onapsis
Securing Business Essentials

CYBER-ATTACKS & SAP SYSTEMS

Is our business-critical infrastructure exposed?

by Mariano Nunez
mnunez@onapsis.com

Black Hat Europe 2012 Briefings

Abstract

Global Fortune 1000 companies, large governmental organizations and defense entities have something in common: they rely on SAP platforms to run their business-critical processes and information. In this scenario, cyber-criminals looking to perform espionage, sabotage or financial fraud attacks know that these systems are keeping the business crown jewels.

But, how difficult is for them to break into an SAP system today? Are we properly protecting the business information or are we exposed?

Five years ago, we were invited to hold the first public presentation on real-world cyber-threats to SAP systems at BlackHat Europe 2007. Since then, we have performed specialized Penetration Tests against the SAP platforms of several of the largest organizations of the world, enabling us to get an educated answer to those questions.

This white-paper analyzes how the “SAP security” concept has evolved over the last years and whether organizations are staying ahead of the real-world threats affecting their SAP platforms.

TABLE OF CONTENTS

Note:

In order to find the latest version of this white-paper, please check the Onapsis Research Labs website at http://www.onapsis.com/

1. INTRODUCTION

Global Fortune-1000 companies, large governmental entities and defense agencies have something in common: most of them rely on SAP systems to run their business-critical processes and information. Key processes such as sales, invoicing, manufacturing, procurement, human resources management and financial planning are managed and processed by systems running SAP software.

This critical nature is what makes them highly attractive for cyber-criminals and cyber-terrorists: if a malicious party is able to compromise an organization's SAP platform, he would be able to engage in espionage, sabotage and financial fraud attacks with severe implications to the business.

This white-paper analyzes how the “SAP security” concept has evolved over the last years and whether organizations are staying ahead of the real-world threats affecting their SAP platforms.

2. A DANGEROUS STATUS-QUO

2.1. What "SAP security" used to be five years ago

Five years ago, the SAP security discipline looked as if it had reached its paramount for most part of the Information Security and Audit communities.

Back then, this practice was regarded as a synonym of "Segregation of Duties (SoD) controls". This kind of controls are designed to ensure that the responsibility of performing critical business operations is split across different individuals, to minimize the chances of fraudulent activities against the organization.

In the SAP world, these controls are implemented by translating dangerous business/technical operations into the respective SAP authorization objects that would enable their execution, and ensuring that no user in the system is enjoying of incompatible authorizations.

2.2. The forgotten layer

While the review and enforcement of SoD controls are one of the pillars of the SAP system's security, they are not the only ones.

SAP business applications are executed by highly-complex technological frameworks, usually referred to as the NetWeaver or BASIS components ("Business Infrastructure"). The Business Infrastructure in charge of critical tasks such as authenticating users, authorizing their activities, interfacing with other systems, encrypting/decrypting sensitive communications and persistent data, auditing security events, etc.

The security of this layer has been traditionally disregarded during SAP implementation projects, as it was considered as an additional barrier to achieving the usually-challenging go-live date, without a clear return on investment. As mentioned before, another important reason was that there was a reigning *false sense of security*, where organizations believed that securing the systems was all about enforcing SoD controls.

The status-quo was broken in BlackHat 2007, when it was publicly demonstrated that SAP security was far beyond SoD controls, and the security of the Business Infrastructure was of paramount importance: just as any other technological component, this layer is prone to security vulnerabilities. If these vulnerabilities were exploited, malicious attackers would be able to perform espionage, sabotage and fraud attacks to the business.

2.3. A different (higher) risk profile

The main concern regarding the lack of security of the Business Infrastructure is that it introduces much higher risks to the platform.

This section details the difference in the characteristics of attacks exploiting weaknesses in the different layers:

Exploitation of a SoD weakness

1. The attacker needs a *valid user account* in the target SAP system.
2. The attacker needs to find out that he has more privileges than he should have, identifying the additional sensitive authorizations that he was granted.
3. Common auditing features may detect his activities.

Exploitation of a Business Infrastructure weakness

1. The attacker **does not need** a *valid user account* in the target SAP system.
2. **A successful attack will allow him to achieve SAP_ALL or equivalent privileges**.
3. Common auditing features **would not** detect his activities.

As it can be observed, attacks to the Business Infrastructure have several advantages from an attacker's point of view: they require less knowledge of the target platform, have greater impact and less chances of being detected.

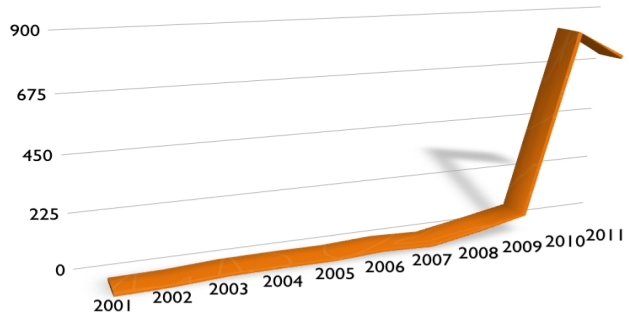
2.4. A rising threat

The number of reported SAP security vulnerabilities has been rising dramatically over the last years.

Five years ago, the total number of released SAP Security Notes was 90, with a yearly average of approximately 20 new issues released through 2004 – 2006.

Since 2007, the number of released SAP Security Notes/patches started to increase in an unprecedented scale. This resulted in a total number of 1900 as of February, 2012, with a yearly average of approximately 600 new notes in 2010 and 2011.

The following chart illustrates the evolution in the number of SAP Security Notes released per year:



The dramatic increase in the number of SAP security patches was driven mainly because of the following factors:

- An increased interest by the information security research community in ERP security vulnerabilities.
- The increased accessibility to SAP systems for the general public.
- SAP's enhanced efforts into increasing the security of its software applications.

In this scenario, organizations are now facing a big challenge:

- The need to understand which of the released SAP security patches are affecting their specific components in their large platform.
- The difficulty in determining which of the SAP systems are missing those applicable security patches.
- The difficulty in prioritizing the implementation of the patches, understanding the associated risk of the existing vulnerability.
- The effort involved in implementing the necessary patches, including proper quality-assurance to minimize disruption of existing business processes.

3. SAP SYSTEMS ON THE INTERNET

A decade ago it was not common to find SAP systems online. Nowadays, due to modern business requirements, many organizations are exposing their SAP platform to be accessed by customers, employees and vendors.

This situation obviously increases the risk of cyber-attacks, as the universe of possible attackers is dramatically expanded. This section analyzes the current exposure of SAP systems to the Internet.

3.1. Public information in search engines

As many SAP systems are connected to the Internet and provide Web interfaces for remote access, it is possible to obtain information from public search engines.

Google

Using Google dorks it is possible to search for common SAP Web applications, such as SAP Enterprise Portals, ITS services, BSP and Webdynpros, which can reveal the presence of an SAP Application Server connected to the Internet.

The following screenshot illustrates a search for exposed Enterprise Portals:

The different SAP web components can be searched through different dorks, such as:

- inurl:/irj/portal (Enterprise Portal)
- inurl:/sap/bc/bsp (SAP Web Application Server)
- inurl:/scripts/wgate (SAP ITS)
- inurl:infoviewapp (SAP Business Objects)

SHODAN

SHODAN is a another useful resource to find SAP systems online. As it indexes the returned Web server banners, this application can be used to expose

systems running SAP web applications just by searching for the string “SAP”.

3.2. Beyond SAP Web applications

In many cases, organizations who are not exposing their SAP platform through Web Applications to the Internet believe that there is no outside access to their platforms. This is usually wrong.

As part of the agreements entered with SAP when purchasing the software licenses, organizations agree on a support contract. This support works mainly by having a connection from SAP offices to the organization's SAP system.

This remote support connection is performed through a special component called SAProuter, which must be remotely available for SAP. While this should be always done through a VPN connection with SAP servers, it has been detected in many cases that the SAProuter was directly exposed to the Internet.

In the short-term, an statistical analysis of sensitive SAP services directly exposed to the Internet, such as the SAProuter, will be published.

4. THE INSIDER THREAT

While enabling access from the Internet to the SAP platform increases the associated risks, by no means should the internal network be considered as a trusted environment.

Large organizations have thousands of employees, outsourced staff, contractors, etc. who are everyday connected to the internal network and must be considered as potential threat agents.

In the ones running SAP platforms, intruders are usually presented with a favourable environment for attacking the SAP systems once they are connected to the network (either physically or through VPN connections).

This situation is commonly caused by:

1. The lack of proper internal network segmentation, by not deploying the SAP servers in a protected, internal DMZ.
2. Even if the previous point is well covered, a new problem arises: some of the SAP components still require the Firewall to allow access to technical services, such as the SAP Gateway, for the execution of certain business processes. This opens a hole in the Firewall which is impossible to close.
3. A possible solution to the previous point is the deployment of an IPS/IDS system, which is able to analyze the allowed traffic and detect attack patterns. However, none of the top-tier IPS/IDS vendors have these capabilities today, which results in a false sense of security.

This scenario highlights the need to ensure that the SAP systems are properly protected, as internal attackers have a favourable situation in regards to reaching the target servers and intend to exploit vulnerabilities in them.

5. FROM THE TRENCHES: THE CURRENT SECURITY LEVEL OF SAP IMPLEMENTATIONS

Since 2005, Onapsis experts have performed several specialized Penetration Tests to the SAP implementations of some of the largest organizations of the world.

In most cases, these projects were performed with the following characteristics:

- Network access to the end-user network (through VPN or onsite) was provided.
- Only a list of IP addresses of the target SAP systems was informed.
- No user/passwords credentials in any systems were provided.

Over these years, these experts have evaluated the security of more than 550 SAP Application Servers in total.

The findings are surprising:

- It would have been possible for an attacker to achieve full control of the SAP platform in more than 95% of the cases.
- The obtained privileges (SAP_ALL or equivalent) would enable a malicious party to perform espionage, sabotage and fraud attacks to the business information and processes managed by the target systems.
- 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 leaded to the initial compromise comprised the exploitation of vulnerabilities that have been in the public domain for more than 5 years.

Many of these vulnerabilities and attack vectors are detailed in the following section.

6. THE TOP-11 VULNERABILITIES AFFECTING THE SAP INFRASTRUCTURE

In 2010, BIZEC – The Business Security Community - was created. BIZEC.org is a non-profit organization focused on security threats affecting ERP systems and business-critical infrastructure.

Among several other projects, the BIZEC TEC/11 lists the most common and most critical security risks affecting the Business Runtime layer/infrastructure of SAP platforms.

The following points detail which are the most common risks and which could be the impact of their successful exploitation.

6.1. BIZEC TEC-01: VULNERABLE SOFTWARE IN USE

Risk
The SAP platform is running based on technological frameworks whose versions are affected by reported security vulnerabilities and the respective fixes have not been applied.

Business Impact
Attackers would be able to exploit reported security vulnerabilities and perform unauthorized activities over the business information processed by the affected SAP system.

6.2. BIZEC TEC-02: STANDARD USERS WITH DEFAULT PASSWORDS

Risk
Users created automatically during the SAP system installation, or other standard procedures, are configured with default, publicly known passwords.

Business Impact
Attackers would be able to login to the affected SAP system using a standard SAP user account. As these accounts are usually highly privileged, the business information would be exposed espionage, sabotage and fraud attacks.

6.3. BIZEC TEC-03: UNSECURED SAP GATEWAY

Risk
The SAP Application Server's Gateway is not restricting the starting, registration or cancellation of external RFC servers.

Business Impact
Attackers would be able to obtain full control of the SAP system. Furthermore, they would be able to intercept and manipulate interfaces used for transmitting sensitive business information.

6.4. BIZEC TEC-04: UNSECURED SAP/ORACLE AUTHENTICATION

Risk
The SAP ABAP Application Server authenticates to the Oracle database through the OPS$ mechanism, and the Oracle's listener has not been secured.

Business Impact
Attackers would be able to obtain full control of the affected SAP system's database, enabling them to create, visualize, modify and/or delete any business information processed by the system.

6.5. BIZEC TEC-05: INSECURE RFC INTERFACES

Risk
The SAP environment is using insecure RFC connections from systems of lower security-classification level to systems with higher security-classification levels.

Business Impact
Attackers would be able to perform RFC pivoting attacks, by first compromising an SAP system with low security-classification and, subsequently, abusing insecure interfaces to compromise SAP systems with higher security classification levels.

6.6. BIZEC TEC-06: INSUFFICIENT SECURITY AUDIT LOGGING

Risk
The SAP System's auditing features are disabled or not properly configured.

Business Impact
It would not be possible to detect suspicious activities or attacks against the SAP system. Furthermore, valuable information for forensic investigations would not be available.

6.7. BIZEC TEC-07: UNSECURED SAP MESSAGE SERVER

Risk
The SAP System's Message Server is not restricting the registration of SAP Application Servers.

Business Impact
Attackers would be able to register malicious SAP Application Servers and perform man-in-the-middle attacks, being able to obtain valid user access credentials and sensitive business information. Attacks against user workstations would also be possible.

6.8. BIZEC TEC-08: DANGEROUS SAP WEB APPLICATIONS

Risk
The SAP Application Server is allowing access to Web applications with reported security vulnerabilities or sensitive functionality.

Business Impact
Attackers would be able to exploit vulnerabilities in such Web applications, enabling them to perform unauthorized activities over the business information processed by the affected SAP system.

6.9. BIZEC TEC-09: UNPROTECTED ACCESS TO ADMINISTRATION SERVICES

Risk
The SAP Application Server is not restricting access to sensitive administration or monitoring services.

Business Impact
Attackers would be able to access administration or monitoring services and perform unauthorized activities over the affected SAP systems, possibly leading to espionage and/or sabotage attacks.

6.10. BIZEC TEC-10: INSECURE NETWORK ENVIRONMENT

Risk
The network environment of the SAP platform is not properly secured through the deployment and configuration of network firewalls, specialized Intrusion Prevention and Detection systems and application-layer gateways.

Business Impact
Attackers would be able to access sensitive SAP network services and possibly exploit vulnerabilities and unsafe configurations in them, leading to the execution of unauthorized activities over the affected SAP platform.

6.11. BIZEC TEC-11: UNENCRYPTED COMMUNICATIONS

Risk
The confidentiality and integrity of communications in the SAP landscape is not enforced. These communications comprise SAP-to-SAP connections as well as interactions between SAP servers and external systems, such as user workstations and third-party systems.

Business Impact
Attackers would be able to access sensitive technical and business information being transferred to/from the SAP environment.

7. DEFENDING THE SAP PLATFORM: PROTECTING OUR BUSINESS-CRITICAL INFRASTRUCTURE

7.1. The Challenges

There are mainly three challenges that arise when planning how to protect the business-critical infrastructure supported by the organization's SAP platform:

- **Knowledge**
  SAP has a wide variety of highly complex technological components, each of them featuring their own, in many cases proprietary, security architectures.
  Having a specialized knowledge of each specific SAP component is highly important in order to ensure a proper lock-down of the systems.

- **Scope**
  Many organizations used to assess and secure only a limited part of the SAP platform: typically the Central Instance and the productive client (mandant) of the Production system.
  In order to provide a resilient infrastructure, the platform must be protected holistically. This comprises every client and every instance in every system of every landscape of the organization. A single hole can jeopardize the security of the entire platform.

- **Periodicity**
  The security of SAP environments is highly dynamic. One the one hand, SAP is continuously releasing new Security Notes which are aimed to protect against the exploitation of known vulnerabilities. On the other hand, SAP administrators periodically interact with the security configuration of the systems, changing parameters that may render the systems vulnerable.
  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 mitigation actions.

7.2. SAP Security - Who is responsible?

Unlike other systems or applications such as LDAP directories, Web servers and Domain controllers, in some organizations the security of SAP applications usually still falls under the domain of “The Business”.

Therefore, this situation results in a clear segregation of duties inconsistency, where the officers in charge of securing the systems are the same ones who are responsible for verifying whether they are secure or not.

While it is acceptable that the organization's SAP teams are responsible for doing their best effort into protecting the SAP platform, it is highly important that the Information Security Manager / CISO department *verifies* whether the current security level matches the organization's defined risk appetite.

The following questions are aimed at serving as a starting point for further thinking of this situation in the reader's organization:

- Is the SAP platform a “blackbox” for the Information Security team?
- Does the Information Security team “trust but verify”?
- Who will be ultimately responsible if there is a security breach in the SAP platform?
- What if the SAP platform is compromised, not by a high-profile and complex attack, but rather as the result of the exploitation of a vulnerability that has been publicly known for several years?

8. CONCLUSIONS

Based on the author's field experience, it can be concluded that many SAP implementations are currently not properly protected and are exposed to high-impact attacks.

The most critical attack vectors comprise the exploitation of technical vulnerabilities and mis-configurations at the infrastructure layer of this platform, as many of them do not even require a valid user account in the target systems.

Over the last years, SAP has improved its internal security efforts and launched several initiatives to raise awareness on the importance of this subject among its customers. The challenge is now for customers to catch-up and protect their systems holistically, reducing the likehood of successful attacks to their business.

It is expected that the information presented in this document helps organizations to better identify their current security posture, understand existing risks and evaluate mitigation activities accordingly.

About Onapsis

Onapsis provides innovative security software solutions to protect ERP systems from cyber-attacks. Through unmatched ERP security, compliance and continuous monitoring products, Onapsis secures the business-critical infrastructure of its global customers against espionage, sabotage and financial fraud threats.

Onapsis X1, the company's flagship product, is the industry's first comprehensive solution for the automated security assessment of SAP platforms. Being the first and only SAP-certified solution of its kind, Onapsis X1 allows customers to perform automated Vulnerability Assessments, Security & Compliance Audits and Penetration Tests over their entire SAP platform.

Onapsis is backed by the Onapsis Research Labs, a world-renowned team of SAP & ERP security experts who are continuously invited to lecture at the leading IT security conferences, such as RSA and BlackHat, and featured by mainstream media such as CNN, Reuters, IDG and New York Times.

For further information about our solutions, please contact us at info@onapsis.com and visit our website at www.onapsis.com.