You are (not) prepared!

A ransomware story

2023-11-17, Elbsides light, Christian Kollee

whoami

- Detection Engineer for a German IT service provider
- Studied Computer Science at FAU Erlangen-Nuremberg
- IT Security professional for more than 10 years
- Digital Forensics & Incident Response for (mostly) small- and medium-sized businesses, hospitals, universities, and international organisations

Chapter 1
–
The Incident is identified

Introducing ACME Inc.

- ACME Inc.
  - 350 employees
  - 4 locations including a production site
- There is only one full-time administrator
  - Supported by local IT service providers
  - The production site is administered by the engineers

A typical morning?

- People already waiting at the admins desk
- Reports of unresponsive services from all parts of the company
- Screenshots of strange file endings on the file servers

ACME Inc. is victim of a Ransomware attack!

What usually happens?

- Hedless chicken mode
- Everyone is doing something
  - Not coordinated or structured
- Makes the situation worse sometimes
  - Data loss
  - Destroy Forensic evidence
- Most SMBs cannot solve this situation on their own

What should happen?

Incident Response Plan

- Prepared before an actual Incident
- At least four topics:
  - Priorities
  - Communication
  - Backups
  - Detection/Investigation Readiness

To pay or not to pay?

- Personal opinion: Don’t support criminals and do NOT pay
- However: if the only option to stay in business is to pay, pay (if you can)
  - No backups is the only reason
  - International Counter Ransomware Initiative wants to ban this

Chapter 2
–
Why Forensics is required?

Manager „discussions“

„We already know what has happend!“
- Director of ACME Inc.

- It costs money!
- It costs time! (Time = Money)
- Just fix the computers!
- Does it provide anything useful?

TL;DR: Yes, it does!

The **less precise** the forensic results, the **more conservative** the re-build.

(G DATA ADAN IR-Team)

Examples:

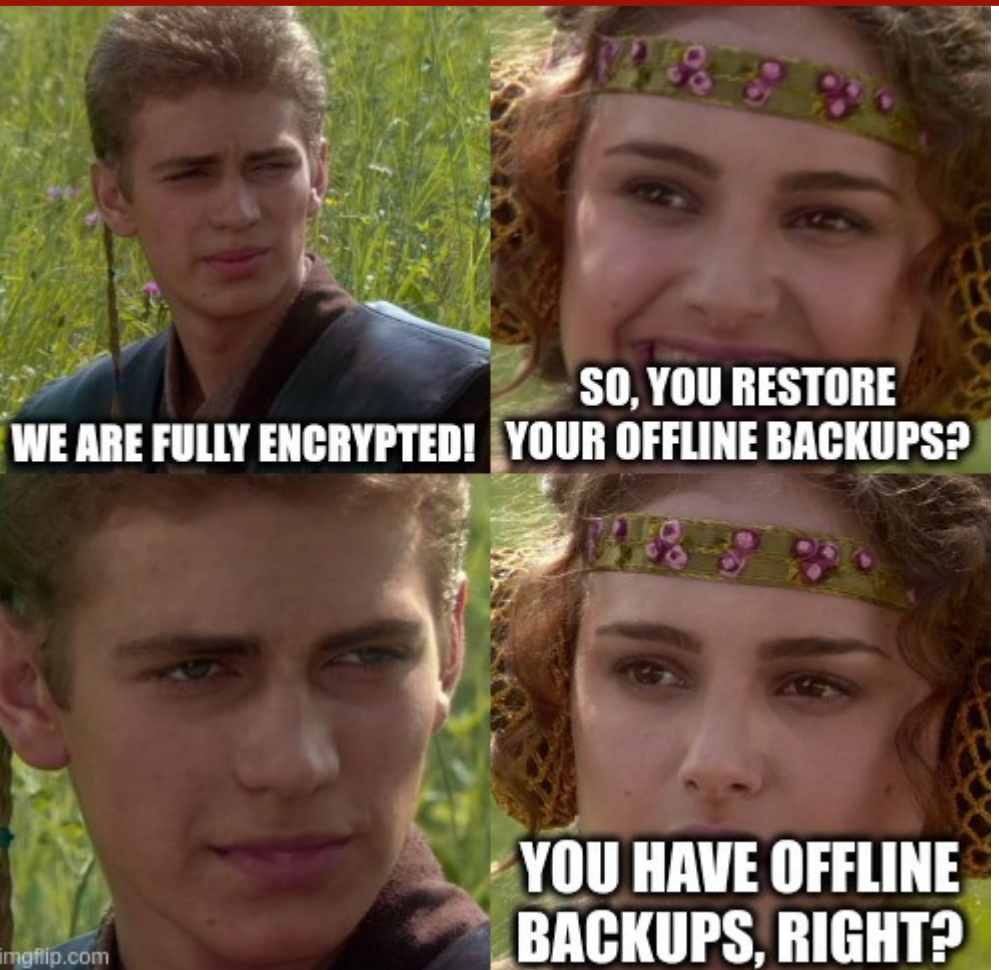
- *No* forensics → *complete* re-build
- *Full* forensics → *exact* re-build

What happend at ACME Inc.?

- Criminals exploited a Citrix vulnerability (CVE-2019-19781)
- Collected Citrix-LDAP user credentials from the appliance
- Collected domain administrator credentials from Group Policy Preferences (GPP)
- Accessed several servers using Cobalt Strike, exfiltrated data using SFTP (by installing Filezilla)
- Executing the Ransomware using an immediate task by creating a Group Policy Object (GPO)

Chapter 3
–
Recovery Pitfalls

(Offline) Backups



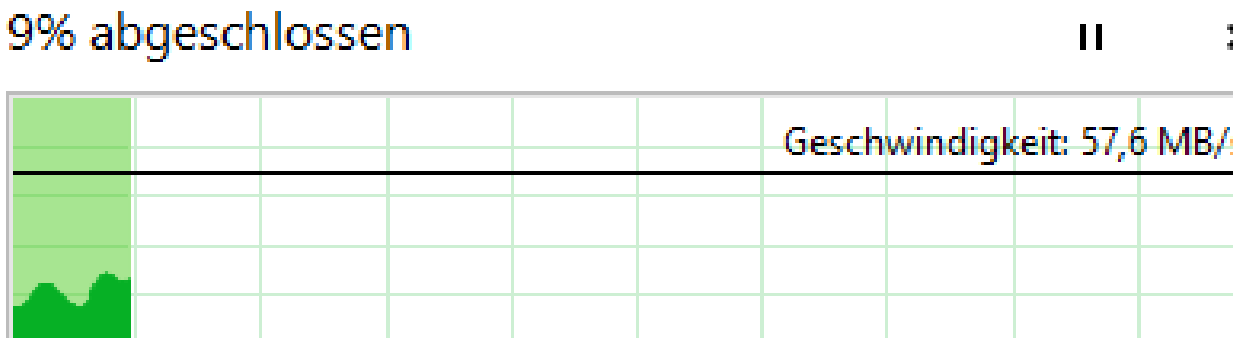
Required!

We have backups!

- Are they accessible within the network? Are they writable?
- Can we restore them?
- Are all required systems in this backup?
- If you store them encrypted, is the decryption key in a secure location?

It always takes longer than expected

- Copying large amounts of data takes time
  - HDDs are still the most used disk type
- If you copy over the Network, connection drops can interrupt the process



So, you received a decryptor

- Decryption takes time
  - Normally, decryptors are not optimized
- Decryption can fail
  - Bug in the decryptor
  - Human failure (deleted files, hard shutdown during decryption)
- Decryption requires space
  - You want a copy of your (encrypted) data

Chapter 4
–
What did we learn?

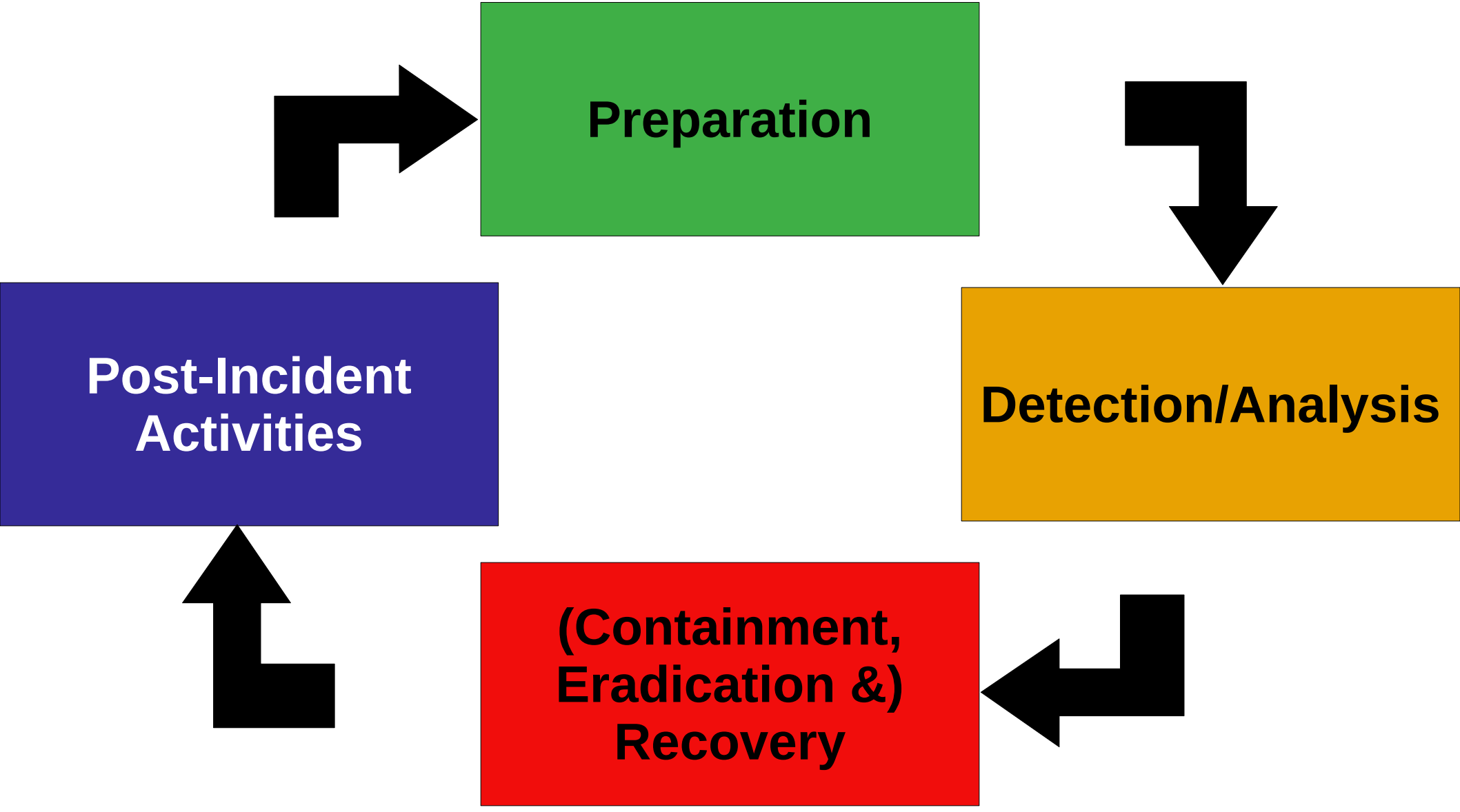
Homework

- Put services behind the VPN to reduce the attack surface
  - Use 2-Factor-Authentication
- Properly patch your systems
- Backups with regular Restore tests
- Rework Priviledged Use/Access Management
- Do proper Network Segmentation
- Monitore the (AV) logs

Epilog
–
Half a year later


GOT RANSOMWARE
38
TWICE IN HALF A YEAR
imgflip.com

Wrap-Up


Preparation
Detection/Analysis
(Containment, Eradication &) Recovery
Post-Incident Activities

Thank you for your attention!