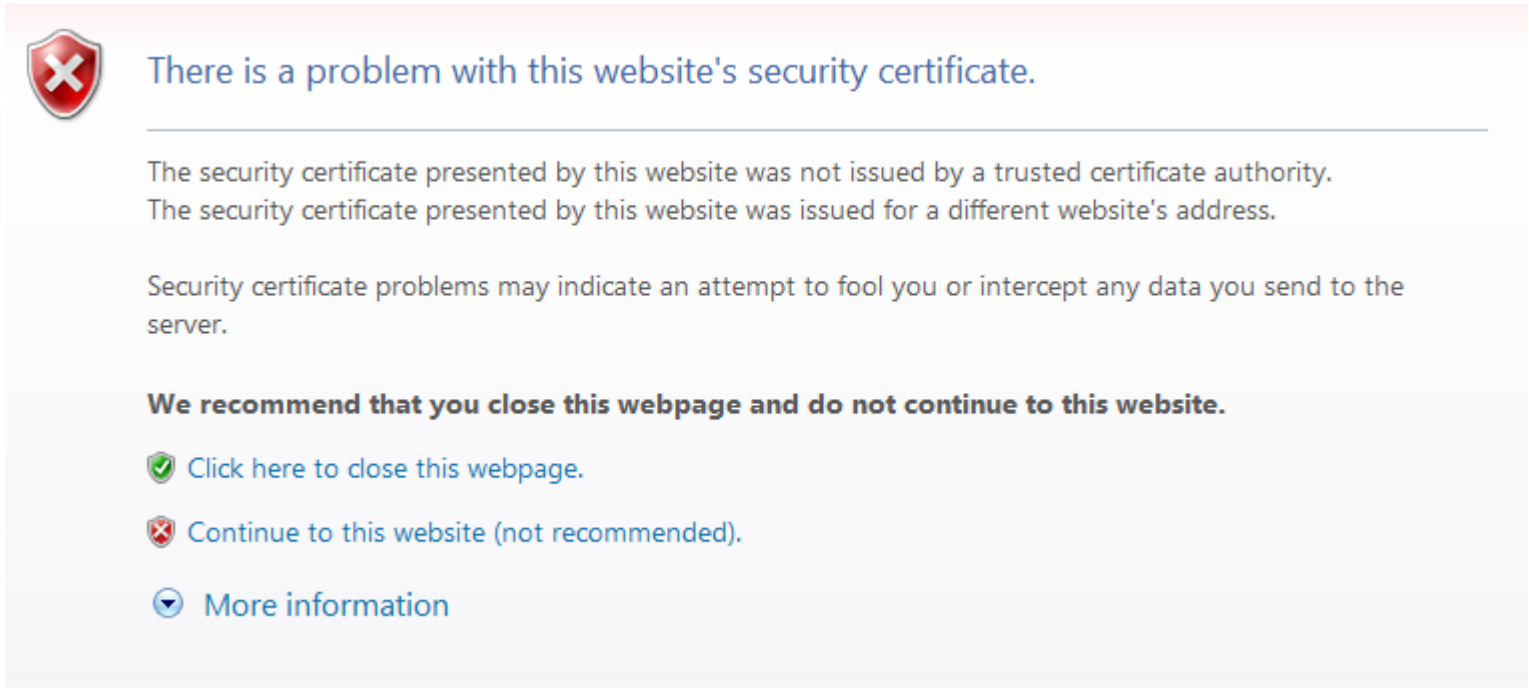
Tietoturva ja modernit verkkopalvelut

Kysymyksiä

- Käyttääkö joku avointa nettiä junassa, verkkokahviloissa tai esim. kampuksella?
- Oletko koskaan ohittanut web-sivulla sertifikaattivahvistusruutua?
- Käyttääkö joku samaa salasanaa useammassa kuin yhdessä palvelussa?
- Foorumien / WoW-killan sivuston / Web-ylläpitäjiä?

ANDERSINNO

Mikä on oikea tapa jatkaa tästä?



ANDERSINNO

Missä tietoturvalla on väliä?

- Verkkopankit
- Sähköposti
  - Kaikki salasanat tulevat ennemmin tai myöhemmin sähköpostiin
- Maksaminen verkossa
  - Luottokorttitiedot yms.

ANDERSINNO

Missä tietoturvalla on väliä?

- Mutta **myös** esimerkiksi:
- Uutissivustot
  - Virheellisen tiedon ujuttaminen luotettuun uutispalveluun.
  - esim. "Nokian kurssille odotettavissa raju nousu! Analyytikot suosittelevat ostamaan!"
- Hakukoneet
  - Hakutulosten järjestäminen tai jopa tiedon piilottaminen kokonaan.

ANDERSINNO

Loppukäyttäjän tapoja suojautua

- Java ja muut turhat lisäkkeet pois päältä selaimissa
- Käyttöjärjestelmän ja selaimen tietoturvapäivitykset asennettuina
- Virustorjunta ja palomuuri toiminnassa
- Salasanahygienia
  - Varaudu siihen, että palveluntarjoaja ei välttämättä huolehdi salasanasi turvallisuudesta.
- Maalaisjärki/terve vainoharhaisuus on sallittua
  - "Varsinais-Suomen salasanavirastosta, päivää!"
- Käytä HTTPS:ää aina kun mahdollista
- Jokaiselle hauskalle Facebook-pelille ei ole pakko antaa tietojaan

ANDERSINNO

Järjestelmän omistajan tapoja suojautua

- Varmista, että järjestelmän toimittaja/ylläpitäjä huolehtii alustapäivityksistä
  - Käyttöjärjestelmä
  - Tietokantamoottori
  - Sovelluskehykset (Django, Ruby on Rails yms.)
  - Kolmansien osapuolien ohjelmat ja kirjastot, yms.
- Toteuta järjestelmä alusta asti modernein työkaluin
- Minimoi hyökkäyspinta-ala
  - tarpeettomat palvelut pois netistä/palomuuratuksi

ANDERSINNO

Sovelluskehittäjän tapoja suojautua

- Tunne yleisimmät haavoittuvuudet (OWASP Top 10)
  - A1: Injection
  - A2: Cross-Site Scripting (XSS)
  - A3: Broken Authentication and Session Management
  - A4: Insecure Direct Object References
  - A5: Cross-Site Request Forgery (CSRF)
  - A6: Security Misconfiguration
  - A7: Insecure Cryptographic Storage
  - A8: Failure to Restrict URL Access
  - A9: Insufficient Transport Layer Protection
  - A10: Unvalidated Redirects and Forwards

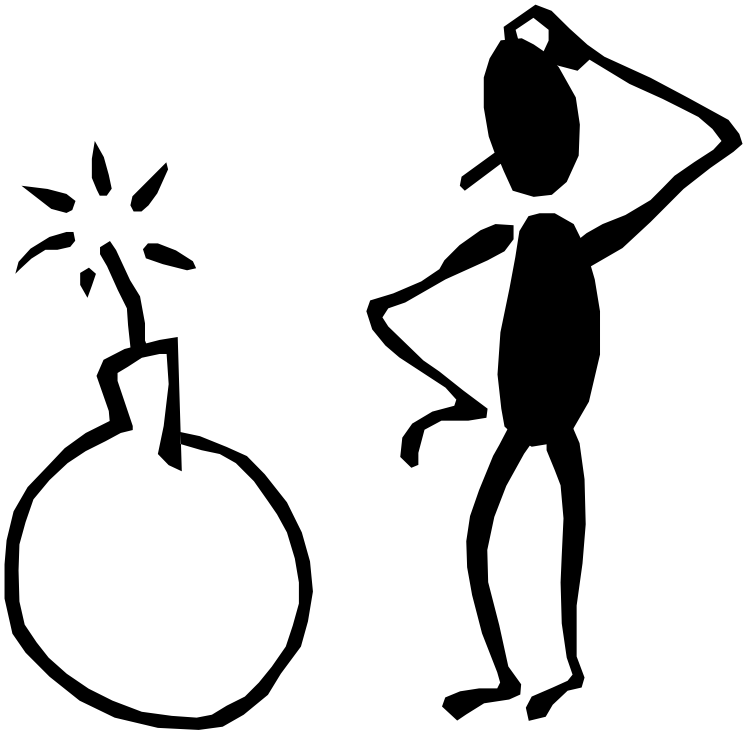
ANDERSINNO

Sovelluskehittäjän tapoja suojautua

- Älä tee turvallisuuskriittistä koodia itse
  - Kryptografia on vaikeaa!
  - Siinä on helppo epäonnistua, vaikka olisi isokin firma. (Esimerkiksi Microsoftin ASP.NET-haavoittuvuudet)
- Varautuminen palvelunestohyökkäyksiin
  - Oikein konfiguroitu palomuuri
  - Kuormantasaus
  - Pyyntöjen tiheyden rajoitus yms.

Suurin uhka on kuitenkin ihminen

- Huolimatta kaikista teknisistä keinoista suurin riskitekijä on kuitenkin ihmisen tekemät inhimilliset virheet
  - Unohtuneet päivitykset
  - Salasanat helposti katoavilla Post-it-lapuilla
  - Jne.



ANDERSINNO

Kysymyksiä?

ANDERSINNO

Kiitos!

http://andersinno.fi