Seminarium i Säkerhetstänkande:

Hur kan vår säkerhet utmanas?

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

### Allmänt

Skydd:

* Använda externa säkerthetsexperter / tjänster för att skydda oss

### Mjukvaran

Skydd:

* Allmänt är det säkrare att använda etablerade, stora lösningar, eftersom de är hårt säkerhetsutsatta och därmed hårt säkrade. Samtidigt blir exploits snabbt kända.
* Tillämpa aktiv säkerhetstestning.
* Databas och Backend
  + Praktiska säkerhetshot från buggar eller bristande implementation
  + SQL-injections
  + Network API-queries
    - Skydd
      * Snål ordentlig ACL
      * Undvika att skicka med data som kan utnyttjas
      * Undvik i så fall också att exponera input för sådan data
  + 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
* Risker med tredjepartskomponenter
  + Sårbarheter i mjukvara vi integrerar
  + Ouppdaterad mjukvara
  + Uppdateringar av mjukvara
* Risker med molntjänster
  + Sårbarheter i tjänst vi integrerar
* Malware, bottar, trojaner
* 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
    - Skydd: CORS restriction
* Skydd av toolchains (publicering, serverdrift)
  + Strategier mot detta kallas för DevSecOps

### Användarna

* Osäker autentisering (lösenord)
  + Skydd:
    - Multipartsautentisering
    - BankID m fl
    - “Säkra lösenord”
      * Password generators
      * Password vaults / hanterare (one password, google, keychain, etc)
      * Olika lösenord på olika ställen
      * Inte använda personliga lösenord
      * Lösenord du lätt kommer ihåg
      * Att inte använda lösenord (biometrics)
    - Rutin att uppmana användare att byta lösenord (samt efter läcka)
    - Flood control (låsa ute användaren efter för många försök)
      * blackholing (ta emot en request (redirected) utan att svara, gärna med lång timeout)
    - T ex BCrypt mot Rainbow table attacks (brute force lösenordsattacker)
* Exponering för virus / spyware / keyloggers via både hårdvara och mjukvara
* Oförsiktiga med länkar / lägger upp farliga länkar
* Social engineering

### Utvecklarna

Allmänt skydd: Utbilda utvecklare och organisation löpande inom säkerhet.

* 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