Oekotex - Security

# Datensicherheit

Sehr hoch, RAID6 als Storage, sämtliche Server laufen als virtuelle Instanzen auf oVirt-Clustern (nur kurzer Ausfall des Services bei Hardwareausfall), eventuell noch redundantes Storage / Switching

2-site Backup (fast local hdd, slower remote Tape, hier noch keine 100%ige Abdeckung)

Engmaschiges Monitoring, KPIs

Redundante Anbindung ans Internet, oVirt-Cluster für Firewalls

Redundante Server für den Zugriff auf die Datenbestände (eventuell redundante Applikationsserver)

Redundante SQL-Server

# Gefahrenszenarien

### - physischer Zugriff

Gering (Interxion), Diebstahl / Verlust eines Laptops mit Datenbank: hoch

### - virtueller Zugriff

Zugriff auf Intranet gesichert durch VPNs

Gefahr des Mißbrauchs einer VPN durch Accountsharing (vor allem im asiatischen Raum ?)

Passwörter oft zu einfach, Passwortänderungen regelmäßig durchführen / erzwingen ?

Gefahr durch zu einfache Kunden / Benutzerpasswörter (Achtung: Komfort), Möglichkeit eines

Kunden auf Daten anderer Kunden zugreifen zu können (kritisch / nicht kritisch)

# Anbindung der Nutzer:

### o über VPN

- über HW von Oekotex (init.at Firewalls)

+ Vorteil: Mehr Kontrolle

- Nachteil: Für Institute Blackbox, Problem bei HW-Ausfall

***Todo: Austausch durch Standard pfSense-Devices***

- über HW von Instituten (z.T. openVPN und IPSec)

+ Vorteil: Besser integriert in Institute

- Nachteil: Weniger Kontrolle durch Oekotex

- über Software VPN (OpenVPN)

+ Vorteil: Zugriff von Überall

- Nachteil: bei Laptopdiebstahl potentielles Sicherheitsrisiko

Generelle Herausforderung: Überblick über VPNs, Benutzungsstatistiken

### o direkt über Portalseiten (wird kommen)

+ Vorteil: Zugriff von überall ohne VPN möglich

- Nachteil:

+ Authentifizierung (WER greift zu) sehr wichtig, auf jeden Fall nur

über 2-Factor auth (SMS, OAuth)

+ Authorisierung (WAS darf der Authentifizierte), Zugriff nur auf ein

genau definiertes Subset des Datenbestandes

# Mögliche Verbesserungen:

Zugriff auf einen Account nur mehr von einer IP zugleich (problematisch bei mobilen Endgeräten mit schnell wechselnden IPs, User hinter einer NAT-Firewall)

Nur mehr eine gültige Session pro User (kann ein Problem sein bei Powerusern die über mehr als ein Browserfenster einsteigen)

Zugriffskontrolle über 2-Factor authentication (bereits teilweise implementiert)

Mitprotokollieren von Zugriffen (passiert jetzt schon)

### Zukünftige Probleme:

- Komplexitätsfalle, unterschiedliche Rollen beim Bearbeiten des Datenbestandes

- vollständige Abdeckung über automatische Tests

- automatische Penetration tests

- Trennung Produktion / Support, 24x7 Support, Schulungen bei Änderungen / neuen Features,

evtl. 2 Produktionsteams