Mistakes happen, either learn from them or rinse and repeat!

Gregor Wegberg | 35th Annual FIRST Conference, 8 June 2023
Gregor Wegberg
Head of Digital Forensics & Incident Response
Lecturer at Eastern Switzerland University of Applied Sciences

Fun fact: I have three passports / citizenships
(I am not a spy)
The following **lessons** are taken from our everyday life (responding to ransomware)
Failure is allowed if we learn from it

“One of the most important parts of incident response is also the most often omitted: learning and improving.”

Source: SP 800-61 Rev. 2
Source: ISO/IEC 27035-1:2023
How major incidents feel for most people

Mistakes happen, either learn from them or rinse and repeat!

8 June 2023
Your very first immediate measure: **Take a break** and drink some coffee/tea and relax.
The right tools are important. But **people** are the crucial factor.

Mistakes happen, either learn from them or rinse and repeat!
DFIR is difficult
Especially under high pressure

Obvious, yet crucial to internalize

► We are humans
► Humans make mistakes
► We will make mistakes

Many find it difficult to accept this during their first major incident.

Assume 50% of staff operates at 50% of normal capacity.
It’s difficult for everyone
What kind of incident is it? Ask questions! Be nice.
Why are you even trying?

Mistakes happen, either learn from them or rinse and repeat!

8 June 2023

Photo by Kelan Chad on Unsplash
Be wary of digital tools. Pen & paper works amazingly well
... to bring order to an incident
Think in **smaller, more modular** playbooks

Don't overwhelm yourself with all-encompassing playbooks, e.g., *THE RANSOMWARE PLAYBOOK*.

Many forms of cyber incidents require the same response activities. You can prepare for this!

- Immediate measures when our gut tells us panic
- Reset passwords and other secrets
Serious incidents take their time

Mistakes happen, either learn from them or rinse and repeat!

8 June 2023
Gregor Wegberg

Mastodon: @groggi@infosec.exchange
LinkedIn: /in/gregorwegberg
E-Mail: gregor.wegberg@oneconsult.com
Twitter: @gwegberg