SECURITY®

security.fi

GDPR, lainsäädäntö ja tietoturva

GDPR.EU

Future. Tomorrow. Today.

SECURITY®

security.fi

Turvallisuuspalveluihin ja kameravalvontaan liittyvä **lainsäädäntö**

Turvallisuuspalveluita ja erityisesti kameravalvontaa koskevaa lainsäädäntö on hyvin hajanaista. Palveluihin ja niiden toteutukseen liittyvää keskeistä sääntelyä on työelämää koskevat laki yksityisyyden suojasta työelämässä (759/2004), yhteistoimintamenettelyä koskeva lainsäädäntö (334/2007) ja työturvallisuuslaki (738/2002). Lisäksi kameravalvontaa koskevat laki yksityisistä turvallisuuspalveluista (1085/2015), tietosuojaa koskeva sääntely (1050/2018) ja rikoslaki (39/1889). Kameravalvontaa koskevia teknisiä viranomaismääräyksiä ei ole.

Tietoturvallisuus ja **lainsäädäntö**

EU:n verkko- ja tietoturvadirektiivissä (NIS-direktiivi, 2016/1148) säädetään yhteiskunnan kriittisen infrastruktuurin tarjoajien ja toimijoiden tietoturvavelvollisuuksista sekä tietoturvahäiriöistä ilmoittamisesta.

Valvira vastaa Suomessa EU:n verkko- ja tietoturvadirektiivin (NIS-direktiivi) mukaisesta valvonnasta terveydenhuollon osalta. Laki velvoittaa huoltovarmuuskriittisiä yrityksiä ja keskeisiä digitaalisten palveluiden tarjoajia ilmoittamaan ja raportoimaan tietoturvaloukkauksista. Suomessa Traficom (Traficom.fi) kokoaa valvovilta viranomaisilta saadut ilmoitukset yhteen ja toimii Suomen yhdyspisteenä EU-jäsenvaltioiden välillä.

Direktiivin valvovat toimialakohtaiset viranomaiset ovat:

Liikenne - Traficom Energiahuolto - Energiavirasto, Terveydenhuolto - Valvira, Finanssiala - Finanssivalvonta, Finanssialan infrastruktuuri - Finanssivalvonta, Vesihuolto - ELY-keskukset Digitaalinen infrastruktuuri - Traficom, Digitaaliset palvelut.

Tietoturvallisuus tulee ottaa vakavasti huomioon kaikissa yrityksissä. Lähes kaikki liiketoiminta on pääosin digitaalista jolloin turvallisuuslaitteiden ja palveluiden riskienhallinnan kulmakivi on: Turvapalveluiden toimittajan tulee olla syvällisesti perillä lainsäädännöstä ja tietoturvallisuudesta.

SECURITY®

security.fi

Tietoturvallisuus ja **termit**

Tietoturvallisuus

Suoritetut toimenpiteet, joiden avulla yritetään varmistaa tiedon saatavuus, eheys ja luottamuksellisuus. Tietoturva kattaa muun muassa tietoaineistojen, laitteistojen ja ohjelmistojen turvaamisen. Tiedon saatavuudella pyritään siihen, että tieto on hyödynnettävissä silloin kun sitä tarvitaan. Eheydellä tarkoitetaan sitä, että tieto on alkuperäistä eikä sitä olla päästy muuttamaan. Tiedon luottamuksellisuudella tarkoitetaan sitä, että tieto on saatavilla vain niille, joille se on tarkoitettu. (Turvallisuuskomitea 2018, 15.)

Tietoturvauhka

Ulkoinen tai sisäinen tietoturvalle haitallinen tapahtuma. Sisäinen tietoturvauhka käsittää organisaation oman henkilökunnan aiheuttaman tietoturvauhan, kuten esimerkiksi tahattoman tietojen luovuttamisen väärälle henkilölle. Ulkoisella tietoturvauhalla tarkoitetaan organisaation ulkopuolelta aiheutuvaa uhkaa, esimerkiksi virusta. (Sanastokeskus TSK 2004.)

Tietoverkkohyökkäys

Turvallisuuskomitean (2018, 30) määritelmän mukaan teko tai toiminta, jonka tavoitteena on tietoverkkoa hyödyntäen vahingoittaa tai väärinkäyttää tietojärjestelmää, tietoverkkoa, dataa tai laitetta. Tietoverkkohyökkäyksen toteutustapoja ovat esimerkiksi palvelinestohyökkäys tai haittaohjelma.

European Commission

GDPR

General Data Protection Regulation

SECURITY®

security.fi

Poliisihallituksen **hyväksymä** virallinen vartiointiliike Suomessa.

Turvasuojaamisen kulmakivi on yksiselitteisesti: Nykyaikainen, ammattitason teknologia ja sen valvontayhteys palvelukeskuksen monitorointiin 24/7.

Keskitymme erittäin korkealaatuiseen teknologiaan ja älykkäisiin palveluihin, joilla pystymme tuottamaan huomisen ratkaisut ylivertaisella käyttökokemuksella kustannustehokkaasti kaikille asiakkalillemme.

Pelkällä laitteella saavutetaan parhaimmillaankin vain vaatimaton turvallisuustaso. Yhteistyö poliisihallituksen hyväksymän liikkeen kanssa on ainoa takuu korkean tason suojaamiseen myös lainsäädäntöön liittyen (GDPR, LYTP).

POLIISI
POLIISIHALLITUS

KKV Kilpailu- ja kuluttajavirasto

TIETOSUOJAVALTUUTETUN TOIMISTO

EDUSKUNTA TURVALLISUUDEN TEKIJÄNÄ

GDPR ja tietosuoja (GDPR – EU 2016/679, LYTP 1085/2015)

Tietosuoja-asetus koskettaa kameravalvontaa, palvelusta muodostuu henkilörekisteri.

- Kuka vastaa henkilörekisteristä ja turvalokista?
- Kuka vastaa kameroiden luvanvaraisuudesta ja kuka tuottaa tietosuojadokumentit kohteelle?
- Miten palveluntuottajan asiakasrekisteri on suojattu omia tietojani koskien?
- Millä tasolla palveluntuottavan verkko on suojattu ja kuka siitä vastaa?
- Kuka konsultoi asiakasta, jos tarvitsen asiantuntijan apua esim. luottamusmiehen / viranomaisen kysyessä tarkennuksia lakisääteisyyteen liittyen?

Palveluihimme sisältyvät mm. vartiointi-, hälytyskeskus-, kuvavalvonta-, etäkäyttö-, kiinteistöautomaatio-, paloilmoitin-linjavalvonta- sekä muut hälytyskeskuspalvelut tietoverkkojen ohessa. Pyrimme myös kehittymään jatkuvasti aktiivisena toimijana osallistumalla dialogiin alan eri viranomaisten kanssa.

Lakisääteiset velvoitteet, niiden noudattaminen ja mahdolliset muutokset niihin liittyen kuuluvat aina palveluumme. Tuotamme asiakkaillemme kaikki ratkaisut lakivelvoitteiden mukaisesti - keskitetysti ja yhdeltä toimittajalta.

SECURITY®

security.fi

EU:n tietosuoja-asetus
ja turvallinen verkkoratkaisu.

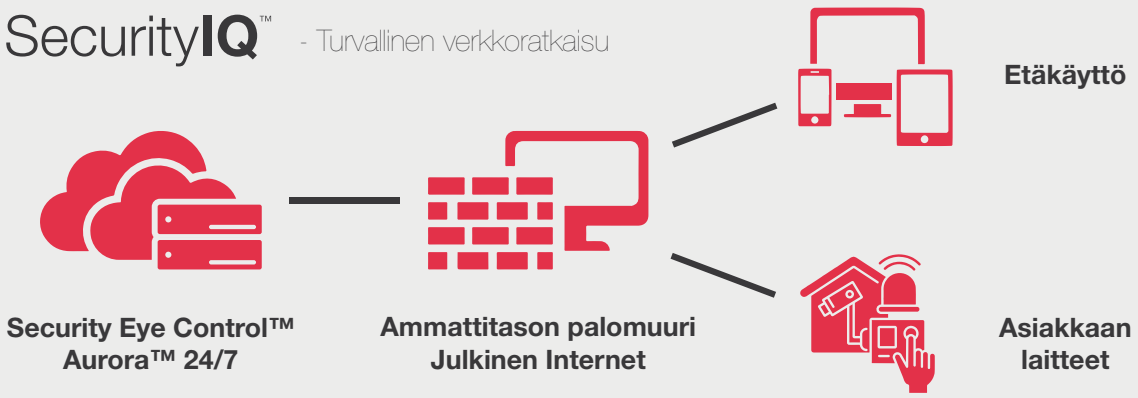
Security IQ™ – Tietoturvallisuus – Erillinen tiedonsiirtopalvelu

Digitalisaation myötä yritysten liiketoiminta, data sekä palvelut siirtyvät yhä vahvemmin verkkoon. Yritykset myös hankkivat eriasteisia etäkäyttöpalveluita kilpailukykynsä optimoimiseen. Tämä trendi avaa myös verkkorikollisille ja hakkereille uusia mahdollisuuksia. Silti suojautuminen uhkia vastaan on usein liian heikkoa.

Onko sinun yrityksesi turvassa tietomurroilta? Miten nykyiset turvallisuusjärjestelmäsi on suojattu ja dokumentoitu?

Miltei kaikki maailman organisaatiot kokoon katsomatta ovat nykypäivän verkkorikollisten kohteena. Toivomme, että käsittelette näitä asioita myös oman organisaationne sisällä ja suhtaudutte vakavasti tulevilta uhilta suojautumiseen. Digitalisoituvassa maailmassa yhä useammat pienet ja keskisuuret yritykset tulevat osaksi yhteiskunnan kriittisiä verkostoja. EU:n tietosuoja-asetus tuottaa yrityksille lisäpaineita myös asiakkaidensa tietojen turvaamiseen. Asetuksen voimaantulon jälkeen sakkorangaistukset tietosuojasääntöjen rikkomisesta voivat olla parikin prosenttia yritysten liikevaihdosta.

https://www.viestintavirasto.fi/kyberturvallisuus/tietoturvanyt/2017/01/ttn201701171301.html



Me olemme valmiita avustamaan teitä matkalla turvallisempaan tietoympäristöön tarjoamalla alan viimeisintä teknologiaa hyödyntävät ratkaisut myös tietoliikenteen osalta. Security IQ™ -verkkoratkaisumme huolehtii etäyhteyksienne optimoinnista, päivittäisestä, ylläpidosta, tuesta sekä arjen sujuvuudesta. Tuotamme kohteeseenne erillisen internetyhteyden etäkäyttöpalveluiden eriyttämiseksi omasta verkostanne.

SECURITY®

security.fi

Tietoturvalliset käytännöt kameravalvontapalveluissamme

Kirjautumiset järjestelmiin

Kun käyttöoikeus on myönnetty, istuntojen aikaa ja tunnistetietoja seurataan. Jos istunto jää lepotilaan tai asiakas syöttää uudelleen virheelliset tunnistetiedot, istunto suljetaan.

Identiteettisuojaus

Käytössä pakotettu salasanan nollaus, mikä estää pääsyn oletustunnistetiedoilla käyttöönoton jälkeen. Ennen salattujen tietojen lähettämistä Digest Access Authentication- palvelu vahvistaa käyttäjän henkilöllisyyden ja estää pelkkää tekstiä kulkemasta yhteyden läpi. Palvelukeskuksemme hallinnoi etäkäytöllä käyttäjätunnuksia ja pääsyoikeuksia.

Datan enkryptaus ja salaus

Datan suojaaminen auttaa sallitun käyttäjän istunnon aikana varmistumaan tietojen turvallisesta siirtämisestä. Käytämme mm SSH sekä HTTPS-yhteyksiä ja epäsymmetrisiä salattuja istuntoja julkisen ja yksityisen avaimen järjestelmillä varmistaen, että vain valtuutettu vastaanottaja näkee tiedostot ja niiden sisällön.

Tiedostojen varmistus

Varmistaa laiteohjelmiston päivityspakettien eheyden ja suojaa ei-toivotuilta hyötykuormilta. Turvattomat palvelut on oletuksena poistettu käytöstä, kun taas järjestelmä tarkkailee aktiivisesti salasanan murtoyrityksiä ja tarkastaa liikennettä ei-toivottujen hyötykuormien varalta. Käyttöoikeuksien keskitetyn hallinnan avulla palvelukeskuksemme järjestelmänvalvojat voivat rajoittaa jokaisen käyttäjän oikeuksia tarpeen mukaan.

Turvallisuusauditointi

Jokainen käyttäjän aiheuttama tapahtuma ja järjestelmään tekemä muutos kirjataan. Lokien poistamisoikeudet ovat erittäin rajoitettuja, mikä tarkoittaa, että tämä ominaisuus on vain palvelukeskuksessamme ja vastuullamme.

Verkkoprotokollien turvallisuus

Käytössä on alan standardiprotokollia, joista monet perustuvat avoimeen lähdekoodiin. Vertaisarvioitujen protokollien käyttö ylläpitää standardeja ja parantaa laatua.

SECURITY®

security.fi

Security Eye Finland Oy

Tammimäenkatu 6
20320 Turku
Finland

www.security.fi
myynti@security.fi

010 229 5600