Security at webCRM

Security at webCRM

This document describes the various IT-security measures employed by webCRM in terms of access and roles, infrastructure as well as procedures and certifications. The purpose of the document is to inform customers, business partners and other shareholders about the procedures and standards we uphold in order to provide the necessary security measures.

Access and roles

The system contains fine grained user access management with more than 90 security access levels.

- You can restrict access to records by territory and responsibility.
- You can restrict access to specific actions like view, edit or delete.
- You can restrict access to menus, modules and utilities.
- You can restrict access to specific reports and data export.
- More than 3 faulty login attempt causes the user to be blocked.

Infrastructure

Our webCRM servers and services are located at Microsoft Azure (Primarily in the West Europe region, secondarily in the North Europe region).

Microsoft Azure runs in datacenters managed and operated by Microsoft. These geographically dispersed datacenters comply with key industry standards, such as ISO/IEC 27001:2013 and NIST SP 800-53, for security and reliability. The datacenters are managed, monitored, and administered by Microsoft operations staff. The operations staff has years of experience in delivering the world's largest online services with 24 x 7 continuity.

For more information about the security and infrastructure at Microsoft Azure please use the following link: https://docs.microsoft.com/en-us/azure/security/fundamentals/infrastructure

Procedures

Only trusted webCRM employees have remote access to the production environment including databases and applications. All traffic between webCRM and the datacenter is carried using a secure encrypted connection.

Each webCRM customer has their own MS SQL database (physical file) with a unique, random name. Periodic incremental backup and full backups for every 24 hours are used.

The webCRM support staff only have access to the customer's system upon explicit request from the customer.