Salasanat haltuun

Neuvoja salasanojen käyttöön ja hallintaan

Viestintävirasto
Kyberturvallisuuskeskus

Sisällys

Salasanat haltuun - Neuvoja salasanojen käyttöön ja hallintaan

Nykyään käyttäjätunnusta ja salasanaa tarvitaan opiskellessa, työelämässä ja vapaa-ajalla. Tunnuksia on käytettävä ja muistettava yhä enemmän, siksi jokaisen on hyvä tietää salasanojen turvallisen käytön yleiset periaatteet.

Salasanoja käytetään joko yksin tai osana käyttäjän todentamista, kun tarkistetaan käyttöoikeuksia eri palveluihin tai järjestelmiin kirjauduttaessa. Erityisesti verkon yli käytettävissä julkisissa palveluissa salasanan käyttö on suosittua, koska se on tunnettu ja helppokäyttöinen todentamismenetelmä.

Tässä julkaisussa kerrotaan salasanojen turvallisesta käytöstä erityisesti käyttäjien näkökulmasta. Myös ylläpidon vaikutusmahdollisuudet salasanojen hyvään hallintaan on huomioitu.

1 Salasanalla todennetaan käyttäjät

Usein verkkopalveluissa ja tietojärjestelmissä on oltava ominaisuudet, joiden avulla valvotaan ja rajataan, kenellä on oikeus päästä käsiksi palvelun tietoihin tai muuttaa palvelun tietoja. Tällöin palvelussa on oltava menetelmä, jolla palvelun tai järjestelmän käyttäjiä *tunnistetaan* ja *todennetaan*.

Käyttäjätunnus ja salasana on yleisesti käytössä oleva tunnistamis- ja todentamismenetelmänä, joilla suojataan tietoja ja rajataan pääsyä eri tietojärjestelmiin.

Käyttäjätunnusta voidaan pitää julkisena tietona, joka on vähintään kohtuullisella vaivalla arvattavissa tai selvitettävissä. Käyttäjätunnuksena käytetään usein esimerkiksi sähköpostiosoitetta.

Salasana on salassa pidettävä tieto, jonka tarkoitus on estää käyttäjätunnuksen luvaton käyttö.

Tunnistamis- ja todentamismenettely valitaan sen perusteella, kuinka arvokkaaksi suojattava tieto arvioidaan.

1.1 Vahva tunnistaminen

Käyttäjän *vahvalla tunnistamisella* tarkoitetaan henkilön yksilöimistä ja tunnisteen aitouden ja oikeellisuuden *todentamista.* Se perustuu vähintään kahteen seuraavista vaihtoehdosta:

1. käyttäjän oma tieto (esimerkiksi salasana)
2. käyttäjän hallussa oleva tieto (esimerkiksi sirukortti tai kertakäyttöiset PIN-koodit)
3. käyttäjän oma biometrinen ominaisuus (esimerkiksi sormenjälki tai iiris).

Käyttäjätunnistusta ja -todennusta tukevana menetelmänä voidaan myös käyttää esimerkiksi käyttäjän loogista sijaintia (IP-osoite).

1.2 Heikko käyttäjätunnistaminen

Kun käyttäjä tunnistetaan ja todennetaan vain yhdellä menettelytavalla, vaikkapa käyttäjätunnuksella ja salasanalla, kyse on *heikosta käyttäjätunnistuksesta*.

Käyttäjätunnus-salasana-paria käytetään lukuisissa kuluttajille suunnatuissa verkkopalveluissa. Pari on käytössä myös esimerkiksi kuluttajien kotitietokoneissa tai oppilaitosten tarjoamissa tietotekniikkapalveluissa, jot-

ka ovat matalampaa suojaustasoa edellyttäviä järjestelmiä.

Käyttäjätunnus-salasana-parin vahvuuksia ja heikkouksia muihin tunnistus- ja todennusmenetelmiin verrattuna käsitellään yksityiskohtaisemmin luvussa 5.

2 Laadukkaan salasanan perusteet

Salasanan laatu vaikuttaa palvelun tietoturvaan, jos järjestelmään ei sisälly muuta todentamismenetelmää. Laadulla tarkoitetaan sitä, ettei sivullinen kykene arvaamaan tai selvittämään salasanaa, vaikka hänellä olisi henkilökohtaisia tietoja käyttäjästä, salasanan laskennallinen tiiviste tai tietoteknisiä apuvälineitä kuten salasanojen murtamiseen tarkoitettuja ohjelmia.

Tyypillisesti käyttäjä voi valita salasanansa melko vapaasti. Käyttäjä voi itse vaikuttaa niin salasanansa kuin myös palvelunsa turvallisuuteen. Lisäksi järjestelmään voidaan asettaa salasanan pituutta ja merkkivalikoimaa koskevia vaatimuksia, joilla lisätään palvelun turvallisuutta. Joihinkin verkkopalveluihin rekisteröidyttäessä järjestelmä luo käyttäjälle tilapäiseksi tarkoitetun salasanan. Se kannattaa vaihtaa omavalintaiseen salasanaan heti palveluun ensikirjautumisen aikana.

2.1 8 merkkiä ei riitä

Pituus varjelee salasanaa sekä sosiaalisilta että teknisiltä huijauksilta seuraavasti:

- Salasanan arvaaminen ja toistaminen on vaikeaa, vaikka hallussa olisi käyttäjän henkilökohtaisia tietoja tai salasanan syöttämisen näkisi.
- Tekninen selvittäminen laskennallisesti on hankalaa, vaikka salasanasta laskettu tiiviste olisi joutunut vääriin käsiin, esimerkiksi tietomurron vuoksi.

Mikä sitten on riittävän pitkä? Salasanoja voidaan murtaa yhä nopeammin tietokoneiden ja muistivälineiden nopeutuessa ja laskentakapasiteetin lisääntyessä. On olemassa taulukoita, joihin on laskettu valmiiksi eri salasanoista muodostuvia tiivisteitä. Esimerkiksi jos on käytössä tiiviste, voidaan selvittää kaikkien 8-merkkiset ja lyhyemmät salasanavaihtoehdot hyvin helposti ja nopeasti.

Hyvä lähtökohta salasanan pituudeksi on **15 merkkiä**. Lähes kaikki nykyaikaiset järjestelmät ja palvelut hyväksyvät 15-merkkisen salasanan. Salasanojen tiivisteen tallennukseen voidaan järjestelmissä käyttää useita menetelmiä. Tallennusmenetelmä on todennäköisesti tuoreempi ja turvallisempi, jos tallennettava salasana on vähintään 15 merkkiä pitkä. Vanhat ja turvattommat menetelmät soveltuvat lyhyempienkin salasanojen tallentamiseen.

Pitempi salasana on aina hyväksi, jos järjestelmä sen vain hyväksyy. Toki sen muistaminen ja kirjoittaminen on hiukan vaikeaa. Salasanojen sijaan tulisikin käyttää salalauseita.

2.2 Salalause on salasanaa turvallisempi

Yksi salasanojen murtamismenetelmä on sanakirjahyökkäys, jossa salasanan arvailuun käytetään valmiita sanaluetteloita. Jos käytetty salasana löytyy sanaluettelosta, se murtuu lähes välittömästi. Kahden tai useamman sanan yhdistäminen hidastaa paljastumista vain vähän. Myös ominaisuus, jolla kirjaimia korvataan numerovastineilla (i =1, o = 0 jne.), on automatisoitu salasanojen murto-ohjelmiin, jolloin hidastava vaikutus lasketaan sekunneissa, korkeintaan minuuteissa.

Sanakirjasta löytymättömän salasanan voi muodostaa vaikkapa poimimalla sanojen alkukirjaimet pitkästä, mutta helposti muistettavasta lauseesta.

Esimerkiksi:

> *"Joulupukki tulee meillä jo jouluaaton iltana, mutta muualla maailmassa usein vasta joulukuun 25. päivän vastaisena yönä!"*

tuottaa kohtalaisen hyvän salasanan:

> *"Jtmjjimmmuvj25vy!".*

Salasanana voi käyttää myös kokonaista lausetta, jonka ei tarvitse olla järkevä, kunhan sen itse muistaa. Esimerkiksi matkalippujen verkkopalveluun voisi toimia salalause:

> *Bussilla matkustaa 2 mustaa kissaa ja 3 valkoista koiraa, eli yhteensä 5 eläintä.*

Kaikki järjestelmät eivät välttämättä hyväksy välilyöntejä. Tällöin lauseen voi kirjoittaa esimerkiksi "yhteen putkeen" tai vaikkapa yhdistää lauseenosat toisiinsa erikoismerkein ("Bussilla_matkustaa#2#mustaa_kissaa..").

2.3 Merkeillä on väliä

Kun salasanassa on käytetty useita eri merkkejä, sen murtaminen on vaikeampaa. Usein vaaditaankin, että salasanassa on isoja ja pieniä kirjaimia, numeroita sekä erikoismerkkejä. Numeroista ei kannata käyttää vain ilmeisiä korvaavuuksia (i=1, o=0), koska ne ovat helposti selvitettävissä. Monimerkkisyyden lisäksi on silti muistettava, että salasanan on oltava tarpeeksi pitkä.

2.4 Apuohjelmien avulla voi luoda ja säilöä salasanoja

Jos omat ideat loppuvat, salasanoja voi muodostaa myös apuohjelmilla. Ohjelmilla voi luoda satunnaisilta vaikuttavia, *pseudosatunnaisia,* salasanoja tai sellaisia kokonaisuuksia, jotka ovat helpommin lausuttavia ja muistettavia. Apuohjelmista on hyötyä myös monimutkaisten salasanojen muodostamisessa. Samaa ohjelmaa on mahdollista hyödyntää salasanojen säilömisessäkin. Näin kaikkia salasanoja ei tarvitse muistaa ulkoa - kunhan ei unohda apuohjelman salasanaa.

2.5 "salasana" ei ole hyvä salasana

Salasanamurtajat kokeilevat ensimmäiseksi "laiskanhelppoja" salasanoja. Näitä ovat esimerkiksi "salasana", "salasana123" tai etunimi "Ellinoora". Vältä myös näppäimistöllä muodostettavia geometrisia kuvioita. Niitä murtajat kokeilevat ensimmäiseksi. Syntymäajat ja henkilötunnukset ovat nekin kelvottomia, myös salasanojen osina.

Muistilista salasanojen muodostukseen:

1. **Riittävän pitkä: Suositellaan vähintään 15 merkkiä**
2. **Salasana ei ole sana: Käytä lausetta tai lyhennettä lorusta**
3. **Merkeillä on väliä: Numerot, kirjainten koot ja erikoismerkit käyttöön**
4. **Käytettävissä on apuohjelmia**
5. **Älä käytä: Yleisiä salasanoja, henkilökohtaisia tietoja tai näppäimistön geometrisia kuvioita**

3 Apuvälineitä salasanaviidakkoon

Nykyihmisen on muistettava lukuisia salasanoja, joita on keksittävä eri palveluihin ja myös vaihdettava säännöllisesti. Muistamisen helpottamiseksi salasanojen hallintaan on olemassa useita tukikeinoja ja teknisiä apuvälineitä.

Käytä seuraavia keinoja, jos kaikkien salasanojen muistaminen käy työlääksi:

- Kirjoita salasana muistilapulle joko kokonaan tai osittain. Säilytä lappu turvallisessa paikassa. Kirjaa tieto niin, ettei siitä ulkopuoliselle selviä, minkä palvelun tai kenen salasanasta on kyse, jos lappu katoaa.

- Tallenna salasana salatussa muodossa tiedostoon tietokoneelle, sähköpostiin tai USB-muistitikulle.

- Käytä salasanojen hallintaan tarkoitettua sovellusta.

Salasanojen hallintasovellukseen on mahdollista tallentaa salasanoja salatussa muodossa siten, että salasanat ovat yhden pääsalasanan takana saatavilla. Tällöin käyttäjän tulee pitää erityistä huolta pääsalasanasta, eikä sitä saa kadottaa tai unohtaa. Useimmilla hallintasovelluksilla voidaan myös luoda laadukkaita ja erilaisia salasanoja eri palveluihin, ja siten pienentää tietomurron vaikutusta.

3.1 Hallintatyökalujen toimintatavoissa eroja

Jos haluaa käyttää salasanojen hallintaan tarkoitettua sovellusta, sen toimintaperiaatteet on hyvä tietää sovellusta valittaessa. Tietyt sovellukset tallentavat salasanat salatussa muodossa pilvipalveluun. Näin ne ovat helposti saatavilla lukuisilta päätelaitteilta. Jos pääsalasana häviää tai sitä käytetään väärin, kaikki salasanat voivat päätyä ulkopuolisen käsiin.

Osa salasanojen hallintasovelluksista taas tallentaa salasanat ainoastaan paikalliselle tietokoneelle tai muulle päätelaitteelle, jolle sovellus on asennettu. Tällöin salasanat ovat heikommin ulkopuolisten ulottuvilla, mutta säilöntä on riippuvainen päätelaitteen toiminnasta, varmuuskopioiden ajantasaisuudesta ja turvallisesta säilömisestä.

Salasanojen hallintaan tarkoitettuja sovelluksia ovat muun muassa:

- Password Safe
- Keepass ja KeepassX
- LastPass
- 1Password
- Keychain
- F-Secure Key.

Viestintävirasto ei ole tarkastanut edellä mainittuja ohjelmistoja, eikä ota kantaa siihen, toimivatko ohjelmistot valmistajien kuvausten mukaisesti.

3.2 Turvakysymyksellä unohtuneen salasanan saa takaisin

Monissa palveluissa käyttäjältä kysytään "turvakysymyksiä". Turvakysymysten avulla käyttäjän identiteetti yritetään todentaa, jos salasana on unohtunut ja tilanne vaatii vanhan salasanan "nollaamista". Käytännössä palvelun ylläpitäjä luo käyttäjälle uuden salasanan.

Turvakysymykset voivat kuitenkin olla petollisia. Jos salasanan urkkija tietää käyttäjästä tarpeeksi, hän voi arvata vastaukset. "Mikä oli ensimmäisen autosi merkki?" "Minkä niminen on lemmikkisi?" "Missä kaupungissa olet syntynyt?".

Tällaisiin kysymyksiin ei pidä vastata rehellisesti! Palvelun kannalta on nimittäin ihan sama, mitä niihin vastataan. Oleellista on itse muistaa, mitä on vastannut. Turvakysymysten vastaukset on syytä suojata yhtä hyvin kuin salasanatkin, koska niiden avulla on mahdollista muuttaa salasanaa.

Usein salasana palautetaan siihen sähköpostiosoitteeseen, joka on ilmoitettu palveluun rekisteröidyttäessä. Jos rekisteröity osoite löytyy palveluntarjoajan käyttäjälistan yhteystiedoista, osoitteeseen lähetetään linkki salasanan nollaamista ja uusimista varten. Sähköpostitilin salasana onkin erityisen tärkeä myös muiden palvelujen hallinnassa.

3.3 Pidä hyvää huolta pääsalasanoista

Osa palveluista ja salasanoista on merkityksellisempiä kuin toiset. Erityisesti on huolehdittava siitä sähköpostiosoitteesta, jonka rekisteröi palveluihin kirjautumisen yhteydessä ja siitä pääsalasanasta, jota käyttää salasanojen säilytysohjelmaan.

Sähköpostiosoitteen ja pääsalasanan paljastuminen avaa mahdollisuuden kirjautua ja vaihtaa myös muiden palveluiden salasanoja.

3.4 Kaksivaiheinen tunnistaminen ja poikkeavuusilmoitukset parantavat tietoturvaa

Kaksivaiheisessa tunnistamisessa ulkopuolinen ei pääse kirjautumaan palveluun tai järjestelmään, vaikka saisi tietoonsa käyttäjätunnuksen ja salasanan. Tämä vähentää väärinkäytösten riskiä merkittävästi etenkin käyttäjälle tärkeissä palveluissa.

Kun palveluun kirjautuvalta kysytään oma käyttäjätunnus ja salasana sekä koodi, jonka palvelu lähettää hänen kännykkäänsä, kyse on kaksivaiheisesta tunnistamisesta. Jotta ulkopuolinen pääsisi kirjautumaan tällaiseen palveluun, hänellä täytyisi olla käyttäjän puhelin hallussaan tai muuten pääsy käyttäjän puhelimeen välitettäviin tietoihin.

Poikkeavista kirjautumisista käyttäjälle ilmoittaminen ei tee tunnistuksesta ja todennuksesta turvallista, mutta sitä voidaan hyödyntää tilin käytön valvonnassa. Näin on mahdollista reagoida nopeammin väärinkäytöksiin ja ilmoittaa todennustietojen joutumisesta vääriin käsiin. Parhaassa tapauksessa käyttäjä ehtii itse estää tilinsä vakavamman väärinkäytön. Vääriä hälytyksiä voi tosin tulla, jos käyttäjä itse kirjautuu palveluun uudelta päätelaitteelta.

4 Salasanojen hyväksikäyttäminen ja murtaminen

Salasanoja voidaan hyväksikäyttää ja varastaa usealla eri tavalla. Tyypillisiä keinoja ovat salasanoja vievät haittaohjelmat, sosiaaliset huijaukset ja palvelujen tietomurrot. Onneksi käyttäjä voi omilla toimillaan ehkäistä salasanavarkauksia ja niiden vaikutuksia.

4.1 Haittaohjelmat varastavat salasanoja

Haittaohjelmat on yksi yleisesti hyödynnetty salasanavarkauskeino. Haittaohjelma voi tutkia päätelaitteen tiedostoja ja löytää selaimiin sekä ohjelmiin tallennettuja salasanoja.

Toisaalta haittaohjelma voi saada selville salasanoja myös näppäimistölukijaa (*engl. keylogger*) hyödyksi käyttäen. Näppäimistönlukija lukee, tallentaa ja toimittaa hyökkääjälle käyttäjän kirjoitukset, mukaan lukien salasanat.

Haittaohjelmien tartuntariskiä voi pienentää esimerkiksi käyttämällä ajantasaista antivirustuotetta. On hyvä huo-

lehtia myös siitä, että käyttöjärjestelmä, selaimet sekä selainliitännäiset tulevat ajantasaisesti päivitettyä.

4.2 Sosiaaliset ja tekniset huijaukset toteutetaan usein sähköpostitse

Myös erilaiset huijaukset ovat tyypillisiä tapoja yrittää varastaa salasanoja. Sähköpostitse voidaan pyytää tietyn palvelun käyttäjätunnusta sekä salasanaa.

Huijaaja on voinut laatia sähköpostiviestiinsä uskottavan oloisen tarinan, jossa pyydetään vaihtamaan salasanaa ja kirjautumaan palveluun sähköpostiviestissä olevan linkin kautta. Linkki ohjaa käyttäjän vierailemaan huijaussivustolla. Sivusto näyttää alkuperäisen palvelun sivustolta ja pyytää syöttämään käyttäjätunnuksen ja salasanan. Todellisuudessa tietojenkalastelusivu lähettää tiedot huijaajalle.

Tietojenkalastelua on tehty myös tekstiviestien, puheluiden ja pikaviestimien välityksellä. Soittoja ja tekstiviestejä on käytetty myös sähköpostihuijausten tukena uskottavuuden lisäämiseksi.

Myöskään yrityksissä esimerkiksi IT-tukihenkilönä esiintyvälle henkilölle ei tule antaa salasanaa. IT-tuki ei koskaan tarvitse tietoa salasanastasi toimiaan varten. Nyrkkisääntönä käyttäjän tulee muistaa, ettei salasanaa kannata antaa kenenkään ulkopuolisen haltuun.

Salasana voidaan viedä myös salakatselun tai -kuuntelun avulla. Tarkkailemalla ihmisiä julkisella paikalla voi nähdä paljon: mitä salasanoja päätelaitteisiin näppäillään ja millaisiin palveluihin kirjaudutaan. Onkin oleellista syöttää salasana niin, etteivät ulkopuoliset näe sitä. Mitä monimutkaisempi salasana on, sitä hankalampi sitä on myös toistaa, muistaa tai päätellä.

4.3 Tietomurtojen avulla päätyy massoittain salasanoja ulkopuolisille

Useimmiten massiivisia salasanamääriä onnistutaan varastamaan, jos suosittuun palveluun kohdistuu tietomurto. Käyttämänsä palvelun tietoturvaan pystyy vain harvoin vaikuttamaan, mutta käyttämällä mahdollisimman pitkiä ja palvelukohtaisia salasanoja sekä hyödyntämällä kaksivaiheista tunnistusta, käyttäjä voi pelastaa paljon. Tällöin tietomurron yhteydessä paljastuneista tiedostoista ei välttämättä pysty selvittämään käyttäjän salasanaa. Vain murrettuun palveluun liittyvät tiedot vaarantuvat, muiden palveluiden käyttöä voi kuitenkin jatkaa.

4.4 Yhteiskäyttöisten päätelaitteiden ja avoimen verkon tietoturva on epävarmaa

Ennen kirjautumista tärkeisiin yhteiskäytössä oleviin päätelaitteisiin, niiden tietoturvaan tulisi kiinnittää huomiota. Yhteiskäyttöisten päätelaitteiden tietoturvallisuudesta ei voi olla varma. Esimerkiksi kirjaston tietokoneella saattaa olla haittaohjelma tai näppäimistölukija.

Verkkoliikenne kulkee avoimissa WLAN-verkoissa salaamattomana, jolloin kuka tahansa voi sitä kuunnella. Myös käyttäjätunnusten sekä salasanojen syöttäminen sivustoille, jotka eivät käytä salattua yhteyttä, näkyy selväkielisenä langallista tai langatonta verkkoa salakuunteleville.

Erityisesti avoimissa WLAN-verkoissa kannattaa kirjautua vain sellaisille verkkosivuille, joiden yhteys on salattu (https://). Huomioida kannattaa myös muiden sovellusten verkkoliikenne, joka sisältää käyttäjätunnuksia sekä salasanoja. Esimerkiksi sähköpostipalveluun kirjautuminen voi tietyissä tapauksissa olla suojaamatonta. Myös FTP-palvelimiin kirjautuminen on yleensä

suojaamatonta. Jos WLAN-verkon liikenne on salattu, on verkkoliikennettä kuuntelevan hyökkääjän hankalampi saada haltuunsa käyttäjätunnuksia ja salasanoja. Salattuihin WLAN-verkkoihin kytkeytyminen edellyttää yleensä käyttäjältä salasanaa. Tulee kuitenkin huomioida, että kaikki salasanaa kysyvät WLAN-verkot eivät salaa liikennettä. Osa salaavista verkoista saattaa käyttää myös sellaista salausta, joka on kotikäyttäjän konsteinkin murrettavissa.

5 Salasanojen vahvuudet, heikkoudet ja tukevat todentamismenetelmät

Salasanojen käytön turvallisuuteen liittyy uhkia, minkä vuoksi niiden turvallisuutta ja käytettävyyttä ajoittain kritisoidaan. Vaihtoehtoisia menetelmiä on kuitenkin saatavilla.

Helppokäyttöisenä ja hyvin tunnettuna menetelmänä salasanoilla on etunsa. Muiden menetelmien onkin ollut hankala syrjäyttää niitä paitsi palveluissa, joissa käyttäjien tunnistamiseen ja todentamiseen on tarvittu luotettavampaa menetelmää.

Salasanojen edut ja haitat on hyvä tunnistaa. Näin käyttäjä ymmärtää ja osaa arvioida, missä palveluissa pelkkä salasana riittää ja missä ei. Kun todentamiseen tarvitaan "lisäkierroksia", on aika pohtia salasanan korvaavan, vaihtoehtoisen palvelun käyttöä. Käyttäjien tulisikin hyödyntää palvelunsa tarjoamia salasanoja tukevia todennusmenetelmiä aina, kun niitä on tarjolla.

5.1 Salasanoilla on etunsa

Salasanojen selkeä vahvuus muihin todentamismenetelmiin verrattuna on niiden edulliset toteutuskustannukset. Useat verkkopalvelut ovat ilmaisia tai toteutettu pienillä alkukustannuksilla.

Biometriset tunnistamismenetelmät (esim. iiris, sormenjälki) tai tunnistamisvälineet (esim. sirukortti) ovat kalliita. Niiden jakaminen on jo pelkästään taloudellisista ja logistisista syistä usein mahdotonta. Salasanat ovatkin käyttäjille tuttu ja hyväksytty menetelmä, joten niiden käyttöönotto on nopeaa eikä vaadi uusien käyttäjien opastusta.

Salasanojen etuihin kuuluu myös **t**ilannejoustavuus. Ne kulkevat helposti käyttäjän mukana. Tärkeimmät salasanat painuvat käyttäjän ulkomuistiin tai ovat lähellä esimerkiksi kännykässä.

Salasana on helppo jakaa käyttäjien kesken. Joissakin palveluissa useat käyttäjät käyttävät samaa tunnistetta. Tällainen tilanne voi syntyä, kun halutaan hallinnoida samaa tiliä tai asiakkuutta, eikä samaan käyttöoikeuteen ole mahdollista liittää useaa erillistä tunnistetta.

Lisäksi salasanojen hallinta mukautuu poikkeustilanteisiin. Salasanan voi nopeasti muuttaa, jos se esimerkiksi unohtuu, vanhenee tai palvelun tietoturvakontrollit muuttuvat tai siihen murtaudutaan. Fyysisen tai biometrisen tunnisteen korvaaminen ja uuden tunnisteen päivittäminen järjestelmään vie aikaa ja on hankalaa, jos esimerkiksi sirukortti katoaa tai sormeen tulee haava.

5.2 Salasanoilla on myös heikkouksia

Vaikka salasanatunnistamisen käyttöönottokustannukset ovat pienet, usein unohdetaan, että salasanojen ylläpitoon kätkeytyy piilokustannuksia. Kun esimerkiksi käyttäjät unohtavat salasanojaan, kasvavat ylläpito- ja asiakaspalvelutarpeet huomattavasti.

Suurin salasanoihin liittyvä ongelma on niiden riippuvuus käyttäjien kyvystä hallita salasanojaan. Käyttäjien on itse keksittävä laadukkaita salasanoja, jotka vaihtelevat palveluittain. Jos käyttäjän salasanat ovat aina samoja, yhden palvelun salasanojen paljastuminen voi vaikuttaa täysin sivullisenkin palvelun tietoturvaan. Tällöin palvelun käyttäjätilien tietoturva ei ole täysin ylläpidon oman osaamisen varassa.

Todentamiseen yksinkäytettyinä salasanat ovat kohtuullisen helposti teknisin apuvälinein murrettavissa ja sosiaalisin menetelmin selvitettävissä. Muutaman käyttäjän paljastuneet heikot salasanat voivat toimia siemeninä, joilla murtaja selvittää salasanojen tallennuksen laskukaavan ja onnistuu paljastamaan myös palvelun muiden käyttäjien paremmin laaditut salasanat.

Varsin usein verkkopalveluissa salasana on ainoa käyttäjän todentamistapa. Valitettavasti pelkän salasanan avulla voi tehdä paljon vahinkoa esiintymällä oikeutettuna käyttäjänä.

5.3 Tukevien todennusmenetelmien käyttö on suositeltavaa

Viestintävirasto suosittelee käyttämään salasanoja tukevia todennusmenetelmiä, kun sellaisia on käytettävissä.

Esimerkiksi useissa kuluttajille suunnatuissa verkkopalveluissa on mahdollista käyttää kaksivaiheista todentamista muun muassa käyttäjätunnus- ja salasanaparilla sekä tekstiviestivarmennuksella.

Myös menetelmiä, joiden avulla tietomurtoyrityksiä voidaan havaita, olisi hyvä käyttää, jos vain sellaisia on tarjolla. On kaikkien etu, jos esimerkiksi epätavallisista kirjautumisyrityksistä saa tiedon niin palvelun käyttäjä kuin ylläpitäjäkin.

6 Ylläpitäjien salasanojen käsittely

Salasanojen turvallisessa käytössä merkittävä vastuu on palvelun käyttäjillä. Kuitenkin suuri merkitys on myös sillä, miten palveluntarjoaja on teknisesti toteuttanut salasanojen hallinnan ja ylläpidon.

Palveluntarjoajan on huolehdittava turvallisesta salasanojen säilytyksestä ja salasanojen hallintaan liittyvistä tukipalveluista, kuten unohtuneen salasanan palautuksesta. Salasanojen hallinnan merkitys nousee esille erityisesti tietomurtojen ja teknisten väärinkäytösten yhteydessä: salasanojen ei haluta päätyvän ulkopuolisten tietoon.

6.1 Säilö salasanat tiivisteinä

Hyvin toteutetussa palvelussa salasanoja ei varastoida järjestelmään, vaan niistä lasketaan niin sanottu tiiviste jonkin yksisuuntaisen tiivistefunktion avulla. Huolellinen salasanojen säilöntä pienentää riskiä, että palvelun salasanoja käytetäisiin väärin.

Jos kirjautumisessa syötetty salasana tuottaa saman tiivisteen kuin järjestelmään talletettu, palvelu toteaa salasanan oikeaksi. Tällöin palvelun ei tarvitse edes tietää käyttäjän oikeaa salasanaa. Yleensä salasanojen murtaminen edellyttää, että murtaja saa haltuunsa tiivisteen, minkä jälkeen oikeaa salasanaa voi yrittää arvailla muualla kuin itse palvelussa sitä varten kehitetyillä ohjelmistoilla.

Salasanatiivisteiden luomiseen on käytettävissä useita vaihtoehtoisia salasanatiivistealgoritmeja. Esimerkiksi algoritmit PBKDF2, bcrypt ja scrypt soveltuvat tiivisteen luomiseen hyvin. Osa salasanatiivistealgoritmeistä hyödyntää tiivisteen muodostamisessa

jotain standardoitua kryptografista tiivistefunktiota, kuten SHA-2:ta. Ei ole suositeltavaa luoda salasanatiivisteitä yksin tällaisella tiivistefunktiolla, vaan käyttää yhtä edellä mainituista algoritmeistä.

6.2 Suolaus parantaa säilöntää

Merkittävä tekijä salasanatiivistealgoritmien turvallisuudessa on niin sanotun *suolan* käyttö.

Suola on satunnaisesti muodostettu uniikki käyttäjäkohtainen merkkijono, jota käytetään yhtenä algoritmin parametrina salasanan lisäksi. Suolan muuttaminen muuttaa myös salasanatiivistettä, vaikka itse salasana pysyisi samana. Tämä vaikeuttaa merkittävästi salasanojen selvittämistä tiivisteiden perusteella, eikä muutaman salasanan murtaminen helpota kaikkien salasanojen murtamista.

Toinen tärkeä tekijä turvallisuudessa on algoritmien hitaus: salasanatiivistealgoritmit ovat huomattavasti hitaampia kuin yleiskäyttöiset kryptografiset tiivistefunktiot. Tämä hankaloittaa salasanojen murtamista väsytysmenetelmällä.

Myös salasanatiivisteet ja suolatut salasanatiivisteet on mahdollista murtaa, jos hyökkääjä tietää käytetyn suolauksen, tiivistefunktion. Tiivistefunktiosta ja erikoismerkkien käytöstä riippuen myös pidemmät salasanat on mahdollista murtaa.

6.3 Ylläpitäjä - tarjoa lisäsuojaa

Palvelun tietoturvaa voi parantaa merkittävästi ottamalla käyttöön menetelmiä, jotka vaikeuttavat huijaamalla saatujen salasanojen käyttöä.

Jos ylläpitäjät eivät tarjoa asiakkailleen lisäsuojaa, ominaisuuksia ei myöskään voi ottaa käyttöön. Muun muassa kaksivaiheinen tunnistaminen ja varoitusilmoitukset poikkeavista kirjautumisista ovat askelia kohti turvallisempia verkkopalveluja, joista hyötyvät niin ylläpitäjät kuin käyttäjätkin. Vahvan tunnistamisen käyttöönottamista suositellaan yleisesti harkittavaksi palvelujen turvallisuuden tehostamisessa.

Yhteystiedot
Viestintävirasto
PL 313
Itämerenkatu 3 A
00181 Helsinki
Puh: 0295 390 100 (vaihde)
kyberturvallisuuskeskus.fi
viestintävirasto.fi