OXSEED.

Archiv on Demand

Beschreibung der Sicherheitsmassnahmen
für die Archivoption auf www.signaturportal.de

Stand: 11/2007

Version 1.0

1.Einleitung

Die Archivkomponente auf www.signaturportal.de wird in technischer Kooperation zwischen dem Archivdienstleister Oxseed AG aus Stuttgart und der Mentana-Claimsoft AG erbracht. Die OXSEED AG erbringt die ECM, Storage und Backupdienstleistungen. Die Mentana-Claimsoft AG erbringt die Langzeitarchivierungsaufgaben gemäß § 17 SigV durch das Produkt Hash-Safe.

Das OXSEED Archiv gewährleistet höchsten Schutz für ihren Business-Content. Mit OXSEED können sich Unternehmen aller Branchen voll und ganz auf umfassenden Schutz verlassen.

Das nachfolgende Dokument beschreibt die Struktur der Sicherheitsmassnahmen um einen Überblick zu den getroffenen Maßnahmen zu ermöglichen. Details können nur gegen Abgabe einer Vertraulichkeitserklärung übermittelt werden. Wenden Sie sich dazu an unsere Hotline:

Hotline: **01805/ 691188** (14 Cent/min. dt. Festnetz, mobil evtl. abweichend) Mo.- Sa. 9.00 Uhr bis 17.00 Uhr

2. Sicherheitsdetails

Zu den organisatorischen Sicherheitsmaßnahmen von OXSEED Archiv gehören unter anderem:

- Ein Team erfahrener System-Ingenieure und Sicherheitsexperten

- Kontinuierlicher Einsatz bewährter und aktueller Sicherheitstechnologien

- Fortlaufende Bewertung neuer Entwicklungen im Bereich der Sicherheit

- Lückenlose Ausfallsicherheit in der gesamten Infrastruktur von OXSEED

- 100%-iger Fokus auf ein sicheres, skalierbares und privates System

Physische Sicherheit

Die OXSEED-Plattform wird zentral in Deutschland im Hochverfügbarkeits-Rechenzentrum der activ logistics AG betrieben. In der Anlage ist die physische Sicherheit durch nachfolgend beschriebene Maßnahmen rund um die Uhr gewährleistet.

Ausstattung des Rechenzentrums

Das Rechenzentrum ist durchgängig auf einen 24 x 7 x 365 - Betrieb ausgerichtet. Im Bereich der Backendsysteme wird an beiden RZ-Standorten durchgängig mit IBM –Technologien gearbeitet. Folgende IBM -Technologien werden eingesetzt:

- IBM I-Series für hostbasierte Geschäftsanwendungen
- IBM Blade- Center als Linux bzw. Windows-Plattform für C/S-Anwendungen (z.B. active Archive)
- IBM DS8000 als operatives SAN-Disk-Storage
- IBMTS3500alsTape-Library für Backup und Archivierung
- IBM DR550 als diskbasiertes Archiv-Storage

TK-Zugänge

- MPLS Zugang terrestrisch
  - Knotenpunkt Niederaula, Glasfaser
- Richtfunkstrecke
  - Knotenpunkt Bad Hersfeld
- GPRS Netzwerk
  - 2 Private GPRS Knoten
- ISDN Einwahl
  - 90 Kanäle
  - 3 Multiplexanschlüsse
  - 2 Richtfunk
  - 1 Kupfer
- 155 MBit Internetanbindung mit Backup

Kommunikation und Protokolle

- FTP (Intranet/ Internet), aktiv und passiv, via SSL
- Internet Mail (smtp, pop)
- VPN (Intranet/Internet)
- Direkte Einwahl über Modem- oder ISDN
- OFTP (VDA 4914) über ISDN, TCP/IP, aktiv und passiv
- X.400/SNADS/CGI&WebEDI
- GPRS-Gateway für mobile Anwendungen
- Leased Line, ATM, Frame Relay und MPLS

Stromversorgung

- Einführung 125 kVA
- USV
  - 32 kVA Drehstrom
  - 20 kVA Drehstrom

•Dieselgenerator 450 kVA (automatische Umschaltung nach 2 Minuten Stromausfall zum Dieselgenerator)

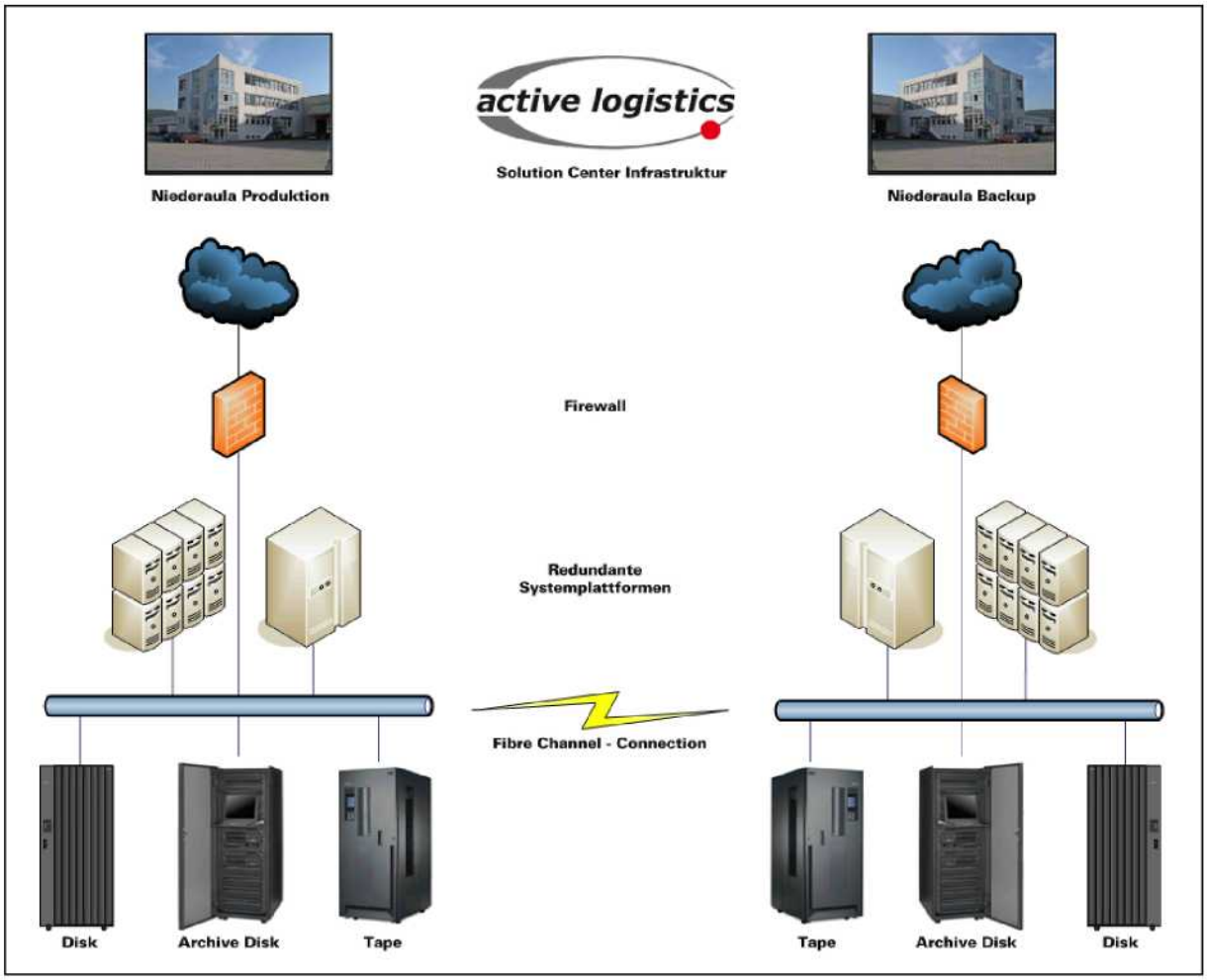
Klima

- 4 Klimatürme
  - O Temperatur 21 Grad
  - O Raumfeuchtigkeit 40%
- 1 Klimaturm wird als Hot-Standby betrieben

Zutrittskontrolle

Die Zutrittsidentifikation erfolgt mittels Fingerabdruck und Bildidentifikation in einem gültigen Personaldokument.

Überblick über das Rechenzentrum:



Schutzmassnahmen auf Applikationsebene:

Bereichsschutz

Der Netzwerkbereich wird von mehreren Firewalls geschützt. Die Firewall-Protokolle werden von OXSEED überwacht und analysiert, damit Sicherheitsrisiken auf proaktive Weise erkannt werden. OXSEED hat ein professionelles Sicherheitsunternehmen beauftragt, die Sicherheitskonfigurationen auf Änderungen, Sicherheitslücken und Fehler initiativ (simulierte Hackerattacken) zu überwachen und regelmäßige Tests zur Ermittlung von Sicherheitsbedrohungen und Eindringlingen durchzuführen.

Datenverschlüsselung

OXSEED setzt die leistungsstärksten Verschlüsselungsprodukte zum Schutz der Kundendaten und Kundenkommunikation ein, darunter ein 128-Bit SSL-Zertifikat und öffentliche RSA-Schlüssel mit 1024 Bit.

Benutzerauthentifikation

Benutzer können nur mit einer gültigen Kombination aus Benutzername und Kennwort auf OXSEED zugreifen. Diese Angaben werden bei der Übertragung mit SSL verschlüsselt. Die Wahl von Kennwörtern, die sich leicht erraten lassen, wird verhindert. Jeder Benutzer wird über ein verschlüsseltes Sitzungs-ID-Cookie eindeutig identifiziert. Um die Sicherheit zusätzlich zu erhöhen, wird der Sitzungsschlüssel automatisch in regelmäßigen Abständen im Hintergrund verworfen und neu wiederhergestellt.

Anwendungssicherheit

Das Virtualisierungskonzept der OXSEED (GRID-Architektur) verhindert, dass die User eines Mandanten auf die Daten eines anderen Mandanten zugreifen können. Das Sicherheitsmodell wird bei jeder Anforderung neu angewendet und während der gesamten Benutzersitzung durchgesetzt.

Interne Systemsicherheit

Innerhalb der Netzwerkbereich-Firewalls werden die Systeme durch Übersetzung der Netzwerkadresse, Anschlussumleitung, IP-Masquerading, nicht routingfähige IP-Adressenschemas und andere Maßnahmen geschützt. Die genauen Details dieser Funktionen sind herstellerspezifisch und geschützt.

Betriebssystemsicherheit

OXSEED gewährleistet eine hohe Sicherheit auf Betriebssystemebene, da für die Produktionsserver nur ein Minimum an Zugriffspunkten verwendet wird. Alle Betriebssystemkonten werden durch wirksame Kennwörter geschützt, und es wird keine gemeinsame Master-Kennwortdatenbank für die Produktionsserver verwendet. Für alle Betriebssysteme werden stets die vom jeweiligen Hersteller empfohlenen Sicherheits- Patches installiert. Außerdem werden alle nicht erforderlichen Benutzer, Protokolle und Prozesse deaktiviert und/oder entfernt, um die Betriebssysteme zu immunisieren (härten).

Datenbanksicherheit

Der Zugriff auf Datenbanken wird nach Möglichkeit immer auf Betriebssystem- und Datenbankverbindungsebene gesteuert, um ein Höchstmaß an Sicherheit zu erzielen. Der Zugriff auf Produktionsdatenbanken ist nur von wenigen Zugangspunkten aus möglich, und für die Produktionsdatenbanken wird keine gemeinsame Master-Kennwortdatenbank verwendet.

Servermanagement-Sicherheit

Alle Daten, die von einem Kunden in die OXSEED-Anwendung eingegeben werden, sind Eigentum dieses Kunden. Die Mitarbeiter bei OXSEED haben keinen direkten Zugriff auf das OXSEED- Produktionssystem, es sei denn, dies ist für die Verwaltung, Wartung und Überwachung des Systems oder für Sicherungen erforderlich. Das Systems Engineering-Team von OXSEED strukturiert eine klares Rollenmodell und die Zugriffsberechtigungen sowie deren Dokumentation für die Verwaltung, Wartung und Überwachung des Systems. Mitarbeiter die Rollen im Archivsystem einnehmen sind festangestellte Mitarbeiter der Oxseed AG deren Zuverlässigkeit durch ein polizeiliches Führungszeugnis überprüft wurde.

Zuverlässigkeit und Datensicherungen

Alle Netzwerkkomponenten, SSL-Beschleuniger, Lastenverteilungsgeräte, Webserver und Anwendungsserver sind in einer ausfallsicheren Konfiguration eingerichtet (HA- AL2). Sämtliche Kundendaten werden auf einem virtualisierten Produktionssystem gefahren, welches in einer Cluster-Konfiguration mit einer zweiten Systeminstanz im Backuprechenzentrum über ein privates Glasfasernetz verbunden ist, um einen ausfallfreien Betrieb zu gewährleisten. Die Speicherung aller Kundendaten erfolgt auf revisionssicheren Storagedevices. Weiterhin werden alle Kundendaten, bis zur zuletzt gespeicherten Transaktion, jede Nacht automatisch in einer primären Tape-Library gesichert. Die Sicherungsbänder werden sofort geklont, um ihre Integrität zu überprüfen. Die geklonten Sicherungskopien werden regelmäßig an einen sicheren, feuerbeständigen externen Aufbewahrungsort gebracht.

Haben Sie weitere Fragen?

Nutzen Sie einen der nachfolgenden Kontakte:
Hotline: **01805/ 691188** (12 Cent/min.) Mo.- Sa. 9.00 Uhr bis 17.00 Uhr
E- Mail: support@signaturportal.de