

Sikkerhed

Kryptering, dubleret hardware og flere internetleverandører

I en SaaS-løsning skal sikkerheden være integreret i alle lag af webapplikationen: krypteringen, netadgangen, webserveren, databasen – og frem for alt i koden.

“ Manglede sikkerhed kan få katastrofale følger for virksomheden og dens kunder. Derfor arbejder TimeLog løbende på at teste og øge sikkerheden i vores produkter. ”



Christoffer Lanstorp
Udviklingschef
TimeLog A/S

Teknisk setup

For at mindske risikoen ved nedbrud i hardwaren er de servere, der huser TimeLog Project, dublerede, dvs. der er to harddiske, to netkort, to strømforsyninger etc.

Der er firewalls foran webserverne og mellem web- og databaseservere. Desuden er serverne dedikerede, hvilket betyder, at de håndterer kun en funktion.

Hver kunde har sin egen database og programkode.

Backup

Hver nat gemmes en fuld backup af hver kundes database, og denne flyttes til en anden fysisk lokation end serverne.

Alle forandringer i databasen registreres desuden løbende i en transaktionslog.

Hosting

TimeLogs løsninger hostes af Progressive IT, der er certificeret som Microsoft ASP Channel Partner og specialiseret i hosting.

Internetforbindelsen fra datacentret er dubleret via to uafhængige leverandører, hvilket betyder næsten 100 % effektiv drifttid.

Krypteret adgang

TimeLog Project tilgås via en 128 bit krypteret forbindelse (HTTPS/SSL), som Verisign leverer og håndterer. Niveaulet for kryptering kan sammenlignes med de fleste netbanker.

SSL-kryptering betyder, at data sendt mellem en registreret bruger og TimeLogs systemer bliver krypteret, så det ikke er muligt at opsamle dele af transmissionen.



ISV/Software Solutions

TimeLogs produkter bygger på Microsofts teknologier.

Siden 2007 har TimeLog været Microsoft Gold Certified Partner samt Microsoft ISV/Software Solutions.

Som en del af certificeringen har Microsoft sikkerhedstestet TimeLogs produkter – og har ikke fundet problemer.

Sådan kan du øge sikkerheden med enkle midler

- Lav en sikkerhedspolitik – lav en enkel sikkerhedspolitik, hvor virksomheden tager stilling til sikkerhedsniveauet og kommunikerer denne politik til medarbejderne.
- Få styr på password – usikre password er den største kilde til sikkerhedsbrister. I TimeLog Project kan man opstille regler for, hvor sikre password skal være. Opbevaring af password er ofte lige så stort et problem, så tag det med i jeres sikkerhedspolitik.
- Luk af for tidligere medarbejdere – forhenværende medarbejdere udgør desværre ofte en stor trussel mod IT-sikkerheden.
- Undgå "master"-password – og undgå at have en model for nye password.
- Hav altid styr på anti-virus software.