Systembeskrivelse

Whistleblower Software

I dette dokument præsenterer vi kort, hvad systemet kan og gør, så du kan føle dig tryg i at vælge os som din samarbejdspartner. Bemærk at systembeskrivelsen er et øjebliksbillede, og at vi kontinuerligt tilbyder ny funktionalitet til gavn for dig, dine kollegaer og potentielle whistleblowere.

“Vi skal hele tiden udvikle os og sørge for, at systemet lever op til de forventninger, vores kunder har i dag og i fremtiden. Vi vil være det rigtige valg for alle, der ønsker at drive gode whistleblowerordninger med fokus på transparens for whistlebloweren og it-sikkerhed i top.”

Ansvarlig for sikkerhed og produkt
CTO, Kristoffer Abell
Tlf.: +45 21 99 11 50
E mail: kab@whistleblowersoftware.com

Introduktion

Systemet er delt op i tre forskellige moduler:

1. Partner
2. Virksomhed
3. Whistleblower

Hver del af systemet opfylder hvert sit formål.

1: Partner

Dette modul kan kun tilgås af partnere/rådgivere. En rådgiver er en ekstern person, som hjælper virksomheder med at drive deres whistleblowerordninger.

Fra modulet har partneren adgang til at sætte indberetningskanaler op for virksomheder. Dertil giver modulet et overblik over alle de sager, som partneren har fået tildelt adgang til på tværs af indberetningskanalerne.

Partner modulet har blandt andet følgende funktionalitet:

- Inviter rådgivere ind i systemet
- Opret virksomhedskonti
- Tilgå virksomhedskonti
- Opsæt branding af partner virksomheden

2: Virksomhed

Virksomhedsmodulet er tilgængeligt for både partnere/ rådgivere samt virksomheden selv.

Følgende er muligt fra virksomhedsmodulet:

- Inviter brugere fra virksomheden, der skal være involveret i sagsbehandlingen.
- Lav indstillinger for adgangskontrol baseret på afdeling og kategori, der sikrer, at forskellige brugere har adgang til de rigtige data.
- Konfigurer whistleblower modulet med både tekst og visuel identitet.
- Kommuniker med whistleblower gennem en sikker chat.
- Anonymiser sager og videregiv adgang til anonymiseret indhold til de rigtige brugere.
- Se fuldstændig aktivitetslog for en sag og det behandlingsforløb, der har været.
- Slet sager.

- Opret en sag manuelt, hvis en sag er kommet ind via andre kanaler, såsom telefonopkald eller et fysisk møde.
- Konfigurer notifikationsindstillinger.

Vi har stort fokus på, at adgang til sager kun gives til de rigtige personer, der har et arbejdsbetinget behov for adgang. Derfor kan man som bruger i systemet ikke tilgå sager, medmindre man (1) eksplicit har fået tildelt adgang af en anden bruger med adgang, eller (2) er konfigureret til at modtage sagen, og whistlebloweren er blevet informeret i forbindelse med oprettelse af sagen om, at netop denne bruger vil få adgang.

3: Whistleblower

Whistleblowermodulet er tilgængeligt gennem et link, der er unikt for virksomheden. Virksomheden vælger selv, hvordan linket deles. Ofte vil det være i et link på deres hjemmeside, alternativt kan det fremgå af deres medarbejderhåndbog eller på et intranet.

Fra whistleblowermodulet er whistlebloweren i stand til følgende:

- Orientere sig i virksomhedens politikker og søge yderligere information stillet til rådighed af virksomheden.
- Indberette en ny sag. Dette gøres gennem en formular, der understøtter skriftlig beskrivelse såvel som mundtlig.
- Følge op på en tidligere oprettet sag vha. et unikt kodeord, der udleveres ved oprettelse af sagen. Herfra er det muligt at kommunikere med sagsbehandleren.

Systemet understøtter naturligvis både anonym og fortrolig indberetning.

Kort om sikkerhed

Brugersikkerhed

Ofte sker sikkerhedsbrud ikke pga. tekniske fejl, men pga. menneskelig fejl eller fysisk adgang. Systemet har en række foranstaltninger, der sikrer, at den rigtige person, der ønsker adgang til systemet, rent faktisk er den rette bruger. Det er f.eks. muligt at slå *to faktor godkendelse* til for alle brugere. Det betyder, at brugeren skal godkende sit login via en SMS, hver gang brugeren logger ind. På den måde sikrer vi, at der ikke sker adgang til data selvom brugerens kodeord afsløres.

Systemet har stort fokus på, at det skal være tydeligt, hvem der har adgang til hvad, så vi sikrer, at ingen har unødvendig adgang til fortrolig data.

Særlige tiltag for sikkerhed og anonymitet

- Mulighed for 100% anonymitet for whistleblowere
  Whistlebloweren afgør selv, om vedkommende vil tilkendegive sig. Uanset hvad der vælges, så opsamles der ikke yderligere informationer (såsom IP adresse) foruden dem, som whistlebloweren selv giver.

- Privacy by Design
  Vores udviklingsproces tager udgangspunkt i Privacy by Design, som består af en række klare principper for, hvordan man sikrer en høj sikkerhed omkring fortrolige data og sikkerhed generelt. Eksempelvis gennem såkaldte privatlivsfremmende teknologier (Privacy Enhancing Technologies PETs) og organisatoriske foranstaltninger.

- End to end kryptering
  Hvor mange konkurrenter ikke benytter end to end kryptering, skiller Whistleblower Software sig ud. Ved hjælp af avancerede krypteringsalgoritmer krypterer Whistleblower Software helt automatisk fortroligt sagsindhold, uden at det bemærkes fra brugerens/whistleblowerens synsvinkel. Dette medfører en usædvanligt høj sikkerhed, da intet data kan læses af en tredjepart, heller ikke af Whistleblower Softwares egne medarbejdere.

- *Sagsindhold kan nemt slettes i henhold til GDPR*
  Når en sag er færdigbehandlet, kan fortrolig data nemt slettes, således at der ikke sker behandling i længere tid end nødvendigt.

- Multifaktor godkendelse
  Det er i systemet muligt at benytte sig af to faktor godkendelse, hvor ens identitet, udover adgangskode ved login, skal bekræftes via SMS. Dette sikrer, at ingen uvedkommende kan tilgå systemet ved blot at have anskaffet sig en adgangskode.

- Begrænset adgang til sager
  Systemet giver som udgangspunkt ikke brugere adgang til alle sager. Der kan på sagsniveau gives adgang til enkeltpersoner, så det sikres, at alene autoriserede brugere kan tilgå den enkelte sag.

  Dette kan også gøres på kategoriniveau, så der ved oprettelse af nye sager automatisk gives adgang til bestemte personer, f.eks. at hvidvasksager alene tilgår til brugere i hvidvaskkategorien.

- Dataopbevaring inden for EU
  Al data opbevares inden for EU s grænser. Data opbevares i Frankfurt, Tyskland hos AWS (Amazon Web Services), hvor der via bl.a. Intrusion Detection, CCTV samt datacenterindgangspunkter sikres fysisk adgang til data. Endvidere er det muligt at få udleveret krypteringsnøglen, således at der ikke er adgang til data fra f.eks. USA.

Kryptering

Al data er krypteret *in transit* (når data transmitteres mellem computere) og *in rest* (det gemte data på selve harddisken. Dvs. at hvis harddisken bliver stjålet, er der alene adgang til krypteret data, der vil være ulæseligt).

Alt sagsindhold er yderligere krypteret. Denne kryptering leveres i to former:

1. Whistleblower Software genererer og holder styr på RSA /AES krypteringsnøgler.
2. Kunden genererer (med hjælp fra os) sine egne RSA /AES krypteringsnøgler, hvorefter vi kun modtager public RSA krypteringsnøglen. Dermed kan medarbejdere hos Whistleblower Software ikke læse dataene (bedre kendt som end to end kryptering).

Dataopbevaring

Der bliver ikke repliceret data til andre fysiske datacentre. Dataene replikeres til flere harddiske i Frankfurt i forskellige "availability zones", som egentlig bare betyder forskellige afdelinger i et datacenter, som hver har deres separate internet og strømforbindelse.

Backup

Daglig backup som udløber efter 5 uger
Ugentlig backup som udløber efter 3 måneder
Månedlig backup som udløber efter 5 år

Da der dagligt foretages en backup, kan der maksimalt mistes 24 timers data.

Logging

Der foretages logning af forskellige hændelser i systemet. Nogle af disse hændelser er:

Hvilke medarbejdere, der tilgår hvilke sager, hvornår og hvorfra.
Hvilke medarbejdere, der har oprettet eller opdateret en bruger eller en sag.

Nogle af disse informationer kan ses direkte fra systemet, andre kan fremskaffes ved anmodning.

Intrusion detection

Whistleblower Software benytter sig af to forskellige slags intrusion detections:

(1) Fysisk intrusion detection, som dækker over den fysiske adgang til datacentret, hvori platforms data opbevares (administreres af AWS).

(2) Network intrusion detection, som overvåger bl.a.:

Flow logs af trafik, som løber rundt i vores lukkede VPC.
DNS logs.

Logs på brug af AWS CLI, SDK, API og management console.

Løbende opdatering/patchning af standard-software

Hos Whistleblower Software prøver vi så vidt som muligt kun at bruge AWS administrerede tjenester, hvilket sikrer høj tilgængelighed og meget sikre tjenester. Imidlertid har ikke alle tjenester muligheden for at blive administreret af AWS.

Tredjepartspakker overvåges automatisk og kontinuerligt for nye sårbarheder, der er blevet opdaget. Når en pakke markeres med en sårbarhed, så opdateres den hurtigst muligt.

Tracking

Der trackes/opsamles ingen oplysninger om whistlebloweren udover den information, som vedkommende selv oplyser.

Whistleblower Software ApS har sat sig for at bygge den bedste whistleblowersoftware løsning på markedet. Sikkerhed og beskyttelse af fortrolige oplysninger er essentielt for alle med en whistleblower løsning og derfor en af grundstenene i systemet.

Har du spørgsmål til sikkerheden, er du altid velkommen til at kontakte vores CTO Kristoffer Abell på Tlf.: +45 21 99 11 50 E mail: kab@whistleblowersoftware.com