Säkerhet

Med Boardeasers molntjänster kan er styrelse tryggt hantera säkerhetsklassad och affärskritisk information. Plattformen är byggd på modern och välbeprövad teknik – en radintegrerade funktioner och rutiner säkerställer en mycket hög säkerhetsnivå.

Detta dokument behandlar följande:

- Applikationssäkerhet
- Infrastruktur
- Internt säkerhetsarbete

Allmänt

Boardeaser är en molntjänst för styrelsearbete, rapportering, management och governance.Det innebär att plattformen hanterar en organisations mest känsliga data.

Kunder med högsta krav på säkerhet

Bland Boardeasers kunder finns organisationer som kräver högsta säkerhetsnivå, däriblandbanker, börsnoterade bolag, forskningsbolag och advokatbyråer. Plattformen är många gånger säkrare än traditionell hantering av pappersdokument, e-postkorrespondens och enkla lagringsplatser för data. I Boardeaser är säkerhetsaspekten en grundsten.

Säkerhetsfunktioner – ett urval

- ✓ All kommunikation är krypterad
- ✓ Alla dokument lagras säkert
- ✓ Krypterad tvåfaktorsinloggning med stöd för BankID och YubiKey
- ✓ Drift och applikationer körs på AWS och Heroku (allt inom EU) med all deras säkerhetoch driftstabilitet
- ✓ Plattformen är GDPR compliant
- ✓ Löpande säkerhet med automatiska penetrationstester varje vecka
- ✓ Oberoende konsulter anlitats för due diligence av säkerhet
- ✓ All personal har sekretessavtal och får löpande säkerhetsutbildning
- ✓ Boardeasers anställda har inte åtkomst till kunds information utan aktivt medgivande

Applikationssäkerhet

All datatrafik till och från Boardeasers användare krypteras, så även uppladdade dokument.Inloggning sker med tvåfaktorsautentisering via BankID och Yubikey.

Krypterad trafik

All data till och från användaren krypteras med https.

Krypterad lagring

All kunddata är krypterad med AES-256. Nyckeln ligger på separat server och säkerhetszon(DMZ).

Inloggningsmetod

Inloggning sker med användarnamn och lösenord.

BankID

Boardeaser stöder inloggning med BankID för alla nordiska länder.

Tvåfaktorsautentisering

Boardeaser erbjuder tvåfaktorsinloggning och autentisering. En styrelse kan också kräva attalla användare använder tvåfaktorsautentisering.

Yubikey

Boardeaser stöder och rekommenderar Yubikey hårdvarunycklar för inloggning. Yubikeyanvänds av alla större mjukvaruföretag internt, t.ex. Google och Facebook.

Inloggnings- och aktivitetlogg

Alla inloggningar och aktiviteter i Boardeaser loggas.

Analys av inloggningsförsök

Alla inloggningsförsök analyseras. Misstänks ovanlig aktivitet larmar Boardeaser omgåendeoch blockerar inloggningen tills analys är färdigställd.

Inloggning på annan ort eller enhet

Boardeaser analyserar inloggning och varnar för ovanlig inloggning på ny ort och ellerenhet, användaren notifieras.

Behörighet

Användare av Boardeaser kan ges olika behörighetsnivåer och tillgång till data. Användarekan tilldelas roller som ger tillgång till valda delar av systemet och dess data.

Visstidsbehörighet

Boardeaser har integrerad funktion för att ge tillgång till data under en begränsad tid, t.ex. åtsupport eller konsulter.

Notifieringar och e-post till användare

Användargenererad information skickas aldrig ut från Boardeaser utan användarens godkännande. E-post från systemet innehåller länkar till den information som ska delges, föratt se informationen krävs inloggning. Samtliga styrelsemöten, beslut, att-göra-uppgifter etc.kodas med nummer och länk.

GDPR

Boardeaser är GDPR compliant.

Infrastruktur

Boardeaser använder världens största leverantör av datainfrastruktur; Amazon Web Services och samt plattformen Heroku. Leverantörerna säkerställer tillgänglighet, backuper,uppdateringar, övervakning 24/7, brandväggar, säkerhetszoner och stora delar av säkerhetsuppföljningen. Därutöver använder Boardeaser ett antal andra leverantörer samt egenutvecklade funktioner för automatiserad och manuell säkerhetsuppföljning.

Informationshantering och lagring

I Boardeaser finns organisationens information lagrad, den är korrekt (ej förändrad) och äralltid tillgänglig.

AWS – Amazon Web Services

Boardeaser använder infrastrukturen AWS, som erbjuder industriledande tillförlitlighet, skalbarhet och säkerhet. Genom att använda AWS minimeras stillestånd och påverkan påkunders tillgänglighet. AWS är en Infrastructure as a Service (IaaS). Allt lagras inom EU.

Läs mer på Amazon.com: https://aws.amazon.com/about-aws/global-infrastructure/

Heroku

Heroku är en av världens största PaaS (Platform as a Service). Heroku sköter redundans, uppgradering, backup och övervakning av databaser, operativsystem, brandväggar, etc. Heroku garanterar att all data är helt separerad från annan kundsdata. Allt inom EU.

Läs mer på Heroku.com: https://www.heroku.com/policy/security

Fillagring

För fillagring används AWS S3 och allt krypteras. Krypteringsnyckeln lagras på annan serveroch säkerhetszon. Allt inom EU.

Automatiska penetrationstest

Penetrationstester utförs automatiskt varje vecka. Boardeaser använder automatiska pen-tester från flera olika leverantörer.

Manuella penetrationstest

Säkerhetskonsulter (tredjepart) gör kontinuerligt manuella säkerhets- samt penetrationstest.

Säkert OS, mjukvara och hårdvara

Heroku och AWS säkerställer att Boardeaser alltid har den säkraste och mest stabila OS,mjukvara och hårdvaran.

Fysisk säkerhet

Både AWS och Heroku har omfattande fysisk säkerhet. Säkerheten inkluderar också vakter, larm, videoövervakning etc.
Läs mer på Heroku.com: https://www.heroku.com/policy/security#physical-security

Brandväggar (Firewalls)

Boardeaser har satt upp brandväggar för att öka säkerheten mellan varje server och funktion. En brandvägg begränsar kommunikationen och möjligheten att ta sig mellan olikaservrar och funktioner, vid exempelvis intrång eller intrångsförsök.

Säkerhetszoner (DMZ)

Med brandväggarna byggs olika säkerhetszoner upp för att maximera säkerheten mot extern och internt intrång. DMZ står för (DeMilitarized Zone) och översätts till svenska med"demilitariserad zon".

DoS förmildra överbelastningsattack

Heroku tillhandahåller omfattande skydd mot överbelastningsattacker ”Distributed Denial ofService” (DDoS). Herokus skydd inkluderar bland annat TCP Syn cookies och mycket mera.

Port Scanning

Boardeasers IaaS (AWS) övervakar kontinuerligt portscanning, rapporterar varje incident, analyserar varje incident, stoppar varje försök och blockerar aktuell användare. Portscanningär ofta ett försteg till en attack eller intrångsförsök.

Behörighet & Autentisering

För alla aktiviteter krävs både behörighet och autentisering.

Spoofing & Sniffing Protections

AWS-hanterade brandväggar hindrar IP-, MAC- och ARP-spoofing på nätverket och mellanvirtuella värdar för att säkerställa att inte spoofing är möjligt. Packetsniffning hindras av infrastrukturen inklusive hypervisor som inte kommer att leverera trafik till ett gränssnitt som det inte inriktar sig till.

Automatisk prestandaövervakning

Boardeasers systemprestanda övervakas kontinuerligt. Vid problem larmas personal på Boardeaser.

Automatisk övervakning av teknisk status

Boardeasers tekniska status, eventuella felkoder och krascher övervakas kontinuerlig. Boardeasers utvecklingsavdelning notifieras.

Övervakning 24/7

AWS och Heroku övervakas 24/7.

Tredjepartstjänst & underleverantörer

Där Boardeaser använder tredjepartstjänst är data krypterad och avidentifierad. Godkännande och autentisering krävs kontinuerligt och har tidsbegränsning.

Ekonomisk data och KPIer

För analys av ekonomisk data och KPIer använder Boardeaser VisualBy. VisualBy användereräven de AWS och Heroku, samt krypterar och avidentifierar all data. Varje session kräver godkännande och autentisering är tidsbegränsad och krävs kontinuerligt.

Antivirus

Boardeasers servrar och all kommunikation till och från kund scannas kontinuerligt för virus.

Linux Operativsystem

Genom att Boardeaser använder Linux som operativsystem minimeras riskerna att drabbasav skadliga virus.

Backup

Backup sköts av Heroku flera gånger om dagen.

Manuell backup

Kund kan närsomhelst ta en komplett backup av sina dokument på Boardeaser.

Intern säkerhet

Boardeaser har ett omfattande och state-of-the-art säkerhetssystem. Utöver det har helabolaget ett starkt fokus på säkerhet som efterlevs genom rutiner och processer. Alla anställda är medvetna om betydelsen av säkerhet och fortbildning sker regelbundet.

Fysisk säkerhet

Boardeasers fysiska lokaler är väl säkrade med fysiskt skydd i flera nivåer. Larm och videoövervakning används enligt strikta rutiner.

Personal

- Sekretessavtal

  All personal på Boardeaser har skrivit på långtgående sekretessavtal.

- Screening

  All personal går igenom en screeningprocess som säkerställer att:

  1. Anställd har den bakgrund som angetts vid anställning
  2. Anställd har den utbildning som angetts vid anställning
  3. Anställd har en sund ekonomi
  4. Anställd är drogfri
  5. Anställd återfinns inte i brottsregister

- Utbildning i säkerhetsarbete

  Boardeaser utbildar all personal i säkerhetsarbete för kunds räkning.

- Åtkomst till kunddata

  Inga anställda hos Boardeaser kan oavsiktligt komma åt kunds data

- Begränsad tillgång till produktion

  Endast ett fåtal driftspersonal och utvecklare har tillgång till produktionsservrar.

Automatisk intrångsanalys

Boardeaser får notifikationer om försök till intrång och analys görs.

Säkerhetskonsult tredjepart

Boardeaser låter regelbundet tredjeparts säkerhetskonsulter utföra säkerhetsrevisioner.

Arbetar enligt ISO 27001

Boardeaser arbetar enligt ISO 27001 och strävar mot att genomföra en certifiering.

Produktionsdata analyseras

Alla interna incidentloggningar och kraschdata analyseras av Boardeaser.
Utvecklingsavdelningen får tillgång till incidentloggningar i realtid.

Automatisk test av ny mjukvara

All mjukvara genomgår omfattande automatiska tester innan den sätts i produktion.

Ny mjukvara testas internt

All ny mjukvara genomgår omfattande tester både av utvecklingsavdelningen, internt inom Boardeaser och i testproduktion hos kund innan färdig produkt lanseras för användare.

Kodstandard

Genom att strikt följa uppsatta kodningsstandard, minimeras risken att skapa säkerhetsproblem i mjukvaran. Kodningsanalys och genomgång görs regelbundet.

Kund äger egna dokument och data

Kund kan när som helst exportera alla sina dokument och lämna plattformen.Kund äger alla sina data.

Ansvarsförsäkring

Boardeaser innehar ansvarsförsäkring.