How Secure is SAP Business ByDesign for Your Business?

Applies to:

SAP Business ByDesign, SAP Research Security and Trust, Cloud security.

Summary

This article provides a high level overview of security mechanisms and control processes of SAP Business ByDesign as an on-demand platform. It discusses the particularity of security/risk considerations of SAP Business ByDesign and mitigation in terms of security mechanisms and control processes. The target audiences are decision makers and consultants.

Author: Mohammad Ashiqur Rahaman

Company: SAP Research, SAP Labs, Sophia Antipolis, France

Created on: March 3, 2012

Author Bio

Mohammad Ashiqur Rahaman is a staff member of the Security and Trust Research Practice, SAP Research, France. He works as a security expert for the SAP Business ByDesign.

Table of Contents

What is SAP Business ByDesign?

SAP Business ByDesign is an on-demand business software for small and medium enterprises. It offers an integrated suite of ready to use business applications as services over web as opposed to running and maintaining locally a costly IT landscape. While this refers to a Software-as-a-Service (SaaS) principle SAP Business ByDesign goes beyond to the extent of providing a platform for developers, i.e. Platform-as-a-Service (PaaS), in a SAP private cloud. Some features of SAP Business ByDesign related to SaaS & PaaS are as follows:

1. Accessible from anywhere, i.e. web-based access
2. No dedicated IT landscape required, i.e. low Total Cost of Ownership (TCO)
3. Customers share physical hardware keeping their data in dedicated tenants, i.e. low TCO
4. Very low administrative tasks, e.g. automatic updates and patch management
5. Partner companies can develop applications (solutions) in SAP Business By Design Studio
6. Partner companies may sell, resell their solutions and services using SAP Store.

Why Security has Special Attention in SAP Business ByDesign?

One of the cloud solution principles is to take the burden of IT infrastructure and data management away from the users. SAP Business ByDesign is *not* an exception and its functionalities are even more extended compared to the traditional cloud solutions considering its PaaS features. Capitalizing SAP Business ByDesign platform, developers can constantly innovate new application solutions. It is needless to say that to fully benefit from a cloud solution Secure data, Secure applications and Secure cloud infrastructure are *must*. The big difference of cloud security as opposed to on-premise security is that the abovementioned three S must be ensured by the cloud solution provider. Recent initiatives by OWASP (OWASP top 10 cloud security risks) and Cloud security alliance (Top Threats to Cloud Computing) confirm this observation. Having said that what is very often *not* understood clearly by the cloud providers is the cloud security.

Fortunately, SAP has clearly understood it and promises to protect customer data, partner solutions in a secure cloud infrastructure which is completely managed by SAP. Ensuring cloud security requires not only security mechanisms but also controlled processes involving partners and customers. Having a long tradition of on-premise software security, SAP has introduced some unique security mechanisms and processes in SAP Business ByDesign which are briefly described below.

How Secure is SAP Business ByDesign for Your Business?

Security in SAP Business ByDesign refers to the protection of resources from unauthorized access, disclosure and modifications. Such resources are the customer data, partner solutions and of course the SAP cloud infrastructure. The following four major security aspects of a user must be considered for appropriate security mechanisms and processes.

1. Identity: What defines me, e.g. end user, B2B user.
2. Authentication: What proofs my identity, e.g. passwords, certificates etc.
3. Authorization: What I can do, e.g. read, write.
4. Audit: Who did what over time.

Just like any on-premise software, for instance, SAP Business Suite, identity, authentication, authorization and audit are equally relevant in cloud computing and therefore ensured in SAP Business ByDesign. With respect to SAP Business ByDesign preventing from specific cloud risks (as OWASP top 10 cloud security risks) one class of security mechanisms and processes may apply for mitigating one or more risks partly or completely. For instance, the mechanisms and control processes described in securing the SAP cloud infrastructure apply to several risks, e.g. R4-Business continuity and resilience, R1-Accountability and data ownership, R3-Regulatory compliance, R8-Incidence analysis and forensic support, and R9-Infrastructure security. In order to ensure identity federation (R2-User Identity Federation) SAML-based authentication tokens are in place in SAP Business ByDesign. In the following, when discussing the security mechanisms and associated control processes of SAP Business ByDesign, their potential applications to the OWASP top 10 cloud security risks are also referenced.

How does SAP Business ByDesign Secure Partner Solutions?

As mentioned developers of a partner company can develop solutions using the SAP Business ByDesign Studio SDK. Developers can program in an easy to learn SAP Business ByDesign scripting language. It supports declarative definitions of access restrictions to the resources which are enforced by the platform. Before a partner solution goes productive a series of controlled activities along with security mechanisms are applied. (OWASP-R10 + R7)

1. **Strict Guideline for Developers:** To ensure the quality of a solution a standard guideline namely Public Solution Model is developed. A developer has to use the prescribed business API and compound services for developing a solution before submitting it to SAP. An active online community/forum is also established to support developers.

2. **Quality Review in SAP:** The submission file contains all the artifacts of a solution. The submission completely occurs over a secure channel, namely, https, from the SAP Business ByDesign studio and thus eavesdropping by man-in-the-middle is prevented. SAP has a structured process to check the quality of the submission. The checks include code review, virus scanning among others. Once a solution passes the quality check the solution can be made available in SAP Store for public.

3. **Backend Compiler:** In order to reduce computing load in the backend the scripting code can be compiled into ABAP in the frontend, i.e. SAP Business ByDesign Studio. However, once the solution is final the original code is recompiled in order to prevent from malicious code injection attacks.

4. **Tenant Separation:** A partner specific development artifacts are stored in an isolated tenant dedicated for the partner. As a result cross-partner solution access is easy to prevent.

5. **Strict Guideline for Implementation Project:** When a customer chooses a partner solution from SAP Store a set of structured activities called Business Configuration (BC) is launched in a sandbox environment. The sandboxing ensures a separate test tenant for the customer where all the scoping and fine tuning occur before migrating to a productive tenant. A productive system can also be changed at any time by triggering change control projects that ensure rapid deployment with system wide data consistency.

6. **Secure & Consistent Core:** As part of SAP Business ByDesign platform SAP provides a set of core business artifacts, such as business objects and compound services that are reusable by the developers of partner companies. To maintain a system wide consistency for all partners this core set of business objects and services cannot be modified by the developers. However, they can develop their own business objects and services which may extend the core.

How does SAP Business ByDesign Secure Customer Data?

Once a customer buys a partner solution from SAP Store and goes productive SAP takes care of customer data in SAP data centre. It is worth mentioning that customer data always belongs to the customer. The types of data include business objects, services, files etc. (OWASP-R5 + R6 + R7)

1. **Private Customer Tenant:** Like the tenant separation for the partner solutions, for each customer a separate tenant space is allocated in the SAP cloud infrastructure. The data which is only associated with the customer is stored in her tenant. As a result, only the respective users of the legitimate customer can access the data remotely.

2. **Secure Communication:** All interactions from a customer browser and tools to a SAP Business ByDesign backend occur over secure channels (TLS/SSL) complying with state-of-the-art open cryptographic standards. Even if a customer initiates an unsecure request (a plain http) it is converted into an https request before redirecting to the SAP Business ByDesign backend.

3. **Strong Authentication:** When interacting over the web with a SAP Business ByDesign system the interacting entity (human users or programs, e.g. web services) must provide some sort of proof about her identity. In this respect there are two possibilities: username/password-based and certificate (X.509)-based authentications. By default strong password policy is configured which can then be strengthened or customized for tenants and user types (e.g. customer, B2B). SAP

certification authority can provide multiple client certificates for the same user for different computers. However, the same certificate cannot be used by multiple users.

4. **Least Authorization:** Only authenticated users will have some access rights (read/write) on the business data. Such a user is associated with well defined UI components (called work center views) which *only* show data and provide actionable UI buttons (edit, delete, print, report etc.) required for her daily work. In this way a work center view encapsulates least possible access rights for the users and thus a work center view can be thought of as a role in access control jargon. More granular access restrictions can be applied by restricting data access based on the access context and access groups assigned to the work center views. For instance, a user assigned with a work center view of "sales" access context and access group of "daily revenue" can only access daily revenue data in the "sales" context but cannot access data related to, for instance, "marketing" context or "monthly revenue" or "quarterly revenue" access groups. A rigorous authorization methodology called Role-based Authorization Management (RBAM) is developed in this regard. RBAM is able to detect potential conflicts between assigned work center views and proposes alternative work center views so that responsibilities in a business process can be distributed and therefore potential frauds and errors can be prevented.

5. **Secure On-Site Tools:** Customers can download and install desktop tools, such as excel plug-ins for uploading/downloading excel data to and from the SAP Business ByDesign backend. Such downloads are digitally signed which can be always verified by the customer so as to prevent from malicious tools pretending as SAP tools. A separate authentication is required to make a secure connection to SAP Business ByDesign even if the same user is logged on from her browser. The passwords are stored in encrypted forms in an operating system specific location and thus can be used only by the current logged on operating system user.

How does SAP Business ByDesign Secure Cloud Infrastructure?

SAP follows best industry control processes of data centers in order to ensure best possible infrastructure security. We highlight only some of the controls. (OWASP- R1 + R3 + R4 + R8 + R9)

1. **Physical Security:** The data centers are distributed (currently in Germany and USA and in preparation in China) and are under 24 hour's surveillance with hundreds of cameras and sensors. The centers are fire-safe, flood-safe and are isolated in computation and storage parts. Based on a biometric security system only designated individuals can access to their designated areas. For data backup and recovery purposes regular backups are performed over redundant hardware storage systems that are supported by multiple connections from several power companies and in-house power supply.

2. **Multilayered Landscape:** The SAP Business ByDesign landscape architecture is multilayered and SAP proprietary. It includes among others a web dispatcher farm, multiple internet connections, multiple firewalls, and an advanced intrusion detection system. While the web dispatcher hides the network topology from the outside world multiple firewalls divide the network into protected segments and thus prevent from unauthorized internet traffic. Multiple internet connections minimize the impact of potential distributed denial of service (DDoS) attacks. Regularly updated anti-virus software checks the uploaded data and files to prevent from viruses and malwares.

3. **Security Logs and Tracing:** All the access to the SAP Business ByDesign is logged in a central place thanks to the isolation of storage from computation parts. At any time this log and tracing data can be retrieved for auditing and regulatory compliance purposes. Such data includes information about changed access rights, current access rights, current users and their activation/deactivation etc.

4. **Indirect Access to Tenants:** Similar to a private tenant, a unique URL is maintained for a customer who can do her daily business only by typing her unique URL in the browser. The actual access to the business data occurs after several redirections in the multilayered landscape. As a result, a business user does not have any direct control over the physical data stored in the tenants except enjoying her access rights.

Continuous Security Analysis of SAP Business ByDesign

Being a hot topic in the software industry cloud-based solutions are also becoming attractive targets for hackers. In order to cope with the increasing threats as depicted in, for instance, OWASP top 10 cloud security risks SAP maintains companywide corporate security standards that are regularly reviewed. These standards are maintained during software development lifecycles including SAP Business ByDesign development. Considering the particularity of cloud solutions SAP performs thorough security analysis by multiple groups inside SAP and by external auditors. (OWASP-R9)

1. **By the development group:** SAP Business ByDesign product and development team performs security analysis by its own security experts. For each topic, for instance, UI, Repository, SDK, Analytics etc. SAP Business ByDesign group has its dedicated security experts.

2. **By the external to the product group:** To complete the systematic approach further threat analysis is performed by fresh minds (i.e. experts external to the product and development). In particular, the members of security and trust practice of SAP Research provide means for effective and regular architecture review, design review and penetration testing.

3. **By the external auditors:** Apart from internal security assessments external auditors perform regular audits (SAS70/ISAE3402 or ISO27001). These include physical security assessment, security process assessment and employee security awareness.

The result of the security analysis takes immediate affects not only in the future SAP Business ByDesign versions but also in the previous versions by appropriate patching and down porting.

Conclusion

In this article we have briefly discussed different security mechanisms and control processes of SAP Business ByDesign. SAP understands cloud computing and its security and strives forward for continuous innovation in security mechanisms and processes. In an ending note, SAP Business ByDesign is secure for your business.

Acknowledgements: Thanks to the colleagues (Hoffelder, Gunter, Cédric Hebert, Martin Haerterich, and Walter Tighzert) for their useful comments and reviews.

Related Content

SAP Business ByDesign

SAP Business ByDesign Studio

https://www.sme.sap.com/irj/sme/community/collaboration/wiki?path=/x/fAJNCw

SAP Store

SAP Business Suite

OWASP top 10 cloud security risks

Top Threats to Cloud Computing

Public Solution Model

https://www.sme.sap.com/irj/sme/community/collaboration/wiki?path=/x/U4cqCw

SAML

Copyright