Miracle42

Organisatoriske og Tekniske foranstaltninger

Marts 2023

Part of itm8®

Indhold

Introduktion

Miracle 42 er dedikeret til at sikre beskyttelse af personoplysninger i overensstemmelse med EU's databeskyttelsesforordning (GDPR).

For at opfylde denne forpligtelse implementerer Miracle 42 ISO/IEC 27001:2022 standarden for styring af informationssikkerhed, som definerer rammerne for etablering, implementering, vedligeholdelse og løbende forbedring af informationssikkerheden.

Organisatoriske og tekniske foranstaltninger

Governance

For at sikre implementering, forbedring, forankring og ledelse af informationssikkerhed og databeskyttelse, har Miracle 42 oprettet en Governance model som omfatter:

- Implementeret et sæt af politikker for informationssikkerhed
- Defineret roller og ansvar for informationssikkerhed
- Implementeret et passende niveau af funktionsadskillelse
- Sikret at informationssikkerhed er forankret i ledelsen
- Sikret nødvendige kontaktflader til myndigheder og interessegrupper
- Sikret at informationssikkerhed er en del af vores projektledelsesmodel

Administration af aktiver

Miracle 42 fører kontrol med informationsaktiver for at sikre beskyttelse og at disse er registreret og anvendes korrekt. Herunder har Miracle 42 implementeret følgende foranstaltninger:

- Informationsaktiver er registreret
- Medarbejdere er instrueret i acceptabel brug af aktiver, herunder om specielle sikkerhedskrav for aktiver udenfor virksomhedens lokationer
- Tilsikre at aktiver returneres efter endt anvendelse
- Procedurer for sikker afskaffelse og sikker genbrug af udstyr, herunder sletning af data

Informations beskyttelse

Miracle 42 har implementeret en række foranstaltninger som danner grundlag for god beskyttelse af informationer, hvilket omfatter følgende:

- Data er klassificeret og mærket udfra følsomhed og fortrolighed.
- Der er fastlagt regler for overførsel af information indenfor organisationen og mellem andre interessenter.
- Der er fastlagt regler for beskyttelse af personlige henførbare oplysninger
- Det sikres at data slettes når organisationen ikke længere har grundlag for at lagre dem.
- Ved overførsel af persondata til test- og udviklingssystemer, foretages enten en pseudonymisering eller anonymisering af persondata.

Medarbejdersikkerhed

Medarbejdere er en vigtig brik i at opretholde og forbedre informationssikkerheden. Derfor er det etableret en række foranstaltninger med det formål at sikre Miracle 42's medarbejdere medvirker til at opretholde og forbedre informationssikkerheden i organisationen. Herunder følgende

- Alle medarbejdere skal kunne præsentere en ren straffeattest
- Der indgås fortroligheds- og tavshedsaftaler med alle medarbejdere
- Alle medarbejdere trænes og testes i informationssikkerhed og GDPR ved ansættelse, og herefter løbende under deres ansættelse.
- Der er opsat regler og kontroller for sikkert fjernarbejde
- Der er kommunikeret disciplinære konsekvenser for brud på organisationens sikkerhedsregler.

Fysisk sikkerhed

Der er implementeret tilstrækkelige foranstaltninger for fysisk sikkerhed, for at forhindre fysisk adgang eller beskadigelse af informationsaktiver. Dette omfatter:

- Adgangskontrol og overvågning af adgang på kontorlokationer og datacentre.
- Anvendelse af ID- og adgangskort for medarbejdere, og gæstekort for gæster for at sikre tydelig identifikation.
- Foranstaltninger for indbrudssikring, samt alarmering ved indbrud
- Minimering af adgange til datacentre
- Videoovervågning af indgange
- Der er implementeret retningslinjer for at arbejde i sikre områder
- Regler for clean desk og låsning af skærm når arbejdspladsen forlades
- Regler for placering af udstyr så kritisk udstyr kun placeres aflåst.
- Kabler og andet udstyr er sikret mod sabotage
- Udstyr vedligeholdes udfra leverandørens anvisninger og anbefalinger

System- og netværkssikkerhed

Systemer og netværk sikres ved at anvende sikre standarder for installation og konfiguration af nye aktiver. Når systemer er etableret, vedligeholdes og overvåges disse gennem nedenstående foranstaltninger.

- Der er implementeret dokumenterede driftsprocedurer for bla. backup, patch management og capacity management m.m.
- Der er implementeret systemer for malware beskyttelse
- Netværk er sikret og segmenteret for at begrænse adgange til det nødvendige.
- Der anvendes change management for at minimere fejl som følge af ændringer og installationer.
- Konfigurationer kontrolleres og overvåges for at sikre at krævede sikkerhedsindstillinger efterleves.
- Der er implementeret procedurer som sikrer at test- og udviklingssystemer er beskyttet på samme måde som produktionssystemer eller på anden måde ikke udgør en forøget risiko.
- Der anvendes kryptografi i kommunikation over åbne netværk eller efter specifik aftale med Miracle 42's kunder.

Applikationssikkerhed

Ved udførelse af udviklingsopgaver for interne systemer eller for kunder, har Miracle 42 implementeret en række foranstaltninger som minimerer risiko for brud på fortrolighed, integritet eller tilgængelighed.

- Adgang til kildekode er begrænset til kun at omfatte nødvendige udviklere
- Der er etableret procedurer for sikker udvikling gennem systemets livscyklus
- Der er defineret krav til applikationssikkerhed som er tilpasset de enkelte systemers kritikalitet
- Der anvendes code-review inden godkendelse af kode.
- Der anvendes procedurer som sikrer funktions- og sikkerhedstest efter releases
- Der er kontrakter og kontroller i de tilfælde udvikling outsources, som sikrer samme sikkerhed og test af kode.
- Hvor muligt anvendes der separate udviklings-, test- og produktionsmiljøer

Identitets- og adgangsstyring

Miracle 42 har implementeret foranstaltninger der sikrer kontrol med brugere, deres rettigheder til systemer, data og kundesystemer. Dette omfatter:

- Kontroller for fysisk og logiske adgange
- Sikre at identiteter er entydige i adgange til assets, infrastruktur og systemer.
- Medarbejdere er trænet i beskyttelse af autentifikations oplysninger.
- Der er etableret systemer der sikrer anvendelse af stærke kodeord, samt forhindrer at flere brugere kan anvende ens kodeord.
- Adgange styres som udgangspunkt gennem roller, hvilket sikrer at adgange som ikke er nødvendige fratages ved interne rotationer.
- Der er etableret procedurer som sikrer at tildeling af rettigheder skal godkendes inden de etableres.
- Privilegeret adgang tildeles kun til en bruger som er separat for medarbejderens daglige brugerkonto.
- Der er etableret periodisk kontrol for standard- og privilegerede brugere
- Der anvendes sikker autentifikation (MFA) for adgang til kritiske applikationer og til kundesystemer.

Trussels- og sårbarhedsstyring

Miracle 42 følger trusselsbilledet, med henblik på tilpasning af sikkerhedskontroller samt håndtering af sårbarheder.

- Miracle 42 følger og vurderer kontinuerligt leverandørernes sårbarheder
- Kritiske sårbarheder håndteres på Miracle 42's systemer, og der sker udmelding til kunder om anbefalet handling
- Miracle 42 følger trusselsbilledet fra samfundet gennem udmeldinger fra myndigheder eller nyheder i presse eller andre medier
- Sikkerhedshændelser analyseres i forhold til potentielt nye trusler
- Der udføres sårbarhedsscanninger for systemer, servere og applikationer på interne systemer, og for kundesystemer der tilkøber denne service

- Sårbarheder håndteres udfra en risikovurdering og mitigeres i videst muligt omfang.

Kontinuitet

Der er etableret en række foranstaltninger for at sikre data og systemers kontinuitet i tilfælde af kritiske incident.

- Infrastruktur, systemer og applikationer er konfigureret med det niveau af redundans der er aftalt med kunden
- Der er etableret beredskabsplaner for håndtering af ekstraordinære kritiske incidents
- Der er etableret beredskabsplaner for Miracle 42's kritiske systemer og services
- Kapacitet i infrastruktur og storage kontrolleres og udvides løbende for at undgå driftsstop
- Der foretages backup af systemer og data, og backup data sikres bedst muligt mod kompromittering
- Der er etableret procedurer for restore af systemer, data og applikationer
- Der udføres restore test for at afprøve medarbejdere, procedurer og backup system

Leverandørsikkerhed

Der anvendes leverandører og underdatabehandlere til levering services til kunder. Miracle 42 stiller krav til leverandører og underdatabehandlere, for at minimere risikoen for sikkerhedshændelser gennem leverandører.

- Leverandører forpligter sig til at overholde sikkerhedsretningslinjer fra Miracle 42 som en del af kontrakten der indgås
- Miracle 42 anvender leverandører og underdatabehandlere, der har tilstrækkelige foranstaltninger for sikkerheden i deres produkter eller leverance
- Miracle 42 fører tilsyn med leverandører og følger op på hændelser ved leverandører
- Miracle 42 sikrer cloudleverandører forpligter sig til at slette data efter endt kundeforhold

Overensstemmelse

Miracle 42's Legal and compliance funktion tilsikrer overholdelse af lovmæssige og kontraktuelle forhold. Herunder også koncernens overholdelse af politikker og principles and rules. Dette omfatter bla.

- Planlægge og udføre Interne audits
- Sikre at der udføres eksterne uafhængige audits
- Planlægge og håndtere audit fra kunder

Styring af informationssikkerhedshændelser

Der er sikret foranstaltninger for at styre sikkerhedshændelser, med henblik på at minimere konsekvens af hændelsen. Der er implementeret procedurer for håndtering af informationssikkerhedshændelser, som omfatter:

- Overvågning og logning for identifikation af sikkerhedshændelser
- Vurdering og analyse af hændelsen
- Reaktion på hændelsen udfra sandsynlige scenarier
- Læring af sikkerhedshændelser med henblik på forbedringer
- Indsamling af bevismateriale ved en hændelse

- Rapportering til kunden og/eller myndigheder