Cloud Security with TFM
(Treamo Finance Monitor)

Introduction

TFM is a Software as a Service (SaaS)-solution for treasury reporting and cash flow forecasting, running on Microsoft's Windows Azure Platform[1]. It has been developed by the Austrian company Treamo Business Consulting. This document describes security related topics that apply to TFM running in Windows Azure.

TFM consist of the following components:

1. Cloud-based Data Storage Layer
    a. Relational Database
    b. Blob Storage
2. Cloud-based Web Servers
    a. Web Services
    b. Dynamic Web Sites
3. Software Components running on the user's client PCs
    a. Thin Client[2]

This document mainly covers items 1 and 2 (software components in the cloud) and does not go into details on item 3 (software components on-premise).

[1] http://www.microsoft.com/windowsazure
[2] Microsoft Silverlight Technology, see http://www.silverlight.net/ for details

Data Centers

At the time of writing[3] all TFM services run in one of the two European datacenters of Windows Azure (Amsterdam and Dublin). Microsoft's datacenters, especially the one in Dublin, have received numerous awards. Here are some examples particularly relevant for Europe[4]:

- Best European Enterprise Datacenter Facility 2010
- Datacentre Leaders Award for Innovation
- European Code of Conduct for Data Centre Sustainability Best Practice

In September 2011 the BSI Group certified Windows Azure datacenters[5] based on the ISO/IEC standard 27001:2005[6]. The certification covers the components Compute, Storage, Virtual Network and Virtual Machine Services. At the time of writing the certification did not yet cover the relational database service of Windows Azure (SQL Azure[7]).

Regarding sustainability Windows Azure datacenters play an important role in Microsoft's strategy for green IT. The Dublin datacenter for instance operates on a PUE[8] factor of 1.25 and uses only 1% of the annual water consumption of a traditional industry datacenter. TFM extends energy efficiency for the hardware into the software layer. TFM supports adding and removing server resources based on the actual workload. This means that TFM does not waste unnecessary resources which leads to less energy consumption and enables lower prices for end customers.

[3] Print date: 2012-01-02
[4] http://bit.ly/aGZuv7,
[5] http://bit.ly/tNfvdD
[6] http://en.wikipedia.org/wiki/ISO/IEC_27001
[7] http://bit.ly/v8Fokk
[8] PUE = Power Usage Efficency, relation of the power consumption of the entire data center facility to the power consumed by core IT components; for details see http://bit.ly/ePkVWK

Governmental Access to Cloud Data

Service providers using the Windows Azure Platform can control in which geographical region data is stored and processed. As mentioned above at the time of writing all TFM services run in datacenters inside the European Union.

However, there are circumstances in which Microsoft has to share data in response to governmental requests. Here is the official statement of Microsoft[9] regarding governmental access to data stored and processed in their cloud datacenters:

> *Any company with a presence in the U.S. is legally required to respond to a valid demand from the U.S. government for information if the company retains custody or control over the data. This is the case regardless of where the data is stored or the existence of any conflicting obligations under the laws where the data is located. Microsoft will only respond to government requests for enterprise customer data when legally required. Understanding general customer concerns in this area, we will try to redirect the requesting entity to the customer to afford it the opportunity to determine how to respond. If unsuccessful, we will use commercially reasonable efforts to notify those customers prior to making any disclosure in response to a government request unless we are legally prohibited from doing so.*

Additionally Microsoft has published an FAQ document regarding to governmental access to data. Please contact Treamo Business Consulting (office@treamo.com) if you want to receive a copy of this document.

Data Storage Layer

TFM stores data in Azure's relational database service SQL Azure as well as in Azure's blob storage.

Relational Data Store

All relational database servers in the cloud used by TFM are three-node failover clusters. In the case of hardware or failures in the underlying system software (operating system or RDBMS software) TFM is automatically redirected to a new cluster node by SQL Azure. All cluster nodes are in the same datacenter facility. At the time of writing databases are not geo-replicated across multiple datacenters.

Network traffic to and from the database layer is SSL encrypted in all cases (both when accessed from cloud-based servers and from on-premise computers). Key handling is provided by the Windows Azure Platform.

Database servers are protected by multiple layers of firewalls. The first layer provides an IP-based firewall. It can restrict the access to TFM customer databases based on IP address ranges. Please contact Treamo if access to your TFM database should be restricted to certain

[9] Source: Harald Leitenmüller, National CTO, Microsoft Austria, 2011-07-12

IP addresses. The second firewall layer ("gateway layer") is a stateful firewall[10] that understands SQL's Tabular Data Stream (TDS) protocol. It protects the database against protocol attacks, brute-force password attacks, etc.

At the time of writing Microsoft does not offer a database backup service that goes beyond the data protection provided by the database cluster. However, Microsoft announced that such a service will be available in the calendar year 2012[11]. Until availability Treamo offers customers periodical backups (liable to pay costs; contact Treamo for prices of the backup service and SLA levels). These backups protect customers from data loss because of user mistakes and enable long-term archiving of data. Backup files are stored in Windows Azure Blob Storage. This means that:

- Backup files are stored on storage clusters (protection against hardware failures)
- Backup files are geo-replicated in both datacenters inside the European Union (Dublin and Amsterdam; disaster protection)
- If necessary access to the backup files for the end customer can be configured. If you want direct access to all database backups (e.g. to be able to restore it on an on-premise SQL Server) please contact your service provider for availability, prices and technical details.

Treamo does not encrypt data that is stored in relational databases. It supports encryption of data stored in Windows Azure Blob Storage (see next chapter). Please contact Treamo if you need detailed information about data encryption.

Blob Storage

Treamo stores binary objects (e.g. images, attached files, etc.) in Windows Azure Blob Storage instead of the relational database. Windows Azure Blob Storage provides exceptional data security especially because of the following reasons:

- The Blob Storage service is covered by the ISO/IEC standard 27001:2005 certification of Windows Azure.
- Like relational databases data stored in the Blob Storage service is always stored on storage clusters (protection against hardware failures).
- All data stored in the Blob Storage service is geo-replicated in both datacenters inside the European Union (Dublin and Amsterdam; disaster protection)

Cloud-based Web Servers

The datacenter facilities in which TFM runs are covered by the ISO/IEC standard 27001:2005 certification of Windows Azure.

[10] http://en.wikipedia.org/wiki/Stateful_firewall
[11] http://bit.ly/mRjYdI, the service will enable restoring databases to any point in time in the last 14 days.

TFM has been designed to support all security and accessibility functions of the Windows Azure Platform:

1. Operating system patches and service packs are automatically maintained by Microsoft. This means that the underlying virtual servers of TFM are guaranteed to have the latest hotfixes installed.
2. All web servers are implemented as clusters (web farms). This configuration prevents down times in case of e.g. hardware failures, operating system updates, etc.
3. TFM services are fully covered by the Windows Azure Service Level Agreements[12] provided by Microsoft.

Firewalls and network components for load balancing between cluster nodes are provided by the Windows Azure Platform and maintained by Microsoft.

All network traffic between storage systems (relational databases, blob storage) and virtual servers running certified TFM services is encrypted (SSL). All web services and web sites provided by TFM servers are SSL secured, too.

Client Components

The core TFM application is a thin client that uses Microsoft Silverlight technology. For specific administrative purposes[13] TFM offers a full client application based on WPF-technology.

The Silverlight client runs inside the Silverlight sandbox[14], it does not need to be installed as a trusted Silverlight application[15]. Therefore the end user's client machine is protected by the Silverlight sandbox.

TFM full client software is installed using a standard-conform Windows Installer package (MSI package). Therefore it supports silent installation and automatic software deployment. All installation components (bootstrapper, MSI package) as well as all application assemblies are strong named and signed using a certificate of the corresponding service provider. If necessary end customers can setup trust policies based on that code signing certificates.

[12] http://www.windowsazure.com/en-us/support/sla/
[13] E.g. customizing the TFM data model, running scripts, etc.
[14] http://msdn.microsoft.com/en-us/library/dd470128(v=vs.95).aspx
[15] http://msdn.microsoft.com/en-us/library/ee721083(v=vs.95).aspx