IDESCO

Take control of your overall security.

Turvallinen kulunvalvontajärjestelmä

Miten järjestelmän turvallisuutta voi parantaa

Tunnistusjärjestelmän turvallisuuteen vaikuttavat tunnisteet eli kortit, niitä lukevat lukijat, lukijoiden ja järjestelmän ohjauksen välinen tiedonsiirto ja järjestelmää käyttävät ihmiset.

Järjestelmän turvallisuusriskit kasvavat, jos järjestelmään valittuja tunnisteita voi kopioida, tai tunnisteen ja lukijan, tai lukijan ja järjestelmän ohjauksen välistä tiedonsiirtoa voi hakkeroida. Kopioimalla tai hakkeroimalla voidaan saada selville esimerkiksi suojaamaton kortin yksilöllinen sarjanumero, johon tunnisteen haltijan oikeus käyttää järjestelmää perustuu. Vääriin käsiin joutuneilla tiedoilla voidaan luoda toinen tunniste, jolla pääsee rakennukseen sisään.

Vanhemmat, tunnisteen yksilöllisen sarjanumeron eli UID:n lukemiseen perustuvat korttiteknologiat sekä lukijan ja järjestelmän välinen Wiegand-tiedonsiirtotapa eivät ole turvallisia, koska niissä tietoa käsitellään salaamattomana. Uudemmissa korttiteknologioissa tunnisteen tiedot suojataan tehokkailla salaustekniikoilla, kuten 128-bittisellä AES-salauksella. Se on käytännössä murtamaton salaustapa.

Turvalliset korttiteknologiat

Turvallisia korttiteknologioita sekä järjestelmän tiedonsiirtotapoja on kahdenlaisia; valmistajakohtaisia ja ns. avoimia teknologioita, jotka perustuvat yleisiin standardeihin. Käytännössä näiden erona on, että valmistajakohtaisen teknologian valitessaan sitoutuu myös jatkossa hankkimaan kortit ja lukijat samalta valmistajalta. Avoimen teknologian valitessaan ei ole yhden valmistajan varassa, vaan voi hankkia laitteita ja tunnisteita muiltakin valmistajilta. Avoin teknologia on turvallisuuden kannalta hyvä valinta, koska sitä kehittävät samaan aikaan useammat yritykset, eikä teknologian tulevaisuus ole vain yhden valmistajan varassa. Me suosittelemme MIFARE DESFire -teknologiaa. Avoin, yleisiin standardeihin perustuva korttiteknologia kehittyy jatkuvasti ja täydentyy koko ajan uusilla turvaominaisuuksilla.

Turvallinen järjestelmän tiedonsiirto

Lukijoiden ja järjestelmän väliseen tiedonsiirtoon kannattaa valita turvallinen, avoin OSDPV2 -standardi, joka on paitsi turvallinen, myös tehokas kaksisuuntainen tiedonsiirtotapa. Sen avulla tietoa voi siirtää myös järjestelmästä lukijoihin päin, joten esimerkiksi lukijoiden päivittäminen keskitetysti järjestelmästä käsin, sekä erilaiset käyttäjäkohtaiset viestit järjestelmästä vaikkapa lukijan näytölle ovat mahdollisia.

Mobiilitunnistus

Puhelimella tunnistautuminen yleistyy. Fyysisen kulkukortin rinnalle on tullut mahdollisuus pitää kulkuoikeuksia puhelimessa, josta lukija lukee ne NFC- tai Bluetooth-yhteydellä. Myös puhelin on yhtä turvallinen tunnistautumistapa kuin salauksella suojatut MIFARE DESFire -tunnisteet. Tiedonsiirto puhelimen ja lukijan välillä

Idesco Oy

Elektroniikkatie 4
90590 Oulu
Finland

Tel. +358 (0)20 743 4175
Email info@idesco.fi
idesco.fi

tapahtuu samalla suojatulla tekniikalla kuin lähimaksamisessa. Puhelimen omasta sormenjälkitunnistuksesta tulee biometriseen tunnistukseen verrattava lisäturvaominaisuus.

Turva-avainten hallinta

Kaikissa turvallisissa korttiteknologioissa lukijat ja tunnisteet ohjelmoidaan turva-avaimilla, jolloin tunnisteen voi lukea vain erikseen sille ohjelmoidulla lukijalla. Aina kun valitsee turva-avaimilla suojatun teknologian, kannattaa varmistaa miten laitevalmistaja suhtautuu turva-avainten omistajuuteen. Jotkut, myös avoimeen teknologiaan perustuvien laitteiden valmistajat pitävät turva-avainten omistajuuden itsellään. Käytännössä se tarkoittaa, että toimittajaa ei voi avoimesta teknologiasta huolimatta vaihtaa, mikäli haluaa jatkossakin saada samaan järjestelmään sopivia lukijoita ja tunnisteita. Me annamme asiakkaan määritellä itse, kuka turva-avaimet omistaa. Koko sen ajan, kun turva-avaimet ovat hallussamme, pidämme ne tallessa tiukimpien tietoturvakäytäntöjen mukaisesti, mutta asiakkaamme saa ne halutessaan myös itselleen.

Pin-koodi

Väärään paikkaan unohtuneen kulkukortin väärinkäyttöä voi estää ottamalla käyttöön pin-koodin, joka on yksinkertainen tapa parantaa minkä tahansa järjestelmän turvatasoa. Pin-koodi on turvallinen siksi, koska sitä ei tallenneta itse korttiin, johon se on liitetty. Pin-koodin verifikaatio tapahtuu järjestelmässä, joka hyväksyy sekä tunnistautujan kortin tiedot sekä hänen antamansa pin-koodin, joiden molempien pitää täsmätä.

Kokonaisturvallisuuden monet tekijät

Kokonaisturvatasoa parannetaan kaikkiin turvallisuuden osatekijöihin kohdistuvilla muutoksilla. Turvallisuus ei riipu vain teknologiasta, vaan siihen vaikuttavat myös muut tekijät, kuten koko järjestelmän turvallisuus, tiedonsiirtotapa lukijoiden ja järjestelmän välillä, tiedon salaustavat ja inhimilliset tekijät.

Järjestelmä on yhtä turvallinen kuin sen heikoin lenkki. Mikään salaustekniikka ei pelasta, jos oven avaaminen tunnistautumalla koetaan vaivalloiseksi ja oven väliin laitetaan este, jotta se pysyisi auki. Mahdollisimman helppokäyttöisten lukijoiden valinta, turvakäytännöistä tiedottaminen, ohjeiden jatkuva päivittäminen ja valvonta ovat kulunvalvonnan turvallisuudesta vastaavien työtä.

Autamme sinua mielellämme kulunvalvontalukjoiden valinnassa! Ota yhteyttä: sales@idesco.fi.

Idesco Oy

Elektroniikkatie 4
90590 Oulu
Finland

Tel. +358 (0)20 743 4175
Email info@idesco.fi
idesco.fi