G DATA

TRUST IN
GERMAN
SICHERHEIT

I told you so!

Musings about a blameless security culture

Tim Berghoff, Security Evangelist
@timberghoff

Tim.Berghoff@gdata.de

$whois

Tim Berghoff

Security Evangelist, G DATA CyberDefense

- With G DATA since 2009
- Does a lot of photo and video work on the side
- Likely to be found at a camera store near you

#ITSec
#MechKeyboards
#Tinkering

The way security incidents are dealt with

- Something goes wrong:
  Who did it?

- How can we make sure that nobody makes mistakes?

- How can we „discourage“ risky behavior?
  (a.k.a. How do we punish?)

Image source: Gizmodo.com

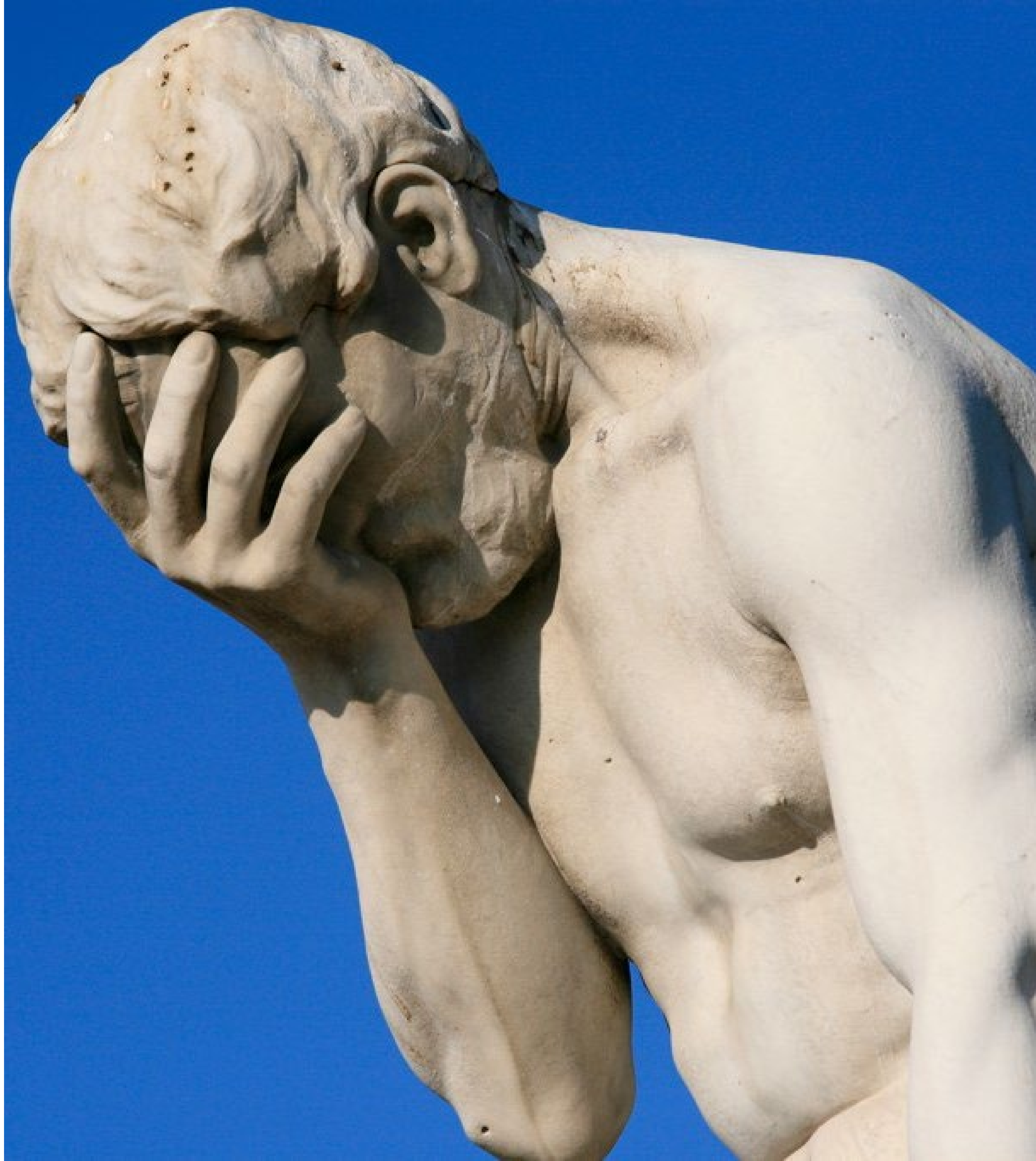
OFF WITH THEIR HEADS!

Why this is a problem?

- The answer is not always that simple
- There may be more than one answer
- Punitive action on „pawns“ will not fix a systemic issue

Often heard phrases after an incident

- „If it had been **me** in charge, this would never have happened!“
- „How did they NOT see that?“
- „How can one person be so stupid?!“
- „Well, I know nothing about security, **BUT**…“



Some harsh truths

- People like simple answers
- IT is usually deterministic in cause vs effect (also, we love us a good riddle)
- Meatspace is political. Always.

Accident at the Three Mile Island NPP

Who was to blame?

- Operator?
  - they shut off some very critical components (one being the primary cooling pumps – duh)
  - Misinterpreted several indicator values
- Manufacturer?
  - Controls & indicators was an absolute UI nightmare
  - Operators had to assume and infer a number of measurements

CORE TEMP

Prominent examples

Accident at the Three Mile Island NPP

Why did the operators do the things they did?

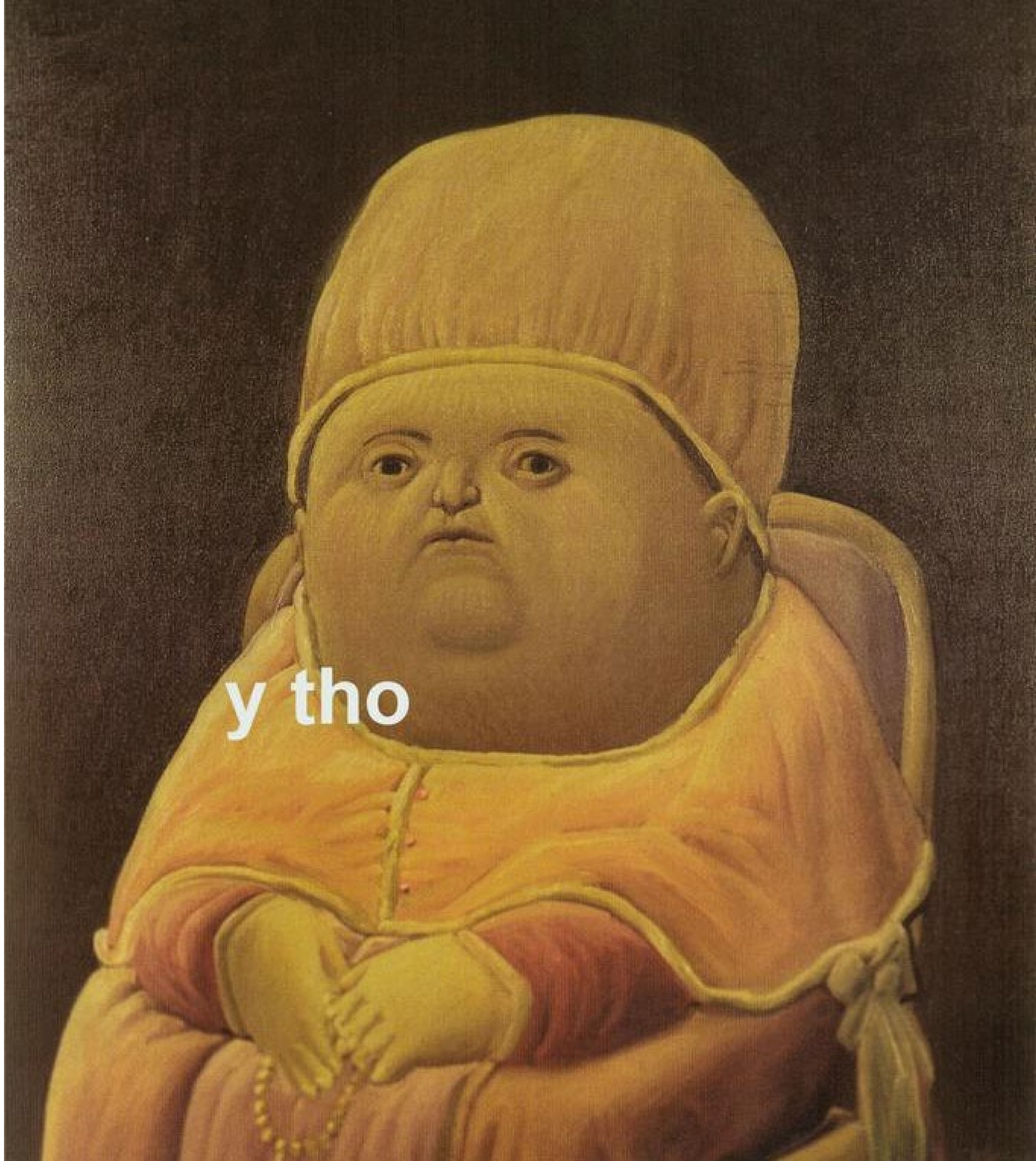
- They were very experienced reactor operators…on navy vessels
- Followed their training (which did not fully translate to power reactors)
- Massive information overload from technical systems
- The system did not feed them critical information quickly enough

They wanted to keep the reactor SAFE

Prominent examples

- The „Alarmtag“ (*alarm day*) in Germany on Sept 10, 2020 (a nationwide test of public alarm systems)
  - Multiple delays and failures
  - Entire campaign was lambasted & ridiculed
  - Head of the responsible department was let go days later

- First nationwide test in 30 years
- Many sirens had been physically removed, starting in the 1990s, despite protests
- Local governments decided to act without coordinating
- Federalism, yay…
- What was the purpose of a **test** again?



How does that help?

(it doesn‘t)

Go blameless?

What „going blameless“ is NOT:

- Sugarcoating things that went wrong
- Making errors „nameless“
- A „one and done“ thing
- A lever for / against a project or person
- Intuitive

- EASY

What „going blameless“ is:

- A systemic approach
- Demanding
  a fundamentally different culture
- Potentially a decade long process
- Excruciatingly hard
- Fraught with losses along the way,
  becaus, again, politics

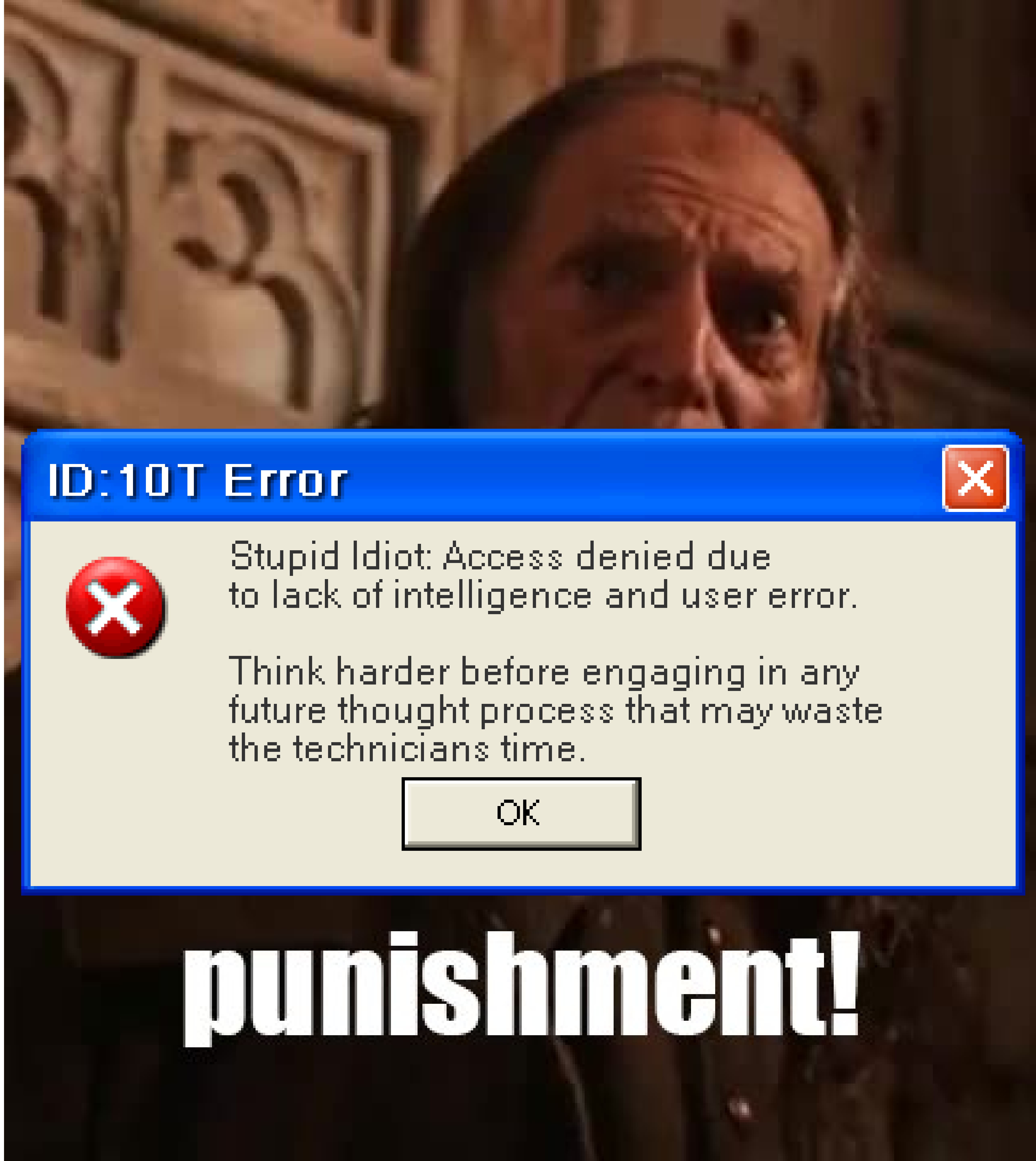
This is all well and good, but…

How does all this translate to security?

Would **YOU** go blameless in security?

A primer on going blameless

- Always assume the best intentions
- Do not always consider users as enemies. (Yes, I know – this is hard)
- Trust that people can do their jobs
- Do no punish



Stupid Idiot: Access denied due to lack of intelligence and user error.

Think harder before engaging in any future thought process that may waste the technicians time.

Ask the right questions:

- Go away from asking „**who** caused an incident“
- Instead, ask „**what made the incident possible**“

Deal with the issue at hand

Focus on fixing it first.

You cannot change what happened.

Duh.

Ask what happened and why

How could this issue have been prevented?

Which measures were not taken that should have been taken?

How can we ensure that something like this does not happen again?

Work towards a solution

Are we missing the right tools?

Are we missing education or information?

Do we require ressources?

Example

Unauthorized external access to a database

- What made this possible?
  - Some forgotten maintenance user account
- Was this preventable, and if so, how?
  - Yes, had the account been deleted
- How can we prevent this from happening again?
  - Review active user accounts on a regular basis and delete inactive accounts
- Do we lack any tooling / education / training to prevent future events like this?
  - No, issue is fixable with available ressources

So is going blameless right for you?

Maybe. Accept three simple truths:

1. This will be difficult.
2. You might fail.
3. You will still have incidents.