Six points for secure data transfer

With a 6-point plan, Bechtle shows what secure data transfers are made of. The system house for IT services got inspired by strategies from the past millennium.

In the fight against shadow IT, Bechtle points to strategies that have already proven themselves 20 years ago. Central mail server with business characteristics at the time terminated the bad habit of sending business documents via private e-mail accounts. A similarly attractive offer would have to be created by system administrators today to stop employees from exchanging business documents via private accounts to cloud service provider.

Such a central business cloud solution would have to be offered at an attractive price point with business features and offer a high level of security. In detail, Bechtle outlines the six criteria that an Enterprise File Sync and Share (EFSS) platform should meet:

Mobile Devices:

- Employees often use several mobile devices at their company, such as smartphones, tablets and phablets. The IT department must secure, connect and keep track of all devices, ideally without complex VPN connections." If there's no regulation, regarding what type of data users are allowed to process, inaccurate handling of information and access can lead to security vulnerabilities, " says Sven Stiefvater, Senior Sales Consultant and Cloud Specialist at Bechtle. For companies, a dedicated user-role concept has the advantage of keeping data from ending up on inadequately secured services.

Multi-level rights management:

- To ensure multi-level rights management for users and data spaces, an intelligent user role concept is required that depicts the individual hierarchical levels with their different access rights. This is how users' rights can be defined in the individual "Data Rooms the Data Space Admin, which is the central role in the IT department, retains the authority over the entire system at all times. Beside him, there are other data room admins, empowering individual departments such as marketing, sales or accounting to manage themselves. The specialist areas thus autonomously manage their authorization rules and design them according to their specific needs.

- **Secure Private Room Function:** A secure private room function is also useful. Setting up closed data spaces for individual users or groups creates a protected "private space" that excludes unauthorized persons. This also applies to administrators who retain the overall control, but do not have access to this data space. Compared to Windows file servers, which can be accessed by unauthorized persons as domain admin, this increases the security aspect.

- **Audit-proof logging:** A system log helps to detect unauthorized actions. The protocol shows, for example, who performed which actions at a given time. All entries must be valid, comply with data protection regulations and be managed and stored in

compliance with the highest security standards. Thus, the data exchange is understandable for the company and can be checked at any time.

- **Zero Knowledge Technology:** Anyone exchanging documents with external business partners via an EFSS solution should always transfer all files encrypted. It does not matter whether notebooks, fixed-line computers or mobile devices are being used and whether the data exchange takes place in a national or international environment. This applies to the transmission process (channel encryption) and the storage in the cloud (server-side encryption) or on the user devices (local encryption) alike. The Triple-Crypt Technology protects sensitive data comprehensively, without slowing down the data transfer. The „zero-knowledge-technology" is especially important. This includes a client-side encryption. It is only offered by a few cloud services and prevents unauthorized file access. In addition to secure data encryption, the location at which the data is kept is of great importance. Data centers in Germany are recommended, which are ideally certified according to the ISO / IEC standard 27001.

- **Image impact through branding:** As with business mail accounts, professional data transfer should also be recognizable as a company's account at first glance. Also, a branding from the URL through the website to the apps is useful. The application thus fits into the corporate design and ensures a homogenous appearance.

With the aforementioned criteria, the IT service provider is, of course, also the advertising its own expertise. Thus, Bechtle Secure Cloud share (PDF) meets the requirements for highly secure and comprehensive exchange and distribution of data.

The original article can be found at http://www.cloudcomputing-insider.de/sechs-punkte-fuer-sicheren-datentransfer-a-475137/