Matti Vuori

Noin 30 tapaa joilla käytettävyysihmiset voivat parantaa järjestelmän tietoturvallisuutta

Tietoturvallisuus on kaikkien järjestelmien kehittämiseen, tuotantoon ja ylläpitoon osallistuvien yhteinen asia. Käytettävyysihmisillä on oma roolinsa, mutta heille tuntuu olevan jäsentymätöntä, mitä kaikkea heidän pitäisi ja he voisivat tehdä asian eteen. Hyvä uutinen on se, että monessa tapauksessa samat asiat tukevat sekä käytettävyyttä että tietoturvallisuutta! Tässä tekstissä on aluksi muutama kymmenen ajatusta asiasta, mutta en pyri esittämään kattavaa listaa, vaan vasta hieman alustusta aiheeseen.

Sisällysluettelo

Huom! Tässä tekstissä ”käytettävyysihmiset” määritetään sumealla logiikalla ja niitä ovat käytettävyysasiantuntijoiden lisäksi esimerkiksi konseptisuunnittelijat ja käyttöliittymäsuunnittelijat.

Selvitä, mikä tieto on tärkeää ja pitää suojata

1. Käytettävyysihmiset ovat ”antropologeja” ja osaavat jäsentää, mitkä tiedot ovat käyttäjille tärkeämpia kuin toiset – niin tiedetään, mitä tietoja käsitellään ja liikutellaan eniten ja ennenkaikkea: mitä pitää suojata.
2. Tietoturvallisuus on aina jossain ihmisten kontekstissa ja käytettävyysihmisillä on eväitä sen selvittämiseen ja kuvaamiseen.

Auta tietosisältöjen kohtuullistamisessa uhkien vähentämiseksi

3. Mitä vähemmän järjestelmässä on tietoa, sitä vähemmän se kiinnostaa muita ihmisiä ja sitä vähemmän se herättää huomiota hauissa. Konseptisuunnittelussa käytettävyysihmiset miettivät käyttäjiltä kaivamiensa tietojen perusteella tarkkaan, mitä järjestelmässä tarvitaan ja jätetään muut pois.

Viesti uhat käyttäjille

4. Uhkien viestiminen käyttäjille selväkielisesti. Tietoturvaviestintää tehdään usein enemmän ajatellen palveluntarjoajan vastuita kuin käyttäjää. Kuitenkin, käyttäjien on yhä enemmän oltava tietoisia tietoriskeistä ja omien toimiensa vaikutuksesta tietoturvallisuudelle. Siinä, että tämä viestintä saadaan perille, tarvitaan käytettävyysihmisten vahvaa panostusta.
5. Käyttöliittymä on järjestelmän kasvot ja on varmistettava, että tietoturvallisuuden ja tietoriskien kulloinenkin taso heijastuu käyttöliittymässä – vaikka markkinointi ei olisikaan asioista aina samaa mieltä.

Mahdollista tietojen näkyvyyden helppo ja turvallinen hallinta

6. Esimerkiksi yhteisöllisissä palveluissa käyttäjän on määritettävä, mitä tietoja itsestään näyttää. Käytettävyysihmisten on varmistettava, että tämä on ymmärrettävää ja helppoa… ja tilanne on koko ajan selvillä.
7. Näkyvyystiedot on oltava helposti auditoitavissa. Eli käyttäjän pitää saada tietojen näkyvyydestä listaus, jota voi miettiä rauhassa.
8. Tällaisissa konfiguraationäytöissä on esitettävä selkeästi jokaiseen tietoon liittyvät mahdolliset uhat ja käyttäjän konfigurointia tukevat faktat.

Anna tukea turvalliselle viestinnälle

9. Käytettävyysihmiset ovat hyvän viestinnän tuntijoita ja pystyvät varmistamaan, että järjestelmän viestintä perustuu turvallisiin käytäntöihin – esimerkiksi kaikki järjestelmien automaattiset sähköpostiviestit.
10. Kokonaispalvelun käytettävyys. Käytettävyysihmisten huomio ei saa jäädä teknisen järjestelmän viesteihin, vaan on katettava myös esimerkiksi markkinoinnin toiminta. Esimerkiksi pankeilla on usein päätös, että palveluun liittyviä sähköpostiviestejä ei lähetetä. Mutta vaikka palvelua pyörittävä henkilökunta muistaa tämän, markkinointi voi tuhota hyvän periaatepohjan ja opettaa käyttäjät alttiiksi phishingille yms. lähettämillään sähköpostiviesteillä.
11. Turvallinen viestintä on joskus kankeaa, jos järjestelmää ei ole suunniteltu hyvin. Esimerkiksi käsin kirjoitettavien linkkien käyttö on hankalaa ja sitä ei tehdä, jos linkit ovat pitkiä kryptisiä

Hyvä viesti menee perille, huono ajatuu roskakoriin

12. Järjestelmät eivät ole käytettävissä, jos niitä koskeva tieto ei mene perille -- esimerkiksi kryptinen varmistus-sähköposti joutuu roskalaatikkoon, koska näyttää spämmiltä. Käytettävyysihmiset voivat varmistaa viestien laadun.

Minimoi tietoturvaratkaisujen haitta arkiselle toiminnalle

13. Varmistetaan, että esimerkiksi salasanan kysymisessä ei liioitella. Jos sitä joutuu naputtelemaan koko ajan, käyttäjät hermostuvat (ja lisääntyy riski sille, että mukaan mahtuu vakoojaohjelmien luvattomia salasanakysymyksiä!)
14. Timeoutien iskeminen kesken lomakkeen syöttyä on klassinen ongelma. Käytettävyysihmisten on tarkistettava tällaiset kommervenkit.
15. Perinteinen este tietojen saatavuudelle on se, että salasanan vaihtotarpeesta ei tule ennakko-varoitusta ja tunnuksella ei enää pääsekään sisään. Käytettävyysihmisten on otettava elinkaariajattelussaan kaikki aikaan liittyvät ilmiöt huomioon.

Tue järjestelmän tilan näkemistä

16. Jo käytettävyyssyistä käyttäjällä pitää olla sopiva näkymä järjestelmän tilaan. Sen arviointi on normaalia käytettävyystyötä. Tietoturvallisuuden näkökulmasta on näyttävä esimerkiksi sisäänkirjautumisen status ja mihin liittyviä tietoja yms. on ladattuna ja käsittelyssä.
17. Tiedonkäsittelyprosessin eheyden näkökulmasta on varmistuttava siitä, että tietoon tehdyt muutokset tapahtuvat ja tallentuvat suunnitellusti. Kaiken prosessiin liittyvän tiedon sopivantasoinen esittäminen ja palaute käyttäjien toimille on tarkistettava.
18. Useat tiedon duplikaattiongelmat (kaksi tilausta, kaksi laskua jne…) syntyvät siitä, että niitä vastaavia käyttötehtäviä ei ole estetty tai käyttäjä ei pysty näkemään järjestelmän tilasta, että yksi pyyntö on jo prosessoitavana. Käytettävyysihmisten on kokeiltava kaikki tällaiset.

Estä väärän tiedon käyttö

19. Vääriä tietoja käytetään ja vääriä ohjelmia asennetaan jne., koska ladattavia tiedostoja ei yksilöidä, vaan käyttäjälle tarjotaan pahimmillaan kryptinen merkkijono tiedostonimenä tai ohjelmistopaketti, jonka versionumeron saa selville vasta sitä asentaessaan. Tällaisen saaminen kiinni on triviaali asia.
20. Tietojärjestelmissä linkitetään helposti vääriä tietoja ihan niin triviaalista syystä, että elementtien nimet eivät näy kokonaan kentissä tai koodit ovat liian samankaltaisia. Näiden asioiden perkaaminen on käytettävyystyön arkea.
21. Joskus tietoja kopioidaan tietojärjestelmiin, koska originaalidokumentin käyttö systeemin osana on liian kankeaa tai epäesteettistä. On poistettava tällaiset alkuperäisen tiedon käytön esteet.
22. Tietoihin liittyy aina metatietoa sen omistajasta, luottamuksellisuudesta. Näiden esittäminen on varmistettava ja tarkastettava käyttöliittymiä analysoitaessa – puutteet eivät nouse käyttäjien valituksina käytettävyystestauksessa, joten analyyttinen ongelmatilanteiden ennakointi on käytettävyysihmisen tärkein strategia. On oleellista vähintäänkin varmistaa, että kun on tietoon liittyviä kysymyksiä, käyttäjälle on heti selvää, mistä ja miten asiaa kysytään.

Arvioi järjestelmän ohjeet ja varoitukset

23. Hyvä järjestelmä ei tarvitse ohjeita… mutta joskus niitä tarvitaan ja varsinkin poikkeustilanteissa, jolloin tiedotkin ovat vaarassa. Käytettävyysihmisten panos ohjeiden ja varoitusten kehittämisessä ja niiden arvioimisessa on oleellista.

Arvioi käyttäjän tunnistamisen käytettävyys

24. Helppous tuottaa varmuutta. Sisäänkirjautuminen eri tavoilla ja sen sujuvuus ovat testattavia asioita.
25. Jos käytetään biometristä tunnistusta, sen epävarmuuden vuoksi on aina tarkistettava ”perinteisen tavan” olemassaolo. Biometrisen tunnistuksen toimivuus käyttöolosuhteissa on testattava – tunnistus voidaan kytkeä pois päältä, jos se on liian epäluotettava.

Muista pääkäyttäjän ja ylläpidon käyttöliittymät

26. Lähes kaikki webbijärjestelmät tuottavat seurantatietoa, logeja tms. Ylläpidon käyttöliittymät suunnitellaan yleensä puutteellisesti ja niiden käytettävyyden arviointiin ja testaukseen ei riitä aina rahaa. Mutta niiden laadun pitää olla hyvä, jotta esimerkiksi logeihin kertyvät tiedot mahdollisesta riskialttiista tai luvattomasta toiminnasta saadaan tuottamaan toimenpiteitä.

Testaa poikkeustilanteita ilmiöiden nostamiseksi esille

27. Aina, kun tilanteissa on häiriöitä, poikkeamia tai muita ongelmia, nousee esille uudenlaisia ilmiöitä. Tämä pätee käytettävyyden analysointiin ja testaukseen. Siinä kannattaa käsitellä kaikenlaisia normaalien työnkulkujen poikkeuksia niin paljon kuin mahdollista. Näin saadaan toiminta ja järjestelmät robusteiksi sekä käytettävyyden että tietoturvallisuuden näkökulmasta.

Minimoi inhimilliset virheet

28. Inhimillisten virheiden systemaattinen analysointi omana aktiviteettinaan erillään muusta käytettävyyden tarkastelusta on joskus paikallaan. Teollisuudessa tätä on tehty pitkään, miksei siis muuallakin.
29. Samoin systemaattinen järjestelmän väärinkäyttömahdollisuuksien tunnistaminen. ”Tavallisille” tuotteille niiden miettiminen on edellytys vaatimustenmukaisuudelle ja CE-merkille.
30. Liian suuret tietomassat ja monimutkaiset käyttöliittymät ovat tyypillinen resepti väärien tietojen syöttämiseen… ja käyttämiseen seuraavassa vaiheessa. Jos työ edellyttää viiden lomakkeen täyttämistä, taktiikka on usein vain kokeilla, meneekö tallennus läpi, olipa syötettynä puutaheinää tai sattumalla jotain relevanttia… Tällaisten tilanteiden tunnistaminen on käytettävyysihmisten arkea.

Laadukasta järjestelmää kohdellaan paremmin

31. Jos järjestelmän laatu ei vastaa käyttäjien odotuksia, sitä ei myöskään kohdella hyvin. Se on vähän kuin 20 vuotta… ruosteinen auto. Mutta kun järjestelmä on hyvin suunniteltu ja toteutettu, sitä kohdellaan paremmin, mikä heijastuu myös järjestelmään syötettäviin tietoihin ja kaikkeen työn laatuun.

Tee tiimityötä

32. Ennenkaikkea käytettävyysihmisten on oltava kokonaisvaltaisia tiimipelureita otettava tämäkin teema sopivasti omakseen. Missään nimessä ei saa ajatella, että se on joidenkin toisten asia.

Osallistu organisaation tietoturvapolitiikan ja ohjeiden kehittämiseen

33. Käytettävyysihmisten on hyvä osallistua tietoturvallisuuden hallintajärjestelmän kehittämiseen, koska heillä on käytännön ymmärrystä erilaisten toimenpiteiden sopivuudesta ihmisten maailmaan – ja keinoja selvittää asioita vaikkapa järjestämällä testi! Samoin heillä on kykyä arvioida ohjeiden ja tietoturvaviestinnän toimivuutta. Esimerkki: organisaatioilla saattaa olla epärealistisia sääntöjä vaikkapa etätöiden järjestelyihin. Tällöin niitä ei noudateta, mikä murentaa koko tietoturvakulttuuria. Käytettävyysihmisten orientaatio mahdollistaa tällaisten tunnistamisen (sama pätee toki, mutta eri muodossa myös ns. ”tavallisiin käyttäjiin”).
34. Näytä mallia! Kun käytettävyysihmiset käsittelevät ja jakavat omaa tietoaan, heidän on hyvä olla esimerkki siitä, miten tietoturvallisuus ja käytettävyys toimivat sopusoinnussa, kumpikin organisaation tavoitteita tukien.

Lopuksi…

35. Olemalla avoin näiden asioiden suhteen autat itseäsi kehittymään koko ajan osaavammaksi ja joustavammaksi ammattilaiseksi.