Exercises: Introduction to Incident Response Elective, KEA

Welcome to your new role as CISO – Chief Information Security Officer, and incident response.

Since we don't have an actual company we will use your current life and use of IT systems for these exercises.

I will reference the CIS controls. We don't need the full framework, but if you want to check it out after it is available at: https://www.cisecurity.org/controls

Exercise 1 - max 15 min

CIS Control 1: Inventory and Control of Hardware Assets

Organisations should have an overview of which hardware assets they use. Who uses them, where they are, what type it is, what is their service contracts etc.

Make a short list of your groups *hardware*

- ☐ Which phone types do you have, high level Apple, Android, others?
- ☐ Which brands of laptops do you have?
- ☐ Which other similar hardware do you have? Tablets etc.

Discuss if you think this sounds important, or registering this is a waste of time.

CIS Control 2: Inventory and Control of Software Assets

Like hardware organisations use a lot of money on software. Which kinds of software is your group dependent on in your day to day lives – include a few portals like Facebook, Instagram, Tik tok, Snapchat

- ☐ Which operating systems do you use: Windows, Mac, Linux, Chromebook, others?
- ☐ Most critical applications: text processing?
- ☐ Email programs?
- ☐ Which browsers do you use?

We know all software has errors and bugs! So we need to update these continously, but how does an organisation get an overview – using this control.

Exercise 2 - max 15 min

CIS Control 3: Continuous Vulnerability Management

- □ When was your devices last updated?
- □ Have you ever been hit by a virus or ransomware?
- □ How often should you update your computers and applications?

Discuss among yourselves, have you turned on auto-update? Why / Why not?

Exercise 3 - max 15 min

CIS Control 10: Data Recovery Capabilities

- ▢ What is a backup of data?
- ▢ Have you ever lost data, maybe a hand-in for studies or digital pictures?
- ▢ How often should one backup data?
- ▢ Is it needed to keep multiple generations of data?

Discuss what is the easiest way to do backup, learn from each other.

Incident Log

Time	Description

Financial

Time	Description	Cost
Total		

Incident

An incident happened!

We will now roll the dice!

D6 is a 6-sided dice, D12 is 12-sides.

Calculate with this table what incident it is, what it will cost your company.

Initial Access D6	Access Level D12	Cleanup Cost D6	Time line D12
1 Phishing	1 Initial Access	Simple 10.000 DKK	1 month
2 Vira/worms	2 Execution	Actual incident 50.000 DKK	2 months
3 Known CVE	3 Persistence	Medium 250.000 DKK	3 months
4 Known CVE	4 Priv esc	Large 500.000 DKK	4 months
5 0-day	5 Defense Evasion	X-Large 1.000.000 DKK	5 months
6 Unknown	6 Credential Access	Super Large 10.000.000 DKK	6 months
	7 Discovery		7 months
	8 Lateral Movement		8 months
	9 Collection		9 months
	10 Command and Control		10 months
	11 Exfiltration		11 months
	12 Impact		12 months
Total			

Mitre ATT&CK https://attack.mitre.org/ – column Initial Access is considered 1 in this game.