onapsis

Securing Business Essentials

SAP (In)Security

Attacks, defenses and current state of the art

Mariano Nunez

mnunez@onapsis.com

March 21th, 2012

Troopers 12, Heidelberg

Disclaimer

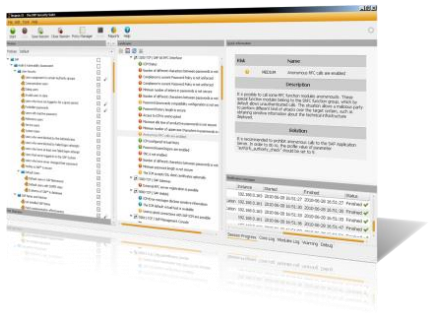
This publication contains references to the products of SAP AG. SAP, R/3, xApps, xApp, SAP NetWeaver, Duet, PartnerEdge, ByDesign, SAP Business ByDesign, and other SAP products and services mentioned herein are trademarks or registered trademarks of SAP AG in Germany and in several other countries all over the world.

Business Objects and the Business Objects logo, BusinessObjects, Crystal Reports, Crystal Decisions, Web Intelligence, Xcelsius and other Business Objects products and services mentioned herein are trademarks or registered trademarks of Business Objects in the United States and/or other countries.

SAP AG is neither the author nor the publisher of this publication and is not responsible for its content, and SAP Group shall not be liable for errors or omissions with respect to the materials.

Who is Onapsis, Inc.?

- Company focused in the **security of ERP systems and business-critical infrastructure** (**SAP®,** Siebel®, Oracle® E-Business Suite™, PeopleSoft®, JD Edwards® …).
- Working with Global Fortune-100 and large governmental organizations.
- What does Onapsis do?
  - Innovative ERP security software (Onapsis X1, Onapsis Bizploit, Onapsis IA).
  - ERP security consulting services.
  - Trainings on business-critical infrastructure security.



Who am I?

- **Co-founder & CEO** at **Onapsis.**
- Discovered 50+ **vulnerabilities** in SAP, Microsoft, IBM, ...
- **Speaker/Trainer** at BlackHat, RSA, HackerHalted, HITB, Ekoparty, DeepSec, ...
- Developer of the first **opensource SAP/ERP PenTesting frameworks.**
- Lead author of the “SAP Security In-Depth” publication.

Agenda

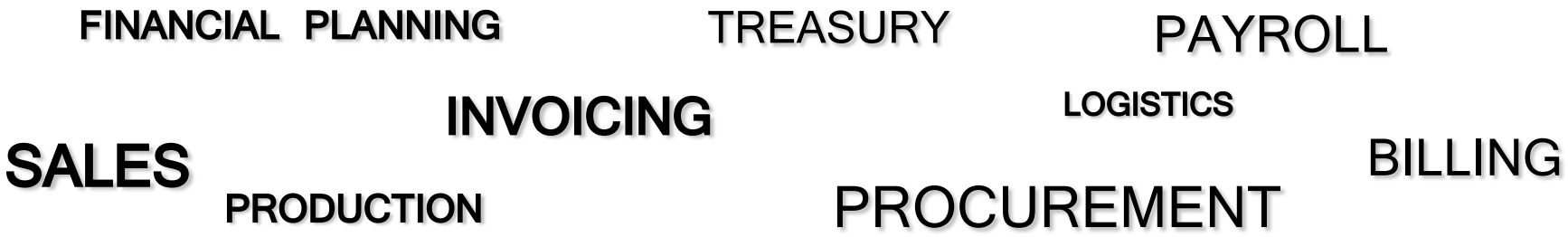
- Introduction
- A dangerous status-quo
- The current security level of SAP implementations
- The TOP-11 vulnerabilities affecting the SAP infrastructure
- Defending the SAP platform
- Conclusions

Introduction

What is SAP?

- **Largest** provider of **business management solutions** in the world.
  - More than 140.000 implementations around the globe.
  - More than 90.000 customers in 120 countries.

- Used by **Global Fortune-1000 companies**, **governmental organizations** and **defense agencies** to **run their every-day business processes.**
  - Such as Revenue / Production / Expenditure business cycles.



A Business-Critical Infrastructure

- **ERP systems store and process the most critical business information in the Organization.**
- **If the SAP platform is breached**, an intruder would be able to perform different attacks such as:
  - **ESPIONAGE:** Obtain customers/vendors/human resources data, financial planning information, balances, profits, sales information, manufacturing recipes, etc.
  - **SABOTAGE:** Paralyze the operation of the organization by shutting down the SAP system, disrupting interfaces with other systems and deleting critical information, etc.
  - **FRAUD:** Modify financial information, tamper sales and purchase orders, create new vendors, modify vendor bank account numbers, etc.

A Dangerous Status-quo

What "SAP Security" used to be 5 years ago

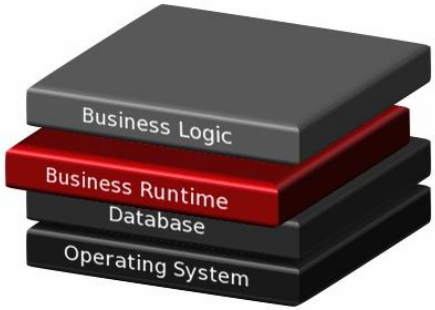
- **"SAP security" was regarded as a synonym of "Segregation of Duties controls".**
  - **Sample goal:** "Make sure that if Tim can create a new vendor, he can not create purchase orders".
  - This was mapped to a SoD matrix with SAP transactions / authorization objects.

- Most large organizations had "SAP Security" in place: they were **spending hundreds of thousands/millions of dollars in SAP security yearly** by having:
  - A dedicated team of SAP security professionals.
  - SoD & GRC software (usually costing **$500K-$2M or more**).

What “SAP Security” really is

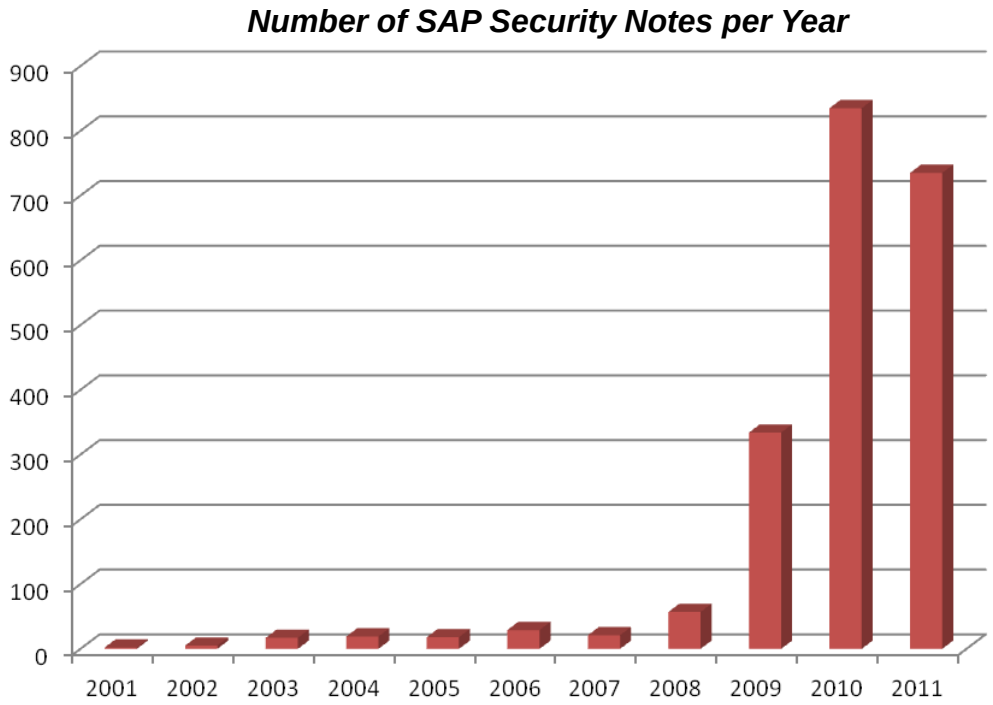
- SAP security is a complex discipline, that must be addressed holistically!
- SoD controls are necessary, but **they are not enough**.
- They only address one of the layers where security must be enforced.

- **The forgotten layer: The Business Infrastructure (NetWeaver/Basis).**
  - Base framework in charge of **critical tasks** such as authentication, authorization, encryption, interfaces, audit, logging, etc.
  - Can be susceptible of security vulnerabilities that, if exploited, can lead to **espionage, sabotage and fraud attacks** to the business information.



A Rising Threat

- **The number of SAP Security Notes** has increased dramatically over the last years.
- Security Notes usually address one or more vulnerabilities.
- Most of these issues affect the *Business Runtime.*



Total:
2068

- From the Trenches - The Current Security Level of SAP Implementations

Over 95% of the systems were exposed to espionage, sabotage and fraud attacks.

Only 5% of the evaluated SAP systems had the proper security audit logging features enabled.

None of the evaluated SAP systems were fully updated with the latest SAP security patches.

In most cases, the attack vectors that lead to the initial compromise resulted from the exploitation of vulnerabilities that have been publicly known for more than 5 years.

The TOP-11 vulnerabilities affecting the SAP infrastructure

BIZEC.org - The Business Application Security Initiative

- **BIZEC.org** is a **non-profit organization** focused on security threats affecting ERP systems and business-critical infrastructure.

- The **BIZEC TEC/11** project lists the most common and most critical security defects and threats affecting the Business Runtime layer/infrastructure of SAP platforms.

  - **BIZEC TEC-01: Vulnerable Software in Use**
  - **BIZEC TEC-02: Standard Users with Default Passwords**
  - **BIZEC TEC-03: Unsecured SAP Gateway**
  - **BIZEC TEC-04: Unsecured SAP/Oracle authentication**
  - **BIZEC TEC-05: Insecure RFC interfaces**
  - **BIZEC TEC-06: Insufficient Security Audit Logging**
  - **BIZEC TEC-07: Unsecured SAP Message Server**
  - **BIZEC TEC-08: Dangerous SAP Web Applications**
  - **BIZEC TEC-09: Unprotected Access to Administration Services**
  - **BIZEC TEC-10: Insecure Network Environment**
  - **BIZEC TEC-11: Unencrypted Communications**

BIZEC
BUSINESS SECURITY

BIZEC.org - The Business Application Security Initiative

- **BIZEC.org** is a **non-profit organization** focused on security threats affecting ERP systems and business-critical infrastructure.

- The **BIZEC TEC/11** project lists the most common and most critical security defects and threats affecting the Business Runtime layer/infrastructure of SAP platforms.

  - **BIZEC TEC-01: Vulnerable Software in Use**
  - **BIZEC TEC-02: Standard Users with Default Passwords**
  - **BIZEC TEC-03: Unsecured SAP Gateway**
  - **BIZEC TEC-04: Unsecured SAP/Oracle authentication**
  - **BIZEC TEC-05: Insecure RFC interfaces**
  - **BIZEC TEC-06: Insufficient Security Audit Logging**
  - **BIZEC TEC-07: Unsecured SAP Message Server**
  - **BIZEC TEC-08: Dangerous SAP Web Applications**
  - **BIZEC TEC-09: Unprotected Access to Administration Services**
  - **BIZEC TEC-10: Insecure Network Environment**
  - **BIZEC TEC-11: Unencrypted Communications**

BIZEC
BUSINESS SECURITY

Unsecured SAP/Oracle authentication

1. SAP connects to the database as the OPS$<username> (eg: OPS$**TL1**adm) **anonymously.**
2. Retrieves user and encrypted password from table SAPUSER.
3. Decrypts the password.
4. Re-connects to the database, using the decrypted credentials, now having access to the full schema.

USERID	PASSWD
SAPSR3-CRYPT	V01/0050ZctvSB67Wv3RWjDBSeLpWwHrWNj05AXb6NEprbkD

Unsecured SAP/Oracle authentication

- There is a special Oracle configuration parameter named REMOTE_OS_AUTHENT.
- If set to TRUE, Oracle "trusts" that the remote system has authenticated the user used for the SQL connection (!)
- The user is created as "indentified externally" in the Oracle database.
- Oracle recommendation: remote_os_authent = false
- SAP default and necessary configuration: remote_os_authent = true

- Protection: Restricting who can connect to the Oracle Database

```
tcp.validnode_checking = yes

tcp.invited_nodes = (192.168.1.102, …)
```

- New versions have a way to connect using the SecStore.

Live Demonstration

Defending the SAP Platform

The Challenges

- **Knowledge.** Understanding how to assess and secure an SAP system requires specialized knowledge.

- **Scope.** The *entire* platform must be secured. This comprises:
  - Every Landscape (ERP, CRM, SCM, …) in the organization
    - Every SAP system in each landscape
      - Every Client (mandant) and App Server in each system
        - Every of the 1500+ configuration parameters of each App Server

- **Periodicity.** The security of the SAP infrastructure **must be evaluated periodically**, *at least after each SAP Security Patch Day*, to verify whether new risks have been raised and evaluate necessary mitigation actions.

SAP Security - Who is responsible?

● Unlike other systems (such as Web servers, domain controllers, etc.), **the security of SAP systems usually falls under the domain of "The Business".**

● This means that the officers in charge of securing the systems are the same ones who are responsible for verifying whether they are secure or not → **FAIL!**

● If the organization's SAP teams are responsible for protecting the SAP platform, **then the Information Security Manager / CISO's department must verify whether the current security level matches the organization's defined risk appetite.**

Conclusions

Conclusions

- **Segregation of Duties controls** are necessary, **but not enough!**

- Many companies state “our SAP system has not been hacked”, but they do not even have the basic auditing features enabled! **How do they know?**

- **SAP is taking important steps into increasing the security of its customers’ systems** (security guides, regular patches, new standards), **but customers are not catching-up** (not an easy task by the way!).

- While “The Business” may work on the security of the platform**, it’s the responsibility of Information Security to verify that they are doing their job correctly**.

- If our business-critical infrastructure is hacked by exploiting a 5-year-old vulnerability, **we are clearly doing something wrong**.

Questions?

mnunez@onapsis.com

@marianonunezdc

Thank you!

www.onapsis.com

Follow us! ***@onapsis***