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 are located at secure, purpose-built facilities, and are monitored around the clock. Our servers are regularly updated with the latest security patches. Infrastructure features include:

- 24/7 SLA availability at 99.97% up-time.
- Powerful Cisco routers.
- Two hardware based stateful-inspection firewalls monitored by an IDS (intrusion detection system).
- 2 central layer3 switches.
- Redundant MPLS Internet connections.
- Redundant power supplies, fire protection and physical security
- Sufficient diesel generator stands by in case of a power cut.
- Data is stored using raid disk technology.
- Daily back-up to a secondary location.
- Https secure socket layer for data encryption.

Procedures and Certifications

webCRM is hosted by Hosters A/S (hereinafter Hosters) in Denmark. A leading and proven hosting provider with equipment and data housed in datacenter locations owned by Nianet A/S – also a proven datacenter provider.

Hosters handles security including server access, patches and updates applying best efforts to install such patches and updates within 30 days from the release date accordingly to manufacturer and best practice. Hosters is ISO27001 certified and ISAE 3402 type 2 audited yearly.

For webCRM, specific web servers and MS SQL servers, the access is limited to a few trusted staff members at the hosting center. The trusted Hosters' staff can access the webCRM servers only when on Hosters' premises or when using a secured VPN with multi-factor login. Hosters' staff is strictly instructed to not store any sensitive passwords on any physical devises outside Hosters premises and only accordingly to the ISO27001 procedures and policies with sensitive passwords stored digitally and encrypted.

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. On-line 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. The customer can grant access from the webCRM Configuration menu in order to handle support tasks.