2016

YoungCRM Sikkerhedsprocedurer

GÆLDENDE FRA: 21. OKTOBER 2016

REBSDORF

Drifts- og sikkerhedsprocedurer

Dette dokument skitserer CompanYoung A/S drifts- og sikkerhedsprocedurer vedr. driften af YoungCRM. Dokumentet bruges til at sikre sikkerhedsprocedurerne i forbindelse med sikkerhedsbrister. Derudover vil der være 2 årlige sikkerhedstjek, for at sikre at procedurerne er tidsvarende og bliver overholdt.

Indholdsfortegnelse

Drift

Backup & sikkerhedskopier

Der tages backup og sikkerhedskopier af database og filer, min. 5 gange dagligt, og backup placeres redundant i 3 forskellige datacentre placeret hhv. i Europa, Asien og USA (via Amazon Web Services).

Vedligehold

System vedligeholdes og udvikles løbende. Bugs m.m. indberettes løbende

Standard vedrørende systemfejl:

- Når en medarbejder bliver bekendt med en fejl skal denne indberettes så snart denne bliver opdaget (indberetningen sker via GitHub).
- Fejlen skal kategoriseres iht. fejlkategorier beskrevet i YoungCRM Service Level Agreement. Ved critical sker dette dagligt. Ved mindre kritiske issues, prioriteres og planlægges disse ugentligt.
- Kritiske fejl forsøges såvidt muligt løst indenfor samme dag. Mindre kritiske fejl ved en af de næstkommende to releases.
- Nye releases lanceres hver tirsdag i tidsrummet kl. 15.00 – 17.00.

Overvågning

Systemet overvåges løbende. Der udarbejdes månedlige statusrapporter på systemet oppetid, som behandles af systemansvarlige og projektansvarlig.

Herudover overvåges systemet dagligt for eventuelle udsving i performance på servere og alle tilknyttede services.

Systemansvarlig modtager notifikationer ved særlige udsving, således en eventuel afhjælpning kan igangsættes med det samme. Dette gælder følgende:

- Servernedbrud
- Systemnedbrud
- Usædvanlig lang svartid
- Systemfejl
- Spikes i performance/forbrug på servere

Systemet overvåges bl.a. ved hjælpe af følgende værktøjer:

- AWS (Amazon Web Services)
- Statuscake
- Sentry
- New Relic

Hackerangreb og anden ulovlig indtrængning

Fysisk sikkerhed

Dette punkt omfatter standarder og procedurer, for hvordan vi sikrer at eksterne ikke har adgang til data i YoungCRM.

Den fysiske adgang til systemet er begrænset således kun tilladte computerer (personale) har adgang til kildekode og database. Kun specifikke medarbejdere er godkendt til at tilgå kildekode og database, og dermed tilgå data og filer.

Standard for adgang til systemet:

- Medarbejder skal være godkendt til at have adgang til systemet
- Al aktivitet skal logges (adgang til filer, databaser m.m.)
- Adgangskoder til hhv. PC, FTP, m.m. skal opdateres kvartalesvis, hvor der ikke anvendes two-factor authentication.

Procedure ved konstateret fysisk breach:

1. Tilføj "Vi oplever driftsproblemer – vi er på sagen" som servicebesked i systemet.
2. Gennemgå logs, og find ud af fra hvilken PC der er skaffet adgang fra
3. Evt. Roll back, eller re-launch ved genetableret sikkerhedsniveau
4. Afhjælp fejlen (luk PC'ens/devicets adgang)
5. Redefiner standarder for adgang til computeren.
6. Kommuniker episoden ud i HelpCenter (og ved længere nedbrud via mail).
7. Foretag sikkerhedsopdatering (opdater samtlige passwords).

Teknologisk sikkerhed

Systemet lever op til de mest gængse og tidssvarende krav til sikkerheden på større SaaS-løsninger.

Standard for teknologisk sikkerhed:

- **Sikker kommunikation (bruger grænseflade)**
  Kunden får aldrig direkte adgang til filer eller databaser
  Kommunikationen mellem bruger og YoungCRM er krypteret og beskyttet med TLS-teknologi. Beskyttelsen forhindrer Man-in-the-middle angreb hvor hackere kan opsnuse data imellem server og brugere.

- **Minimum af yderside der kan angribes**
  YoungCRM-domænet peger ned på vores Elastic Load Balancer (ELB), som sender kommunikationen videre til vore servere. De tilgængelige porte er 80 (http) og 443 (https). Port 80 bruges udelukkende til omdiregering til vores sikre forbindelse over port 443.
  Udover vores hovedservere har vi også en realtidsserver. Den har kun åbent for port 8080. Realtidsserveren bruges til direkte kommunikation til brugere af YoungCRM. Den har ikke adgang til YoungCRM data.
  Alt kommunikation mellem servere foregår på et undernet som ikke kan tilgåes udefra.

- **Særlig kryptering af CPR numre**
  CPR numre krypteres ydereligere, kan adgang hertil skal tildeles til den specifikke bruger, således dette er synligt i brugergrænseflade. Denne adgang kan kun tildeles af en CompanYoung medarbejder på kundens opfordring.

- **Sikker kommunikation (back end og systemadgang)**

For at få adgang til YoungCRMs servere, skal man bruge en nøgle som er krypteret. Desuden er kommunikationen låst til CompanYoungs IP.

- **Database**
  YoungCRM bruger MySQL som database lagt på en Amazon RDS. RDS'en sørger for løbende sikkerhedskopiering og versionering. Vores database er såkaldt Multi A-Z database, som er spredt på flere zoner. Dvs. at hvis en zone går ned, så kan dataene stadig tilgås idet de er i replikeret i andre zoner.

- **Filer**
  YoungCRM anvender Amazon Simple Storage Service (S3) til sikkerhedskopiering af alle systemfiler samt brugerfiler. Disse data sikkerhedskopieres minimum hvert 5. Minut med 99,99999 % dataholdbarhed.

- **DDoS-modforanstaltninger**
  Vores serverne logger alle forbindelser og ser noget mistænkeligt ud, kommer IP'en i karantæne. Desuden benytter vi AWS' indbyggede DdoS-beskyttelse.

Procedure ved teknologisk breach (hackerangreb):

1. Tilføj "Vi oplever driftsproblemer – vi er på sagen" som servicebesked i systemet.
2. Gennemgå logs, og find ud af hvor hullet findes
3. Udbedre fejlen (opdatering af system)
4. Evt. Roll back, eller re-launch ved genetableret sikkerhedsniveau
5. Redefiner sikkerhedsstandarder
6. Kommuniker episoden ud i HelpCenter (og ved længere nedbrug via mail).
7. Foretag sikkerhedsopdatering (opdater samtlige passwords).

Bortkomst af udstyr

Bortkommer en medarbejders udstyr med eventuel adgang til kritisk indhold, herunder filer, data, dokumentation eller loginoplysninger, træder visse procedurer i kraft.

Procedure ved bortkomst af udstyr:

1. Samtlige kodeord (loginoplysninger) vedr. systemet og eventuelle affilieret systemer skiftes.
2. Adgange til udstyret forsøges slettes via fjernstyring.
3. Er udstyret blevet stjålet politianmeldes dette

Intern adgang til systemet

Personale og enheder med adgang til systemet

Den fysiske adgang til systemet er begrænset således kun tilladte computerer (personale) har adgang til kildekode og database. Kun specifikke medarbejdere er godkendt til at tilgå kildekode og database, og dermed tilgå data og filer.

Herudover er der krav til hvilke enheder og hvorfra man må tilgå systemet.

Standard for adgang til systemet:

- Medarbejderen skal være godkendt til at tilgå systemet, og har underskrevet en erklæring omkring brugen heraf.
- Enheden systemet tilgås igennem skal være godkendt
- Medarbejderen skal skifte sine loginoplysninger minimum én gang i kvartalet
- Al aktivitet skal logges (person, handling, enhed)
- Medarbejderen SKAL gøre opmærksom på hvis en enhed er mistet eller enheden tænkes at være inficeret med malware, virus eller tilsvarende.

Listen over personer og enheder kan udleveres hvis nødvendigt.

Intern misbrug af systemet

Adgangen til systemet er begrænset til enkelte medarbejdere, som kun må tilgå systemet i professionelt øjemed. Herunder findes reglerne for tilgang til systemet og konsekvensen ved brud heraf.

Standard for adgang til systemet:

- Medarbejder skal være godkendt til at have adgang til systemet
- Al aktivitet skal logges (adgang til filer, databaser m.m.)
- Adgangskoder til hhv. PC, FTP, m.m. skal opdateres kvartalsvis.
- Adgangen til systemet må på ingen måde anvendes til private formål
- Medarbejderen må ikke dele hele eller dele af dataen eller kildekoden internt eller eksternt, uden tilladelse.
- Medarbejderen må ikke tilgå systemet fra enheder der ikke er godkendt hertil.
- Medarbejderen skal oplyse hvis man har foretaget forkert brug af systemet
- Medarbejderen skal låse sin enhed når den forlades
- Enheden SKAL være beskyttet med kodeord

Procedure ved konstatering af en medarbejders misbrug af systemet:

1. Vurder om der er sket skade på systemet, og hvorvidt det skal lukkes ned.
2. Vurder omfanget af misbruget
3. Suspender medarbejderen og luk pågældende ud af systemet
4. Foretag intern undersøgelse af misbruget og vurder konsekvenserne.
5. Eventuelt redefinering af sikkerhedsstandarderne.
6. Kommuniker episoden ud i HelpCenter (og ved længere nedbrud via mail).

Ved misbrug af systemet kan den pågældende medarbejders ansættelsesforhold ophøre.

Erhvervsmæssige spionage

Systemet og dets beskaffenhed er strengt fortroligt, og må ikke deles eksternt.

Standard for erhvervsmæssige spionage:

- Medarbejderen må ikke dele hele eller dele af dataen eller kildekoden internt eller eksternt, uden tilladelse.

- Medarbejderen må ikke give andre personer, der ikke er godkendt, adgang til systemet.

Procedure ved konstatering af erhvervsmæssige spionage:

1. Vurder om der er sket skade på systemet, og hvorvidt det skal lukkes ned.
2. Vurder omfanget af spionage, og hvad der er blevet delt og til hvem
3. Suspender medarbejderen og luk pågældende ud af systemet
4. Foretag intern undersøgelse af spionagen og vurder konsekvenserne.
5. Eventuelt redefinering af sikkerhedsstandarderne.
6. Kommuniker episoden ud i HelpCenter (og ved længere nedbrud via mail).

Ved gentagende overtrædelse af standarderne vedr. erhvervsmæssige spionage vil den pågældende medarbejders ansættelsesforhold blive taget op til overvejelser.

Fysisk adgang til systemet

Enheder med tilgang til systemet skal være beskyttet så adgangen hertil er så sikker som muligt.

Standarder:

- Enheder på arbejdspladen skal være beskyttet med password
- Enheder på arbejdspladsen skal være låst fysisk inde om natten
- Mistes en enhed skal dette meldes så snart tabet opdages
- Two-factor authentication anvendes hvor det er muligt

Procedure ved overtrædelse:

1. Vurder om der er sket skade på systemet, og hvorvidt det skal lukkes ned.
2. Vurder hvorvidt andre procedurer skal træde i kraft (eks. bortkomst af udstyr)
3. Påtal medarbejderens manglende overholdelse af standarderne
4. Eventuelt redefinering af sikkerhedsstandarderne.
5. Fjernes fra two-factor authentication

Tyveri af data / software / hardware

I tilfælde af at en medarbejder stjæler data

Standard for tyveri (følgende anses for tyveri):

- Medarbejderen må ikke hente systemet fysisk ned på en enhed medmindre der er givet tilladelse hertil. Dette gælder for USB-lagerenheder, computere, mobile enheder og tilsvarende.
- Medarbejderen må ikke give andre personer, der ikke er godkendt, adgang til systemet.
- Medarbejderen må ikke fjerne en enhed fra arbejdspladsen, medmindre der er givet tilladelse hertil.
- Medarbejderen må ikke anvende private enheder til at tilgå systemet.
- Medarbejderen må ikke lade andre tilgå de enheder der tilgår systemet.

Procedure ved konstatering af tyveri:

1. Vurder om der er sket skade på systemet, og hvorvidt det skal lukkes ned.
2. Vurder omfanget af tyveriet
3. Suspender medarbejderen og luk pågældende ud af systemet
4. Foretag intern undersøgelse af tyveriet og vurder konsekvenserne.
5. Eventuelt redefinering af sikkerhedsstandarderne.
6. Kommuniker episoden ud i HelpCenter (og ved længere nedbrud via mail).

Ved misbrug af systemet kan den pågældende medarbejders ansættelsesforhold ophøre.

Organisering

Ansvarsforhold og roller

Der findes en række forskellige ansvarsforhold og roller vedr. drift af systemet, samt hvilke rettigheder/tilladelser man har.

Systemansvarlig

Den systemansvarlige er ansvarlig for at systemets sikkerhed bliver overholdt

Projektansvarlig

Det er Projektansvarligs ansvar at sikkerhedsprocedurer ajourføres minimum én gang årligt. Det er desuden den systemansvarliges opgave at tjekke sikkerhedsproceduren minimum to gange årligt.

Log for hver systemtjek skal føres.

Fratrådte medarbejdere

Ved fratrådt medarbejder gennemføres en sikkerhedsopdatering som involverer:

- Opdatering af samtlige passwords (adgange, software, brugere, servere m.m.)
- Fjernelse af alle adgange til systemet
- Tilbagekaldelse af fysiske enheder
- Undersøge medarbejderens berøringsflade med henblik på komplet sikkerhedsgennemgang
- Gennemførelse af CompanYoungs generelle offboarding-procedurer.

Godkendelser

Følgende personer og enheder er godkendt til at tilgå systemet:

Systemadgang

Systemadgang er adgang til alle facetter af systemet, herunder servere, databaser, filer + administratoradgange til de understøttende 3. Parts leverandører.

Thomas Bolander

Godkendelse givet: 01.01.2016
Titel: Senior Developer (+ Systemansvarlig)
Enheder:

- Arbejds Stationær PC (Vestre Havnepromenade 1B, 3. Sal)
- Macbook (bærbar computer)

Kevin Rebsdorf

Godkendelse givet: 01.01.2016
Titel: CEO (+ Projektansvarlig)
Enheder:

- iMac (hjemmecomputer)
- Macbook (bærbar computer)

Kristian Vassard

Godkendelse givet: 01.01.2016
Titel: Developer
Enheder:

- Arbejds stationær PC (Vestre Havnepromenade 1B, 3. Sal)
- Macbook (bærbar)

Erik Carrillo

Godkendelse givet: 01.01.2016
Titel: Head of Customer Care
Enheder:

- PC (hjemmecomputer)
- Macbook (bærbar computer)

Camilla Christensen

Godkendelse givet: 01.01.2016
Titel: Customer Care Specialist
Enheder:

- Macbook (bærbar computer)

CompanYoung Admin-rettigheder

Med en CompanYoung admin-rettighed, har du mulighed for at tilgå alle organisationer i YoungCRM. Dermed har disse personer mulighed for at tilgå alt data indsamlet via YoungCRM, men ikke til selve kodebasen m.m. som personer med Systemadgang.

Anders Bøegh
Godkendelse givet: 01.01.2016
Titel: Head of Delivery

Morten Kyvsgaard
Godkendelse givet: 01.01.2016
Titel: Digital Media Specialist

Daniel Birkholm
Godkendelse givet: 01.01.2016
Titel: CCO