movendos

Yhteenveto Movendos-tietojärjestelmien tietoturvapolitiikasta ja -käytännöistä

V2.7 – 8. Tammikuuta, 2020

Yleinen tietoturvapolitiikka ja sen tavoitteet

Movendos Oy:n toiminnan ydin perustuu tietoon, ja tiedon turvaaminen on oleellinen osa yrityksen toiminnan ja palvelujen laatua, kokonaisturvallisuutta ja kaikkien yrityksessä työskentelevien päivittäistä työtä. Tietoturvallisuus koostuu tiedon luottamuksellisuudesta, eheydestä ja käytettävyydestä. Movendos Oy:n tietoturvapolitiikka määrittelee tietojen turvaamisen tavoitteet, vastuut ja toteutuskeinot yrityksessä.

Tietoturvallisuuden hyvä hallinta edellyttää toiminnan jatkuvaa seuraamista, suunnittelua, koulutusta, viestintää ja varautumista erilaisiin uhkatilanteisiin. Tietoturvallisuudesta huolehditaan Movendos Oy:ssa kansallisten ja kansainvälisten tietoturvallisuutta koskevien säädösten mukaisesti. Movendos Oy:n tietoturvatyön tavoitteena on turvata riittävällä ja tarkoituksenmukaisella tavalla yrityksen ylläpitämien ja/tai kehittämien tietojen, tietojärjestelmien ja palveluiden toiminta, estää niiden valtuudeton käyttö sekä tiedon tahallinen tai tahaton tuhoutuminen tai vääristyminen.

Tietoturvapolitiikka on julkinen asiakirja ja se voidaan antaa kaikille siitä kiinnostuneille tiedoksi. Julkisen tietoturvapolitiikan lisäksi yrityksellä on sisäisiä tietoturvaan liittyviä toimintaohjeita ja dokumentteja, jotka eivät ole julkisia.

Vastuut ja organisointi

Vastuu tietoturvallisuudesta ja sen kokonaisvaltaisesta kehittämisestä Movendos Oy:ssa on yrityksen toimitusjohtajalla, joka toimii myös yrityksen tietosuojavastaavana. Movendos Oy:n operatiivinen johtoryhmä (hallitus) vastaa tietoturvallisuuden päälinjauksista, ohjauksesta ja seurannasta.

Koko yrityksen henkilöstö osallistuu tietojen turvaamiseksi tehtävään jatkuvaan tietoturvan kehittämis-, toteuttamis-, ja seurantatyöhön. Jokaisen yrityksessä työskentelevän on tunnettava yrityksen tietoturvapolitiikka ja noudatettava sen perusteella annettuja ohjeita ja määräyksiä. Jokainen Movendos Oy:n työntekijä, Movendos Oy:n ylläpitäminen palvelujen henkilötietoja tai muita tietoja käsittelevä henkilö tai palveluiden käyttäjä on omalta osaltaan vastuussa tietosuojan ja tietoturvan toteuttamisesta sekä tietoturva- ja tietosuojaohjeiden noudattamisesta. Jokainen henkilö on velvollinen raportoimaan havaitsemistaan tietosuojaan tai tietoturvaan liittyvistä uhista yrityksen tietosuoja- ja tietoturvavastaavalle.

Movendos palvelun tietoturva: toteutuskeinot

Keskeisiä periaatteita ovat:

1) Movendos tietojärjestelmät ja kehitysympäristöt pidetään aina ajan tasalla automaattisilla turvapäivityksillä.
2) Movendoksella on lukittavat toimitilat ja avaimia on luovutettu vain nimetyille henkilöille. Toimitilat pidetään aina lukittuina kun Movendos -henkilökuntaa ei ole paikalla.

Movendos-palvelu tietoturva-auditoidaan säännöllisesti ulkopuolisen tahon toimesta. Viimeisimmän auditoinnin maaliskuussa 2018 suoritti tietoturvayhtiö 2NS jolla on vuosien kokemus lukuisista erilaisista ja erikokoisista tietoturva-auditoinneista. Palvelusta ei löytynyt kriittisiä tietoturvahaavoittuvuuksia. Movendos-palvelu on 2NS yhtiön jatkuvan tietoturva seurannan kohteena ja laajempi auditointi suoritetaan vuosittain. Yhteenveto Movendos -palvelun tietoturva-auditoinneista löytyy liiteenä tämän dokumentin lopusta.

1) Kaikki tietoliikenne käyttäjän päätelaiteen ja Movendos -palvelun välillä on aina SSL suojattua (256 bittinen salausavain).
2) SSL sertifikaattien hallinta:
    a) Movendos sertifikaatteja hallinnoi yksi nimetty henkilö
    b) Sertifikaattien salainen avain säilytetään erillisessä järjestelmässä, johon vain nimetyllä henkilöllä on pääsy.
3) Kaikki palvelun komponentit pidetään ajan tasalla automaattisin tietoturvapäivityksin.
4) Movendos -palvelun käyttöoikeudet ja käyttäjäroolit:
    a) Movendos palvelun palvelimet: Palvelimille on pääsy vain määritellyistä IP osoitteista niillä nimetyillä henkilöillä, joiden työtehtävät sitä vaativat (palvelun ylläpito sekä jatkokehitys) ja sisäänkirjaantumisessa on käytössä kaksivaiheinen tunnistautuminen.
    b) Movendos palvelun tietokantapalvelimet: Palvelimille on pääsy vain määritellyistä IP osoitteista niillä nimetyillä henkilöillä, joiden työtehtävät sitä vaativat (palvelun ylläpito sekä jatkokehitys) ja sisäänkirjaantumisessa on käytössä kaksivaiheinen tunnistautuminen.
    c) Administrator: Vain Movendos henkilökunnan jäsenillä, joiden työtehtävät niin vaativat, on pääsy Movendos palvelun administrator tason tietoon. Vain administrator -roolilla on pääsy Movendos -palvelun organisaatiotason tietoon. Administrator salasana vaihdetaan säännöllisesti osana tietoturvaprosessia.
    d) Supervisor: Pääsy vain oman organisaation valmentaja- ja asiakastason tietoon
    e) Valmentaja laajennetuin oikeuksin: Pääsy vain henkilökohtaisiin ja oman organisaation asiakkaiden tietoihin
    f) Valmentaja: Pääsy vain henkilökohtaisiin ja omien valmennettavien tietoihin
    g) Asiakas: Pääsy vain henkilökohtaisiin tietoihin
5) Asiakastunnusten luonti: Kaikki uuden asiakastunnukset luodaan ammattilaisen toimesta (valmentaja), joka varmistuu asiakkaan henkilöllisyydestä ennen tilin luontia. Asiakkaat eivät voi itse luoda itselleen tiliä.
6) Käyttäjätunnukset:
    a) Kaikki käyttäjätunnukset ovat henkilökohtaisia.
    b) Salasana vaaditaan aina palveluun sisäänkirjautumisen yhteydessä.
    c) Palvelun salasanoilla on seuraavat minimivaatimukset: vähintään 8 merkkiä, joista vähintään yhden on oltava iso kirjain ja vähintään yhden pieni kirjain sekä lisäksi yhden on oltava numero.
7) Movendos -palvelu kerää audit-lokia palvelun käytöstä. Loki sisältää tiedon siitä, kuka käytti palvelua sekä koska ja kuinka hän sitä käytti. Audit lokissa ei ole henkilökohtaisia tietoja. Pääsy tuohon lokitietoon on vain nimetyillä henkilöillä ja vain ennalta määritetyistä IP osoitteista.

8) Movendos -palveluympäristöön on rakennettu lukuisia automaattisia tarkkailumekanismeja havaitsemaan palvelussa mahdollisesti tapahtuvia poikkeavia tilanteita, kuten esimerkiksi palvelunestohyökkäyksiä. Seurattavia asioita ovat esimerkiksi palvelun servereiden ja tietokantaservereiden tilanne (kuormitus, levytila, muisti, …), palveluun tulevan ja lähtevän liikenteen määrä, IP-osoitteesta tuleva poikkeavan suuri liikennemäärä, palvelun vasteajat, ynnä muut vastaavat asiat. Palvelun nimetyt ylläpitäjät saavat automaattisen ilmoituksen kaikista epänormaaliksi luokitelluista tilanteista.
9) Kaikki palvelun käyttäjädata pysyy EU-alueen sisällä.
10) Videopuheluominaisuus:
    a) Perustuu ns. WebRTC-teknologiaan, joka mahdollistaa suorat nettiselaiten väliset yhteydet yhteydet (P2P).
    Lisää aiheesta mm. seuraavasta linkistä. http://webrtc-security.github.io/
    b) Kuvausta WebRTC-teknologian tietoturva-arkkitehtuurista: https://tools.ietf.org/html/draft-ietf-rtcweb-security-arch-12

Seuranta ja ongelmatilanteiden käsittely

Tietoturvavastaavan tehtävänä on seurata ja valvoa Movendos Oy:n tietoturvan toteutumista ja ryhtyä tarvittaessa toimenpiteisiin tietoturvan parantamiseksi. Kaikki yrityksessä työskentelevät ja Movendos Oy:n palveluiden keräämää tietoa käsittelevät ovat velvollisia raportoimaan havaitsemistaan tietosuojaan tai tietoturvaan liittyvistä uhista yrityksen tietosuoja- ja tietoturvavastaavalle.

Tietoturvavastaavan yhteystiedot

Toimitusjohtaja Arto Leppisaari. Sähköposti: arto.leppisaari@movendos.com, puh. +358 50 5117305.

movendos

Yhteenvedot Movendos palvelulle ulkopuolisen tahon suorittamista tietoturva-auditoinneista

Tietoturva-auditointi, syyskuu 2019

Kyberturvapalveluihin erikoistunut Nixy Oy suoritti HUS Työterveyden tilauksesta tietoturva-auditoinnin Movendos Health Platform-alustalle keskittyen mSurvey ja mBooking toiminnallisuuksiin. Auditointi suoritettiin syyskuussa 2019.

Auditointi suoritettiin blackbox-menetelmällä ulkopuolisen hyökkäjän näkökulmasta. Auditointi piti sisällään yleisimmät tietoturvahaavoittuustyypit verkkosovelluksissa (OWASP Top 10)

Auditoinnissa ei havaittu kriittisiä haavoittuvuuksia mSurvey ja mBooking toiminnallisuuksissa.

Tarkemmat tiedot auditoinnista:
Arto Leppisaari. Sähköposti: arto.leppisaari@movendos.com, puh. +358 50 5117305.

movendos

2NS

REPORT, INFORMATION SECURITY AUDIT

Date:	26.3.2018
Customer:	Movendos
Service:	Survey feature of movendos.com
Auditor:	Second Nature Security Oy

Statement:
Independent information security auditor Second Nature Security Oy (2NS) has audited the Survey feature of movendos.com service in December 2017 and verified the fixes made in March 2018. According to the audit and the verification, no critical vulnerabilities were found from the Survey feature.

About the audit:
Methodologies used in the audit are based on industry standards, such as OSSTMM (Open Source Security Testing Methodology Manual) and OWASP (Open Web Application Security Project).

Time and workload of the audit:
Audit was completed in December 2017. Workload of the audit was 8 man-days. Verification was completed in March 2018. Workload of the verification was 1,5 man-days.

Auditor:
2NS (Second Nature Security Oy) is an independent auditor that has audit experience from hundreds of business critical applications. 2NS has reported and released multiple advisories related to for example products from following companies: A-Link, Buffalo, Checkpoint, F-Secure, HP, IBM, Oracle, Xerox, Zyxel. More information: www.2ns.fi

movendos

VINCIT

Innokas ohjelmistotalo, joka tekee kaikkensa asiakkaidensa ja työntekijöidensä eteen. Takuulla.

Tietoturva-auditoinnin tiivistelmä

3. maaliskuuta 2016

Movendoksen mCoach-verkkopalvelulle tehtiin tietoturva-auditointi Tammi–Helmikuussa 2016. Auditoinnin työmäärä oli 5 henkilötyöpäivää ja sen suoritti tietoturvaan erikoistunut Vincit Black Ducks –asiantuntija, jolla usean vuoden kokemus lukuisista tietoturva-auditoinnista.

Auditointi suoritettiin blackbox-menetelmällä ulkopuolisen hyökkääjän näkökulmasta. Blackbox-menetelmässä auditoijalla ei ole etukäteen annettua tietoa kohteen toteutustavasta tai teknisistä ratkaisuista. Auditoija pyrkii käytettävissä olevan ajan puitteissa havaitsemaan mahdollisimman laajasti ulkopuolisen hyökkääjän käytettävissä olevia tietoturvaongelmia kohdepalvelussa.

Auditointi piti sisällään yleisimmät tietoturvahaavoittuvuustyypit verkkosovelluksissa (OWASP Top 10), kuten injektiohaavoittuvuudet (esim. SQL-injektio), autentikaatio ja isuntunnonhallintaongelmat ja cross-site scripting (XSS). Lisäksi auditoinnissa tarkastettiin vaatimuksia ASVS v3.0 standardin tasosta 1 palveluun soveltuvin osin.

Auditoinnissa ei havaittu kriittisiä haavoittuvuuksia.

Muiden löydösten osalta kuvaukset toimitettiin Movendokselle. Löydöksistä korjattavat käytiin Movendoksen kanssa läpi. Korjattavien löydösten lisäksi palvelussa ei ole tunnettuja haavoittuvuuksia.

Auditointi suoritettiin mCoach-palvelun kehitysympäristössä.