

# Sicherheit

## Für uns gibt es nichts wichtigeres, als die Sicherheit der Kundendaten

Bei einer SaaS-Lösung muss die Sicherheit in alle Niveaus integriert sein; bei der Verschlüsselung, Internetzugang, Webserver, Datenbank – und besonders in der Kodierung.

“ **Mangelnde Sicherheit kann katastrophale Folgen für ein Unternehmen und deren Kunden haben. Deshalb arbeitet TimeLog laufend an der Sicherheit für unsere Produkte.** ”



**Christoffer Lanstorp**  
Entwicklungsleiter  
TimeLog A/S  
Dänemark

### Versorgungssicherheit

TimeLogs Lösungen werden von Progressive IT gehostet, die zertifizierte Microsoft ASP Channel Partner und Hosting Spezialisten sind.

Die Internetverbindung vom Progressive IT's Datencenter ist über zwei unabhängige Internetlieferanten gespiegelt. Das ergibt fast 100% effektive Betriebszeit.

### Verschlüsselter Zugängen und Firewalls

TimeLog Project läuft über eine 128 Bit verschlüsselte Verbindung (HTTPS/SSL), die von VeriSign geliefert und gesteuert wird. Das Niveau der Verschlüsselung kann mit dem vieler Banken verglichen werden.

SSL-Verschlüsselung bedeutet, dass alle Daten, die verschickt werden, verschlüsselt sind, dadurch können nicht Teile der Transmission erfasst werden.

Firewalls sind sowohl vor dem Webserver und zwischen dem Web- und Datenserver.

### Datensicherung der Datenbank

Jeder Kunde hat seine eigene Datenbank und Programmcode. Jede Nacht wird ein gesamtes Backup der Datenbank gespeichert, auch in einem Log und zu einem physisch anderen Ort gebracht.

Man kann eine Sicherheitskopie der Datenbank bestellen, die ans Unternehmen geliefert wird.

### Doppelte Hardware

Um das Zusammenbruch Risiko der Hardware zu minimieren, sind die Server dubliert. Das bedeutet, zwei Harddisks, zwei Netzkarten, zwei Stromversorgungen usw.

Darüber hinaus sind die Server dezidiert, sie können nur eine Aufgabe bewältigen.

**Microsoft**  
**GOLD CERTIFIED**

*Partner*

### ISV/Software Solutions

TimeLogs Produkte bauen auf die Technologie von Microsoft.

Seit 2007 ist TimeLog Microsoft Gold Certified Partner, wie auch Microsoft ISV/Software Solutions.

Als ein Teil der Anforderungen hat Microsoft einen Sicherheitstest der TimeLog Produkte durchgeführt – und kein Problem gefunden..

### IT Sicherheit mit einfachen Mitteln verbessern

- Eine Sicherheitspolitik erstellen – eine simple Sicherheitspolitik, bei der das Unternehmen Stellung zur Sicherheit nimmt und dies an die Mitarbeiter weiter gibt.
- Passwort Regeln – unsichere Passwörter sind für viele Sicherheitsprobleme verantwortlich. In TimeLog Project können Regeln für Passwörter aufgestellt werden. Die Passwortverwahrung ist problematisch, bedenken Sie das in der Sicherheitspolitik.
- Frühere Mitarbeiter deaktivieren – sie können eine Drohung für die Sicherheit sein.
- Hauptpasswörter umgehen – oder Modelle für neue Passwörter.
- Aktualisieren Sie immer das Antivirenprogramm.