





pindena
påmeldingssystem



Sikkerhet i Pindena påmeldingssystem

Sist endret dato: 23.06.2026

Innhold

Innhold **2**
1. Om dokumentet **3**
2. Definisjoner **3**
3. Sikkerhet på klientsiden **3**
4. Sikkerhetstiltak i infrastruktur **3**
4.1. Server 3
4.1.1. Amazon Web Services 3
4.1.2. Deploi AS 4
4.2. Nettverk 4
4.3. Brannmur 4
4.4. Backup 4
4.5. Fysisk sikring 4
4.6. Kryptering 5
4.6.1. Data i ro (at rest) 5
4.6.2. Data som overføres (in transit) 5
4.7. E-post 5
5. Sikkerhetstiltak i koden **5**
5.1. Innebygde tiltak 5
5.1.1. Laravel 5
5.1.2. Databasetilgang 6
5.1.3. Rolletilgang 6
5.1.4. Forebygge øktkapring 6
5.1.5. Logging 6
5.2. Innstillinger i systemet for systemadministrator 6
5.3. Funksjoner for brukere 7
6. Organisatoriske sikkerhetstiltak **7**

1.Om dokumentet

Dette dokumentet beskriver hvordan sikkerhet er håndtert i Pindena. Dokumentet beskriver sikkerhetstiltak i detalj, både for infrastruktur, kode og organisatorisk.

Dette dokumentet brukes også som vedlegg til Databehandleravtale.

2.Definisjoner

Kunden er organisasjonen som har kjøpt tilgang til påmeldingssystemet, representert ved en eller flere personer som har beslutningsmyndighet på vegne av Kunden.
Brukeren er en ansatt hos Kunden som har administratortilgang til påmeldingssystemet.
Registrert er en som har blitt registrert i påmeldingssystemet.

3.Sikkerhet på klientsiden

Krypterte forbindelser og sikkerhet i programvaren på serversiden hjelper ikke hvis man har virus/trojanere eller andre sikkerhetshull på sin egen PC. Sikkerheten begynner på den siden brukeren sitter. Brukernavnet og passordet brukeren mottar er personlig – som bruker bør du ikke gi det til andre, og huske å endre passord etter du har logget inn.

4.Sikkerhetstiltak i infrastruktur

4.1.Server

Alle webservere er konfigurert med Laravel Forge og bruker nyeste LTS-versjon av operativsystemet Ubuntu, for tiden versjon 20.04 LTS.

Laravel Forge har følgende sikkerhetstiltak på hver server:

- Automatisk daglige sikkerhetsoppdateringer (innebygget i Ubuntu).
- Bare nøkkelbasert innlogging, ikke med passord.
- Unikt root-passord på hver server.
- Se også 4.3. Brannmur.

4.1.1.Amazon Web Services

Hos Amazon har vi servere i Stockholm, Sverige. Her bruker vi EC2 som webserver, med databaser i RDS og opplastede filer i S3.

Se også https://docs.aws.amazon.com/security/, for videre informasjon om de tre tjenestene som benyttes (EC2, RDS, S3).

4.1.2. Deploi AS

Vi bruker Dedikert Virtuell Server fra Deploi som er plassert i datasenter i Oslo, med databaser og opplastede filer på samme server.

Se også https://deploi.no/virtuell-server/.

4.2. Nettverk

Amazon og Deploi har redundant internett, altså (minst) to internettlinjer koblet til hver server.

4.3. Brannmur

Laravel Forge sørger for at alle porter på webserverne blokkeres i utgangspunktet, men åpner eksplisitt portene for SSH, HTTP og HTTPS.

Alle Amazon-tjenestene er i tillegg plassert i en felles VPC (Virtual Private Cloud) med en Security Group som sørger for at webserverne (EC2) kan koble seg til databaseserverne (RDS).

4.4. Backup

Databehandler tar daglig backup av alle serverne og databaser. På norsk server tas det også backup av filer som lastes opp i systemet. Vi bruker leverandørenes backup-system, som også har funksjoner for gjenoppretting etter hendelser, på alle serverne.

Se også https://aws.amazon.com/backup/ og https://deploi.no/backup/.

4.5. Fysisk sikring

Server-leverandørene har mange tiltak for fysisk sikring, blant annet:

- Låssystemer med tilgang for et begrenset antall personer.
- Brannsikring med varsling og brannhemmende tiltak.
- Avbruddsfri strømforsyning og dieselaggregat for reservestrøm.
- Temperatur- og fuktkontroll.
- og mye mer.

Se også https://aws.amazon.com/compliance/data-center/ og https://deploi.no/datasenter/.

Pindenas kontorlokaler er sikret med låssystemer som krever adgangskort hele døgnet og kode utenfor arbeidstiden. Det er først en kontroll på ytterdørene til lokalene utenfor vanlig arbeidstid (8-16). Deretter er det kontroll for å komme seg inn i Pindena kontoret sin dør. For å komme seg gjennom kontrollen kreves det eget personifisert adgangskort.

Ansattes pc er sikret med passord og automatisk låsing når man går fra maskinen.

4.6. Kryptering

4.6.1. Data i ro (at rest)

Pindena bruker server-side kryptering på våre databaser i Amazon RDS og på filer som lastes opp til Amazon S3. Krypteringsnøkkelen er generert og lagret i Amazon KMS (Key Management Service).

På Deploi-servere krypterer vi ikke databaser eller filer.

4.6.2. Data som overføres (in transit)

Pindena bruker https på alle installasjoner for å kryptere trafikken mellom nettleser og server. På de fleste servere tillater vi bare TLS1.3, men noen av de eldre har også TLS1.2.

SMS som sendes med Vianett (Link Mobility) krypteres ikke.
E-post sendt via Make er kryptert med TLS.

4.7. E-post

Via både Amazon og Deploi servere sender vi e-post via vårt Make-abonnement med dedikert IP-adresse.

Dersom Brukeren har definert at et felt kan inneholde sensitive data blir ikke dette feltet tatt med i e-postbekreftelser, og dermed ikke sendt på e-post.

5. Sikkerhetstiltak i koden

5.1. Innebygde tiltak

Dette kapittelet beskriver sikkerhetstiltak vi har bygget inn i koden for å gi best mulig sikkerhet mot angrep og brukerfeil. Hos Pindena utvikles kode med krav om å ivareta personvern i koding, og alle steg. Fra skriving av kravspesifikasjon til koding til testing er informasjonssikkerheten og personvern i fokus.

5.1.1. Laravel

Pindena bruker rammeverket Laravel og funksjoner som gir beskyttelse mot tre typer angrep:

- Eloquent ORM og Query Builder beskytter mot ”SQL Injection attack”.
- Escaping av data som skal presenteres på nettsiden beskytter mot ”XSS attack” (Cross Site Scripting).
- CSRF token med tilhørende sjekk beskytter mot “CSRF attack” (Cross-Site Request Forgery).

5.1.2. Databasetilgang

Hver kundeinstallasjon har en egen database, og kobler til med en egen databasebruker som bare har tilgang til den databasen.

5.1.3. Rolletilgang

Hver Bruker i systemet har en definert rolle. Hver rolle kontrollerer følgende elementer i administratordelen av påmeldingssystemet:

- Hvilke sider Brukeren kan se.
- Hvilke menyelementer Brukeren kan se.
- Hvilke funksjoner Brukeren kan utføre (klikk på knapper som endrer data etc).

Sidene for Registrerte er åpne og tilgjengelige for alle, men Brukeren kan velge å begrense tilgangen, se punkt 5.3. Skjema for Registrerte er satt opp med reCAPTCHA for å begrense spam registreringer, dette kan Brukeren velge å fjerne fra skjema om behov.

5.1.4. Forebygge øktkapring

Følgende er gjort for å forebygge øktkapring (session hijacking):

- Session tidsavbrudd ved inaktivitet (session utløper etter to timer med inaktivitet, og Bruker blir logget ut).
- Bytte av session cookie-id ved pålogging for å hindre ”session fixation”.

5.1.5. Logging

Logger brukes for sporing i tilfelle angrep. Følgende logger finnes:

- System-logger på server.
- Brukslogg i webserver. Logger hva som har skjedd i webserver
- Feil-logger i webserver og Laravel.

Vi logger også bruker-id og tidspunkt for når en record ble opprettet og når den sist ble endret i de fleste databasetabellene. Logger avhenger av aktivitet og kan derfor være i lengre tid, men vanlig er 14 dager basert på bruk.

5.2. Innstillinger i systemet for systemadministrator

Dette kapittelet beskriver sikkerhetsinnstillinger som Kunden kan gjøre selv, eller be Pindena om å gjøre.

Kunden kan definere:

- Definere link til side for personvernerklæring, som vil bli vist sammen med reservert felt for samtykke.
- Definere hvor lang tid deltagerinformasjon skal være lagret etter at aktiviteten er ferdig. Deretter vil det bli slettet fra Pindena Påmeldingssystem og så fra databasen.

- Definere hvor lang tid sensitive data skal være lagret etter at aktiviteten er ferdig. Deretter vil det bli slettet fra Pindena Påmeldingssystem, også i databasen.
- Velge å holde aktivitetslisten skjult for de som ikke er innlogget som brukere.
- Aktivere SSO med Azure-AD som sikker innlogging for brukerne.

5.3. Funksjoner for brukere

Når brukeren oppretter aktiviteter/arrangement er det flere valg den personen kan gjøre for å øke informasjonssikkerheten.

Dette kapittelet beskriver sikkerhetsinnstillinger som Brukeren kan gjøre selv.

Brukeren kan:

- Aktivere to-faktor autentisering som innlogging på sin bruker
- Definere om det er, og hvilke, felt i skjemaet som kan inneholde sensitive data.
  Informasjon i disse feltene vil ikke bli sendt ut i epostbekreftelse.
  Informasjonen blir slettet fra løsningen kort tid etter at aktiviteten er ferdig, hvis Kunden har aktivert funksjonen.
- Aktivere reservert felt for samtykke med link til side for personvern.
- Begrense tilgangen så bare inviterte kan melde seg på.
- Begrense tilgangen så bare inviterte kan se innholdet i en aktivitet.
- Begrense tilgangen ved å kreve SMS-verifisering.
- Begrense visningen av aktiviteten på aktivitetslisten.
- Begrense tilgangen så man kan kun melde seg på hvis man har deltatt og bestått på en aktivitet med et oppsatt stikkord fra før av.

6. Organisatoriske sikkerhetstiltak

Dette kapittelet beskriver hvordan Pindena er organisert med tanke på sikkerhet, og hvilke prosesser og tjenester vi har gående.

- Begrenset antall personer har tilgang til kundedata.
  Det er bare support- og driftspersonell som har mulighet til å logge inn i kundens installasjon og se personopplysninger. Dette gjøres bare ved behov, f. eks. når kunden trenger hjelp av support.
- Pindena sletter alle kundens data tidligst 2 uker etter, senest 90 dager, ved oppsigelse, med mindre annet er avtalt.
- Ekstern overvåking og varsling.
  Pindena har en server utenfor produksjonsmiljøene som sjekker at alle kunde-serverne er i live og svarer riktig på forespørsel. Når en server ikke svarer (riktig) over litt tid så varsles driftspersonell på SMS. En ny SMS sendes når serveren svarer riktig igjen.
- Intern overvåking og varsling.
  På hver server overvåkes CPU-, minne- og diskbruk. Når grensene overskrides sendes en e-post til driftspersonell. En ny e-post sendes når serveren er under grensene igjen.

- Sårbarhetsskanning / Penetrasjonstesting.
  Pindena har et abonnement på en tjeneste som leter etter sikkerhetshull i systemet og varsler oss hvis den finner noe. Denne skannen kjøres også ved hver nye release.