

Byggeweb sikkerhetsbeskrivelse

Pr. 1. januar 2010

.....

Byggeweb ønsker at være ledende når det gjelder sikkerhet. Ikke bare i sammenligning med andre leverandører av prosjektweb, men også sammenlignet med lignende systemer for andre bransjer som normalt stiller større krav til sikkerheten enn det som er vanlig for prosjektweb.

En del av denne sikkerheten er at vi kun bruker generelle vendinger når vi omtaler Byggewebs sikkerhetsfunksjoner offentlig. Men beskrivelsen som følger vil likevel gi et bilde av de områdene der vi har gjort en spesiell innsats for å holde et høyt sikkerhetsnivå. Våre prosedyrer når det gjelder sikkerhet inneholder både en egen sikkerhetsorganisasjon og -teknologi i tillegg til flere 3. parts sikkerhetsteknologier.

Fysisk sikkerhet

Byggewebs produksjonsutstyr er plassert hos TDC Hosting. Der er de under overvåkning døgnet rundt, året rundt. Dette inkluderer bl.a. adgangskontroll, videoovervåkning, detektering av innbrudd og innbruddsforsøk og logg over alle besøkende. Dessuten er det etablert ekstraordinær sikring av dører og vinduer, nødstrøm vha. UPS'er og dieselgeneratorer i tilfelle hhv. kortere og lengre strømbrudd, kjøleanlegg for å kunne opprettholde konstant luftfuktighet og temperatur, samt brannsikring i form av brannvarsling og automatisk brannslukkingsanlegg.

Perimeter-forsvar

Perimeteren er beskyttet av brannmurer - kjøpt fra industriledende produsenter. Dessuten overvåkes Byggeweb-serverne 24 timer i døgnet.

Operativ systemsikkerhet

Byggeweb bruker et minimalt antall adgangspunkter til alle produksjonsserverne. Vi beskytter alle opererende systemkonti med sterke passord, og produksjonsservere deler ikke en database med master-passord. Alle operative systemer har økt sikkerhet ved å fjerne alle unødvendige brukere, protokoller og prosesser. Alle

produksjonsservere oppdateres kontinuerlig for å møte nye trusler og sikkerhetsbrister.

Database-sikkerhet

Database-adgang er kontrollert av både operativsystemet og på databasenivå. Adgang til produksjonsdatabasen er begrenset til et lite antall punkter, og produksjonsdatabasen deler ikke en database med master-passord.

Servermanagement-sikkerhet

Alle data som lastes opp og er skrevet inn i Byggeweb av en kunde er kundens eiendom. Kun betrodde ansatte har direkte adgang til Byggeweb sitt produksjonsmiljø, og kun i det omfanget som er nødvendig for systemvedlikehold, overvåkning og backup.

Reliabilitet og Backup

Komponenter i webservere og applikasjonsservere er konfigurert redundant der det er nødvendig. Alle kundedata er lagret på disker og speilet over flere forskjellige disker og kontrollere. På alle kundedata opp til og med den siste transaksjonen blir det automatisk tatt backup av hver natt, året rundt.

Applikasjons-sikkerhet

Vår modell for applikasjonssikkerhet forhindrer at en Byggeweb-kunde får adgang til en annen Byggeweb-kundes data. Sikkerhetsmodellen blir brukt på nytt for hver eneste forespørsel, og er gjeldende for hele den perioden en brukersession varer.

Kryptering av data

Byggeweb bruker den sterkeste kryptering tilgjengelig på Internettet i øyeblikket, 128 bit, for å beskytte kundedata og kommunikasjon via SSL (Secure Socket Layer). Data er ved bruk av SSL-kryptering under transporten til og fra Byggeweb-serverne fullstendig beskyttet mot å bli fanget opp og misbrukt.

Bruker-identifikasjon

Byggeweb kan kun åpnes med en gyldig kombinasjon av brukernavn og passord som bli kryptert vha. SSL når den overføres. Ved adgang til Byggeweb via Internet Explorer 5.0 eller høyere (eller Netscape 4.5 eller høyere), beskytter SSL-teknologi informasjonen både ved server-identifisering og datakryptering. Det er umulig for uvedkommende å avlytte kommunikasjonen mellom klient og servere.

En kryptert ID-cookie brukes til å identifisere hver bruker unikt. Byggeweb utsteder en "session cookie" kun for å samle opp kryptert

identitetsinformasjon i den perioden den bestemte session varer.

”Session cookie” inneholder verken brukernavn eller pass på brukeren og Byggeweb bruker ikke cookies til å lagre fortrolig bruker- eller sessioninformasjon. I stedet brukes mer avanserte sikkerhetsmetoder basert på dynamiske data og kodete session-ID’er.

Det er derfor umulig å gjenskape en gyldig session cookie. Dette gir en sikkerhet på at data kun er til rådighet for registrerte Byggeweb-brukere i utvalgte virksomheter. Data vil derfor være fullstendig utilgjengelig for konkurrenter og øvrige uvedkommende.

Passord-sikkerhet

Passord skal minst være 8 karakterer lange og inneholde både tall i tillegg til store og små bokstaver. Passord sendes av sikkerhetsmessige årsaker ikke via e-post.

Driftsikkerhet

Byggewebs servere er utstyrt med full redundans i forhold til driftsmiljøet og den direkte adgangen til IP-backbone. Dvs. at erstatningsutstyr eller alternative forbindelser er klar til at ta over dersom det skjer brudd. Det er ingen øvre kapasitetsgrense siden det – av hensyn til redundansen - er to forbindelser inn i huset. Begge forbindelsene er 622 MB og oppgraderes løpende.

Byggeweb har minst 9 år sammenhengende drift med årlige oppetider på over 99,9 %.

Uavhengige sikkerhetstester

Programvaren blir løpende testet av uavhengig sikkerhetsfirmaer. Byggeweb ble bl.a. testet i mai 2006 av sikkerhetsfirmaet Secode (www.secode.dk). Secodes anbefaling er om en strammere passord-politikk og obligatorisk anvendelse av SSL-kryptering ved innlogging er fulgt fra og med versjon 6.04. Byggeweb inneholder ingen kjente sikkerhetsbrister.