Veiligheid en betrouwbaarheid

datum: november 2017

Vanaf het leggen van de eerste fundamenten van HRorganizer is rekening gehouden met de veiligheid en betrouwbaarheid van het systeem. Veiligheid om ervoor te zorgen dat gegevens alleen door gerechtigde personen gebruikt kan worden. Betrouwbaar, zodat gebruikers altijd de beschikking hebben over het systeem.

Dit heeft geresulteerd in:

- 100% uptime vanaf 2013
- nog nimmer is een poging tot digitale inbraak geslaagd.

Op alle niveaus is rekening gehouden met de veiligheid en betrouwbaarheid.

Op gebruikersniveau

- Beveiligde toegang met persoonlijke toegangsgegevens.
- Strikte geautomatiseerde procedure voor het herstellen van de toegang, wanneer het wachtwoord zoek is.
- Op aanvraag uit te breiden met digitale certificaten of eenmalige toegangscodes (al dan niet tijdgebonden).

Op mobiele en op webapplicatie niveau

- Volledig beveiligde verbinding (https, ssl).
- Ontworpen om gegevens van licentiehouders strikt te scheiden.
- Ontworpen om alle bekende aanvalsmethoden te weerstaan (bijv sql-injection).
- 99,8% gegarandeerde beschikbaarheid.

Op het niveau van de fysieke verbinding

Dit ligt in vertrouwde handen van Capitar (www.capitar.com)

- Datacenters volledig tweevoudig aangesloten op de door Capitar beheerde netwerk infrastructuur.
- Deze infrastructuur is voorzien van meerdere redundante internetverbindingen (Gigabit Ethernet backbone).

Niveau fysieke locatie centrale computer(s)

Dit ligt in de vertrouwde handen van Telecity group (www.telecitygroup.nl)

- Stroomvoorziening: meervoudig uitgevoerde, schaalbare high capacity, permanent gegarandeerd met Uninterruptible Power Supply (UPS)-systemen en on-site backup dieselgeneratoren.
- Branddetectie en –bestrijding: Very Early Smoke Detection Apparatus (VESDA) in elke ruimte geïnstalleerd, verbonden met het Building Management System (BMS) dat continu in de gaten gehouden wordt vanuit een netwerk operationscenter. Brand wordt in een zeer vroeg stadium gedetecteerd en via een koppeling met een brandbestrijdingsysteem gebaseerd op milieuvriendelijk gas of een watermist onmiddellijk geblust met minimale beschadiging van de apparatuur. Verlies van data en bedrijfsonderbreking wordt op deze manier voorkomen.
- Airconditioning: alle datavloeren op een constante temperatuur en een relatieve lage vochtigheid.
- Fysiek beveiliging: fysieke veiligheidsgrenzen, 24x7x365 monitoring door on-site personeel die alle personen die het gebouw binnengaan controleren, een CCTV-videocamerabewaking, en alarmering bij inbraak.
- Toegang: individueel programmeerbare toegangskaarten en visuele identificatie, alleen toegang indien de on-site engineer uw verzoek goedkeurt. Verantwoorde standaardprocedures zorgen ervoor dat we snel toegang krijgen tot de apparatuur, dag en nacht.

Niveau centrale computers (Capitar)

- Meerdere computers met virtualisatie hard- and software op verschillende fysieke lokaties.
- Automatische ‘failover’ van virtuele servers naar andere fysieke machines bij het falen van hardware.
- Gegevens opslag via FC SAN (Fiber Channel Storage Area Network) meervoudig uitgevoerd.

Niveau centrale virtuele servers (Capitar)

- Voor gepland onderhoud kunnen servers verplaatst worden tijdens de operatie (door virtualisatie).
- Op afstand alleen toegankelijk vanaf Spijk 5 in Wageningen.
- Nachtelijke database back-up.
- Eenvoudig op te schalen.