Welcome to

6. Reporting on Incident Response

Introduction to Incident Response Elective, KEA

Henrik Kramselund he/him han/ham xhek@kea.dk @kramse

Slides are available as PDF, kramse@Github

6-Reporting-on-Incident-Response.tex in the repo security-courses

Goals for today

-
-
-

Photo by Thomas Galler on Unsplash

Plan for today

-
-
-
-
-

Exercise theme:

-
-
-

Time schedule – wednesday March 30.

This day we will be doing a larger project, get started planning incident response

- 1) Going over a few cases from Denmark – first 45min
- 2) Plan your incident response, the mission – 45 min
- Break 15min
- 3) Plan your incident response, tools – 45min
- 4) Plan your incident response, processes 45min

Times are suggested, in real life this process would take months!

Part 1: Go over a few more cases

Let's go over some of the recent cases from Denmark

You are most likely to find jobs in Denmark, and we know danish companies better

Example cases and Categories from Denmark

Start by finding a few cases from Denmark, we already talked about Maersk but feel free to re-use this data.

Cases I know are: Forsvaret (2023), Demant (2019), Ecco (2022), kommuner, infrastruktur

Try to put them in categories and find examples of each category:

- DDoS
- Data leaks – check datatilsynets perhaps
- Ransomware Demant – ransomware, but may stealing data too?
- ... more categories here, maybe use Mitre ATT&CK for inspiration

Response

- What did they do, consider advice from book

- Could they have responded differently
- What were they missing, could they learn from this
- What are some things we definitely would have *ready* for handling incidents
- What did it cost them, input for security budgets

Part 2-4) Plan your incident response

Congratulations – you are now the CISO

And we would like to A) Avoid incidents B) Resolve any incident efficiently

- Rest of today we will plan our incident response in Company XYX

Company XYX

This medium sized company with 100 employees produce a cheese cutter and sell them all over the world. They are the number one brand of cheese cutters, loved by chefs around the world.

- Turnover is in the millions
- Orders are flowing in through a web shop for customers
- Another web shop is used by B2B segment for ordering 1.000s of cheese cutters

Help them, they don't have a CISO, they don't have security people, they are afraid of security incidents – but don't know anything about them

Your Goal

There will be a management and board meeting soon, and you will present

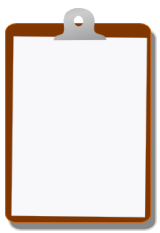
- The XYX Security Organisation
- The XYX security org mission statement
- The Basic XYX Incident Response Process
- The contact list for incident handling, feel free to add external companies
- A list of systems and tools to put in place before incidents (CMDB?)
- A list of programs, applications, tools, hardware to use for incidents (external drives and go-bag?)

Further inspiration

We have our main book, and have links to other documents, so feel free to find inspiration in:

- NIST documents SP800 series
- Awesome lists, like: https://github.com/meirwah/awesome-incident-response

For Next Time



Think about the subjects from this time, write down questions

Check the plan for chapters to read in the books

Visit web sites and download papers if needed

Retry the exercises to get more confident using the tools

Read the books! Play with tools