**Seminarie i Säkerhetstänkande:**

**Hur kan vår säkerhet utmanas?**

**Vilka delar av verksamheten kan vara hotade och på vilka sätt?**

### **Mjukvaran**

* **Databas och Backend**
  + - **Praktiska säkerhetshot från buggar eller bristande implementation**
    - **SQL-injections**
      * skydd - implementera säkra sätt att läsa in datan ( Validera och använd förberedda statements
    - **Network API-queries**
      * skydd - whitelisting
    - **Bristande Access Control**
* **Integritetshot mot användarna**
  + **(GDPR, lagstiftning för att skydda personuppgifter)**
* **DDos-attacker**
  + **Stänger ner / kraschar tjänsten genom att överbelasta nätverket med många requests**
    - skydd - lägger en timeout om det blir mer än X antal requests i minuten
* **Risker med tredjepartskomponenter**
  + **Sårbarheter i mjukvara vi integrerar**
  + **Ouppdaterad mjukvara**
  + **Uppdateringar av mjukvara**
    - skydd - skapa egna komponenter för att inte förlita sig för mycket på tredjepartskomponenter.
    - skydd - Fråga behörighet att kolla upp tredjepartskomponenter
    - En vägs kommunikations tillåtelse ex med hjälp av datadiods
* **Risker med molntjänster**
  + **Sårbarheter i tjänst vi integrerar**
* **Malware, bottar, trojaner**
  + - skydd - Anlita externa tjänster för att testa gränssnittet.
* **Klienten: Gränssnittet, nätverkslagret (API) är Attackvektor nr 1**
  + **User Input:** 
    - **Inputfält**
    - **URL-fältet**
    - **Network API-queries**
  + **Osäkra cookies**
  + **Local Storage**
* **Man in the middle-attack (t ex Wireshark)**
  + **Föråldrade säkerhetsprotokoll som exponerar sessions**
  + **Session hijacking (använda andras konton)**
* **XSS - Cross Site Scripting**
  + **När din klient läser filer från tredje part, har du ingen kontroll över att det som läses in inte kan exekvera kod (t ex kod som kan använda dina autentiserade resurser)**
  + **Cross Domain Scripting**
    - **Defense: CORS restriction**

### **Användarna**

* **Osäkra lösenord**
  + skydd - komplicerar processen i val av lösenord bl a måste innehålla tecken, siffra och stor bokstav
  + skydd - Dela inte ut lösenordet
* **Oförsiktiga med länkar / lägger upp farliga länkar**
  + skydd - Utbilda / meddela användare hur de bör agera.
  + skydd - Kolla länk namnet, avsändaren etc.
* **Social engineering**
  + skydd - Inte vara en liten bitch och låta folk manipulera en…
  + skydd - Låst arbetsmiljö, vakt in till byggnad / arbetsplatsen.
  + skydd - skeptisk till obehöriga / personer som inte är anställda på företaget.

### **Utvecklarna**

* **Egen bristande säkerhet kan äventyra mjukvarans integritet**
  + **Att vara oförsiktig med inkommande fishing attempts (mail, telefon, etc)**
  + **Bristande egen mjukvara (Keyloggers, Spyware)**
* **Bristande kvalitetskontroll (testning, m m)**

### **Annan infrastruktur**

* **RFID / nfc / wireless chip hacking (flipperzero)**
* **WiFi hacking**
* **Bluetooth hacking**
* **USB-minnen**