.**

The call you never want to receive

CERT-IS contacted us with a warning about information from our systems.

Active Directory information appeared to be “in the wild”
Early concern around deeper compromise
Later analysis suggested directory information from AD
The actor mentioned was Karakurt
The exact path was unclear at the time

What we knew, feared and did not know

Incident stories become too clean after the fact.

We knew

AD information was exposed

We feared

Password material might be exposed
Access might still exist
More systems might be affected

We did not know

The exact entry path
The full scope
The safest level of communication

Containment before perfection

We acted before perfect certainty, because waiting also carried risk.

Reduce risk quickly
Keep essential services available where possible
Protect sensitive systems
Bring in expertise
Act before perfect certainty

Help over ego

Humility may be one of the most practical security controls you have.



Recognise limits
Bring in experts or specialists
Ask service providers for extra hands
Listen
Solve problems, don't defend the why

No shame, no scapegoat

Inside the incident, usefulness matters more than cleverness.

Useful review

This system created risk. How do we reduce it?
This process was unclear. Who owns it next time?
This communication was too slow. What role or template do we need?

Unhelpful criticism

How could anyone allow this?
Who is responsible for this mess?
I would never have done that.
This proves everything is broken.

The human incident

Taking care of the incident team is not softness. It is resilience.

Eat
Drink water
Take breaks
Step away from the screen
Sleep
Hand work over
Stop trying to be everywhere

Communication under constraint

Everyone wants information. Different audiences need different information.

Users

Protective guidance
Practical steps
Avoid panic

Leadership & authorities

Risk and decisions
Formal notification
Clear uncertainty

Public & peers

Understandable statement
Lessons when safe
No free intelligence

The outside noise

Judgement from limited information is easy. Support is more useful.

Tactless social media discussion
Support from people in the IT community
Mixed understanding, genuine concern and misunderstanding
User education cannot start during the incident

Be a cheerleader, not just a commentator.

First, how it ended

The incident was over in days. The work that came out of it took years.

WHAT WE REBUILT

Over in days. Rebuilt over years.

- Domain controllers rebuilt
- Segmentation reworked, firewall rules reviewed
- Procedures written down, not carried in heads
- Regular scanning, far more aggressive patching
- SOC service, better AV and email scanning
- **Security experts every two weeks, for two years**

The questions I would answer first

Asked what to do now, I would not start with a product. I would start here.

- 1 Know who to call
- 2 Know who decides
- 3 Know what you can shut down
- 4 Know how you will communicate
- 5 Know where your logs are
- 6 Know what you cannot do alone
- 7 Look after your people

20/20 Hindsight

Hindsight is clear. Incident response is not.

You are not too small to be interesting
You will not have all the facts when decisions are needed
Containment cannot wait for perfect certainty in the first phase
Communication is part of incident response
Culture matters under pressure
Look after the people doing the work

Not certainty. Humility.