Säkerhet och förtroende

Boardeaser AB

2018-05-07

Boardeaser är en molntjänst för styrelsearbete, en organisations mest känsliga data. Boardeaser är en mycket säker plattform för styrelsearbete, många gånger säkrare än papper, e-mail och enkla lagringsplatser för data. Boardeaser har från början utvecklats med säkerhet i åtanke. Boardeasers kunder har mycket höga säkerhetskrav: Banker, noterade bolag (flera olika listor), forskningsbolag, advokatbyråer, etc.

Ett utdrag av säkerhetsfunktionerna: All kommunikation är krypterad, alla dokument lagras krypterad, 2-faktors inloggning, BankID och YubiKey. Boardeaser drift och applikationerna körs på AWS och Heroku (allt inom EU) med all deras säkerhet och driftstabilitet. Boardeaser fokuserar på löpande säkerhet med automatiska penetrationstester som körs varje vecka, oberoende konsulter anlitats för due dilligence av säkerhet. All personal har sekretessavtal och får löpande säkerhetsutbildning. Ingen anställd kommer åt kunds information oavsiktligt. Alla aktiviteter loggas internt och externt. Boardeaser är GDPR complient.

Boardeaser applikations säkerhet

Boardeaser är en modern och mycket säker molntjänst. All datatrafik till och från användaren krypteras. Alla uppladdade dokument krypteras. Två-faktors inloggning med BankID och Yubikey.

Krypterad trafik

All data till och från användaren krypteras med https.

Krypterad lagring

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

Inloggning

Inloggning sker med användarnamn och lösenord.

Två faktors autentisering

Boardeaser erbjuder två faktors inloggning och autentisering. En styrelse kan också kräva att alla användare använder två faktors autentisering. Boardeaser stöder BankID och det säkrare hårdvara stödet Yubikey.

BankID

Boardeaser stöder inloggning med BankID.

Yubikey

Boardeaser rekommenderar Yubikey hårdvara nycklar för inloggning. Yubikey används av alla större mjukvaruföretag internt: Google, Facebook, etc.

Alla inloggningar och aktiviteter loggas

Alla inloggningar och aktiviteter i Boardeaser loggas.

Alla inloggningsförsök analyseras

Alla inloggningsförsök analyseras, misstänks något ovanligt larmar Boardeaser och blockerar den inloggaren.

Inloggning på olika orter

Boardeaser analyserar inloggning och varnar för ovanlig inloggning och på ny ort och eller dator, användaren informeras.

Kund kan ge visstids access till data

Boardeaser har funktion för att ge access till data under en begränsad tid, t ex för support eller konsulter.

Behörighet

Användare av Boardeaser kan ha olika behörighet och tillgång till data.

Roller som ger access till delar av system

Användare av Boardeaser kan ha olika roller som ger tillgång till olika delar av systemet och dess data.

Notifieringar och e-mail till användare

Användargenererad information skickas aldrig ut från Boardeaser, utan användarens godkännande. E-post från systemet innehåller länkar, inloggning krävs för att se informationen.
Alla styrelsemöten, beslut, att-göra uppgifter, etc. kodas med nummer och länk.

GDPR

Boardeaser är GDPR compliant.

Boardeaser Infrastruktur

Boardeaser använder AWS data infrastruktur (världens största) och Heroku plattform på Irland (inom EU). De leverantörerna säkerställer tillgänglighet, backuper, nya versioner, övervakning 24/7, brandväggar, säkerhetszoner och stora delar av säkerhetsuppföljning. Därutöver använder Boardeaser ett antal andra leverantörer tillsammans med egenutvecklade funktioner för säkerhetsuppföljning automatiskt och som stöd för manuell uppföljning.

Informationen finns, är korrekt, tillgänglig och lätt komma åt

I Boardeaser finns informationen kvar, är korrekt (ej förändrad), alltid tillgänglig och lätt att komma åt.

Amazon Web Services (AWS)

Boardeaser använder infrastrukturen AWS. Världens största datortjänst (AWS) erbjuder industri ledande tillförlitlighet, skalbarhet och säkerhet.
Genom att använda AWS minimeras stillestånd och påverkan på kunders tillgänglighet.
AWS är en Infrastructure as a Service (IaaS). Allt lagras inom EU.

Heroku

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.

Fillagring

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

Penetrationstestning

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

Säker plattform

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

Fysisk säkerhet

Både AWS och Heroku har omfattande fysisk säkerhet. Läs gärna mera på: https://www.heroku.com/policy/security#physical-security . Säkerheten inkluderar också vakter, larm, videoövervakning, etc.
Boardeasers fysiska lokaler är väl säkrade med fysiskt skydd i flera nivåer, larm och videoövervakning.

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 olika servrar 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 överbelastnings attacker ”Distributed Denial of Service” (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 den användaren. Portscanning är ofta ett försteg till en attack eller intrångsförsök.

Behörighet & Autentisering

För alla aktiviteter krävs både behörighet och autentisering.

Spoofing och Sniffing Protections

AWS hanterade brandväggar hindrar IP, MAC och ARP spoofing på nätverket och mellan virtuella 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 Boardeaser personal.

Automatisk övervakning teknisk status

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

Övervakning 24/7

AWS och Heroku övervakas 24/7.

Tredjepartstjänst

Där Boardeaser använder tredjeparts-tjänst är data krypterad och av identifierad. Samt godkännande och autentisering krävs kontinuerligt och är tidsbegränsat.

Ekonomiskdata och KPIer

För analys av ekonomiskdata och KPIer använder Boardeaser WizCFO. WizCFO använder också AWS och Heroku, samt allt data krypterad och av identifierad. För varje session behövs godkännande och autentisering krävs kontinuerligt och är tidsbegränsat.

Antivirus

Alla 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 drabbas av skadliga virus.

Backup

Backup sköts av Heroku flera gånger om dagen.

Kunds backup

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

Boardeaser säkerhetsarbete

Boardeaser har ett omfattande och state-of-the-art säkerhetssystem. Till det kommer ett fokus från hela bolaget på säkerhet, stödd av rutiner och processer för säkerhetsarbete. Alla i bolaget är väl medvetna om viken av säkerhet och dess betydelse, utbildning sker regelbundet.

All personal har skrivit på sekretessavtal

All Boardeaser personal har skrivit på långtgående sekretessavtal.

Utbildning i säkerhetsarbete

Boardeaser utbildar all personal i säkerhetsarbete och vikten av säkerhet för kundsräkning.

Ingen Boardeaser anställd kan oavsiktligt komma åt kunds data

Ingen anställd hos Boardeaser kan oavsiktligt komma åt kunds data.

Begränsad tillgång till produktion

Endast ett fåtal driftspersonal / utvecklare har tillgång till produktionsservrar.

Automatisk intrångsanalys

Boardeaser får notifikationer om försök till intrång och analys görs.

Tredje parts säkerhetskonsult

Boardeaser låter regelbundet tredjeparts säkerhetskonsulter utföra säkerhetsrevisioner.

Arbetar enligt ISO 27001

Boardeaser arbetar enligt ISO 27001 och på väg att genomföra en certifiering.

All produktionsdata analyseras

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

Automatisk test av ny mjukvara

Alla mjukvara genomgår alltid omfattande automatiska tester innan den sätts i produktion.

All ny mjukvara testas internt

All ny mjukvara genom går omfattande tester både av utvecklingsavdelningen, internt inom Boardeaser och i test-produktion hos kund innan full produktion.

Kodstandard

Genom att strikt följa uppsatta kodningsstandard, minskas risken för att skapa säkerhetsproblem i mjukvaran. Kodnings analys och genomgång görs regelbundet.

Kund äger sina egna dokument och data

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

Boardeaser har ansvarsförsäkring

Boardeaser har ansvarsförsäkring.