Kursbeskrivning Säkerhetsmedvetenhet

Version Information

ID	Date	Resp	Comment
PA2	2022	F Beste	New format

Information

Detta är en modern/uppdaterad halvdagskurs för de personer som vill få en introduktion till de säkerhetsproblem som finns inom IT-baserad verksamhet.

Kursen ger en överblick över hotbild, hotaktörer, de metoder dessa använder för att komma åt information eller skada systemen. Aktuella exempel ges på hur hoten ser ut och hur man undviker dessa.

Kursen ger också några nyttiga tips och ”*best practise*” för att höja säkerhetsmedvetenheten generellt hos alla medarbetare.

Målet med kursen är att höja medvetenhet och vaksamhet hos medarbetarna, i synnerhet de med icke-teknisk bakgrund, med målet att antalet säkerhetsincidenter minskar.

Kursinnehåll

Introduktion

- Cybersäkerhet
- Hotbilder och aktörer
- Säkerhetsbegrepp
- Bra principer för säkerhet

Hotgenomgång

- Phishing
  - Bedrägerier via mail, mm, scams
- *Malware*
  - Virus
  - Logical bomb
  - Maskar
  - Trojaner
  - Hoax
  - Keylogger, Spyware
  - Adware, spam
  - Ransomware
- Drive-by download

- Identitetskapning
- Denial-of-Service
- Man-in-the-middle attack (MITM)
- Risker med Wi-Fi (WLAN)
- Social engineering
- Flyttbar media
  - *Exempel: Social engineering + flyttbar media*
- Faror med sociala media
  - *Exempel: typiskt facebook-virus*
- Faran med att lämna ut persondata
- Insiderbrott

Fysisk säkerhet

- Clean desk policy
- Shoulder surfing
- Tailgating
- Fysisk säkerhet och omvärldskontroll

Policy och rutiner för säkerhet

- Databehandling och integritet
- Hur undviker vi phishing?
- Riskhantering med Wi-Fi (WLAN)
- Lösenord och säkerhet
  - Så snabbt knäcks dåliga lösenord
  - Hantera läckta lösenord
- Våndan med ”FB-tester” och liknande
- Säkerhet vid videokonferenser
- Säkra Internet-vanor
- Bring-your-own-device (BYOB) policy
- VPN
- Användarbeteende
- Vilka program är säkra att ladda ner?

Lagar och framtiden

- Lagar och regelverk
- Världen efter lösenord
- Framtid?
- Slutord