SAP Basis Security

The crown jewels exposed

Tom Schouten and Jeroen Kunis

Organizations today are exposed to new security risks due to the implementation of SAP systems. Research shows that across industries these risks have been insufficiently mitigated. In addition, knowledge and tools to exploit these weaknesses are becoming easily accessible. These developments threaten the availability, continuity and particularly the reliability of the SAP system. Various vulnerable components within the SAP landscape can be secured in a relatively easy manner. However, this requires a multi-disciplinary team with capabilities within the application and the infrastructural layer.

Tom Schouten MSc RE
is consultant at KPMG Advisory NV
schouten.tom@kpmg.nl

Jeroen Kunis MSc RE
is senior manager at KPMG Advisory NV
kunis.jeroen@kpmg.nl

Introduction

In the past few decades the definition of the terms 'segregation of duties' and 'security' were blurred by IT Audit and security professionals. Many SAP professionals refer to SAP security as the processes around authentication, roles and authorization profiles. The prevailing opinion is that users should only be allowed to access those functions in the system that are specifically and exclusively part of their job responsibilities and domain. This method should prevent staff from harming the organization and its system. Several organizations have invested lots of energy and efforts into their authorization concepts, partly as a requirement of the Sarbanes-Oxley Act ([Vree06]). Implementation of a sound segregation of duties concept doesn't ensure that vulnerabilities in other (technical) aspects, such as the SAP gateway, password hashes or default internet services are automatically mitigated.

The security of SAP at the Basis level often requires keen attention

SAP systems are becoming increasingly complex, partly due to the increase of SAP functionalities and products. Organizations are progressively implementing SAP systems in addition to the enterprise core component (ECC), unconsciously creating an expansion of access paths to confidential and valuable data: the organization's crown jewels. Moreover, SAP embraces technologies such as Java, HTTP, SOAP, XML and open SQL. Consequently, this has resulted in the adoption of all the inherent security risks that accompany these technologies. A single vulnerability in just one of the SAP systems can potentially compromise the whole IT landscape ([Edmo11]). Organizations must immediately mitigate the vulnerabilities within SAP that have been discovered over the past few years, to protect SAP's integrity, continuity and especially its reliability. This includes technical components such as the SAP gateway, SAP Application Server, SAP Message Server, Internet Communication Manager and SAP router, as well as hashing algorithms and various ports/services that are opened during an implementation (SAP Management Console). These subjects have been addressed in various SAP security notes.

In the sections below, we elaborate on a number of vulnerabilities within the SAP landscape that we have encountered. We start with the password encryption method of SAP NetWeaver. Following that, we will take a closer look into SAP systems that can be accessed through the internet. We will conclude with a description of the risks caused by the absence of SAP security notes. The security and integrity of SAP at the Basis level often requires keen attention. By this article, we call for renewed attention on these aspects.

Vulnerabilities

The password encryption method within SAP (hashes)

Within SAP, passwords are saved in the user master record table in an encrypted format. An important aspect of saving a password is the way it has been encrypted. The encryption method is also called the 'hashing algorithm'. Hashes are irreversible encryptions that make it impossible to retrieve the original password. The hashing algorithm that is used within SAP has been modified several times over the past few years. This was provoked by shortcomings in former algorithms, which were revealed by security researchers. At the same time, password-cracking tools became increasingly effective when it came to guessing combinations of passwords, by using rainbow tables. Within a rainbow table, all possible passwords and accompanying hashes are pre-listed without the need of further calculations. Using this method, passwords can be retrieved or matched to the corresponding hash easily. Password cracking tools can be applied to assess the complexity of the passwords used.

An efficient method to secure passwords is the use of a so-called 'salt', by adding a random series of characters to the password before it is encrypted. This makes it more difficult for password-cracking tools to retrieve the password. Prior to the introduction of SAP NetWeaver 7.1 or SAP NetWeaver 7.0 with Enhancement Pack 2, the user name was added as default salt for password encryption, as shown in Figure 1.

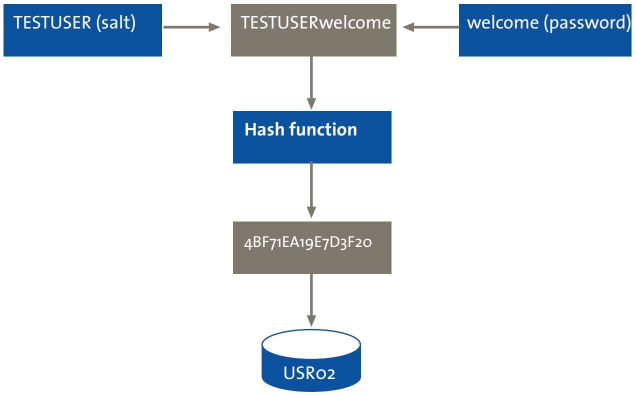


Figure 1. **Hash function.**

John the Ripper (JTR), a well-known password-cracking tool, contains a module for analyzing SAP passwords. On the internet, various tools are available to download the password hashes from the user table (USR02) and prepare them for JTR. The authors have learned by experience that approximately 5 percent of all passwords are retrieved by JTR within 60 minutes. Most likely, JTR will retrieve a user with unlimited access rights (SAP_ALL).

On 21 February 2009, SAP introduced a security patch[1] with a robust hashing algorithm using a random salt. However, passwords that employ this new method are by default saved within the old, vulnerable format, due

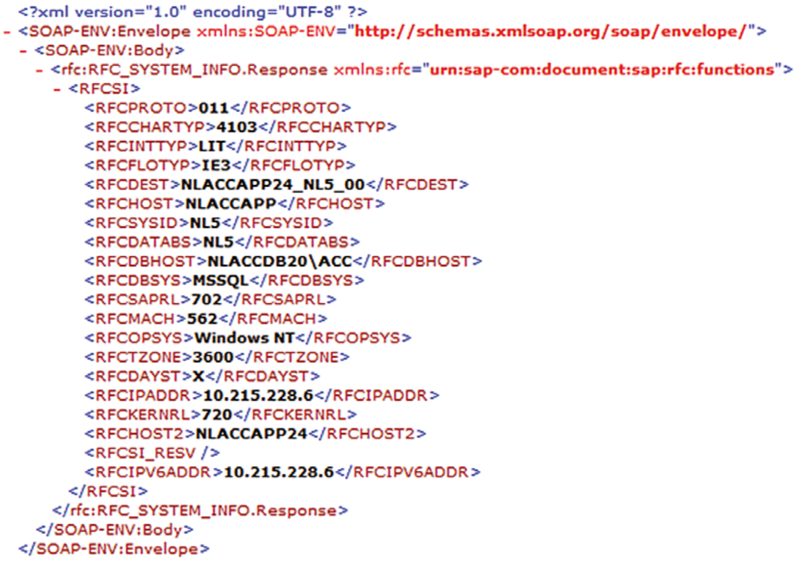
[1] https://websmp230.sap-ag.de/sap/support/notes/991968

to compatibility requirements by other (SAP) systems. Hence, this solution is ineffective against hackers, as a weak password hash is still available. Fortunately, SAP provided security parameters to prevent hashes from being saved in the older vulnerable format.[2] Unfortunately, this solution introduces new challenges regarding the system's connectivity with older kernels (interfacing). As a mitigating measure, authorizations that provide access to the password hashes should be restricted as much as possible. This would restrict the opportunity to view and misuse the hashes to a minimum number of people.

Unintentional exposure on the internet

Potential vulnerabilities that are frequently overlooked are included within SAP's Internet Communication Framework services. A growing number of organizations make their SAP systems available for connections with customers, suppliers, partners and their own staff ([Poly10]). The expansion of functionalities causes organizations to expose their traditional internal systems, which were partly designed in the era of the mainframe, externally to the internet. Search engine Shodan[3], for e.g., gives an impression of the number of SAP systems that can be accessed via the internet. Shodan is a search engine that can determine, among other things, which software is being used per website. For instance, when this article was being written (August 2013), 7.493 SAP systems were linked to the internet via the SAP ICM (Internet Communication Manager).

The search results from Figure 2 provide an overview of various publicly accessible SAP NetWeaver Application Servers. The majority of the SAP systems (1,762) are located in the US, followed by Germany (1,007), Mexico (409) and India (350). Making SAP functionalities available via the internet provides many advantages to organizations, but at the same time this may expose them— however unintentionally —to risks associated with the internet. SAP systems are becoming more accessible targets for cyber criminals or hackers, partly due to the exposure of vulnerabilities and misconfigurations within the (historically internal phasing) SAP system. Inherent vulnerabilities from default internet services can be misused by hackers for a targeted cyber attack. An example of a SAP service employing the so-called 'Internet Communication Manager' is the Info (/sap/public/info) service (refer to Figure 3). Our previous search, in Shodan, revealed various SAP servers offering this service via the internet unintentionally, allowing confidential information about the operating system, the database version, IP addresses and the SAP system Identifier to become publicly accessible (information disclosure). The spectrum of vulnerabilities that can be accessed by hackers can thus be expanded to the underlying layers as well. In addition, the risk exists that hackers will misuse unknown vulnerabilities via so-called 'zero day exploits', or misuse services with saved credentials. It is imperative to identify the services that are being offered via the internet. Particularly services that are accessible to the public or that bring specific security risks should be deactivated.[4]



```
  <?xml version="1.0" encoding="UTF-8" ?>
- <SOAP-ENV:Envelope xmlns:SOAP-ENV="http://schemas.xmlsoap.org/soap/envelope/">
  - <SOAP-ENV:Body>
    - <rfc:RFC_SYSTEM_INFO.Response xmlns:rfc="urn:sap-com:document:sap:rfc:functions">
      - <RFCSI>
          <RFCPROTO>011</RFCPROTO>
          <RFCCHARTYP>4103</RFCCHARTYP>
          <RFCINTTYP>LIT</RFCINTTYP>
          <RFCFLOTYP>IE3</RFCFLOTYP>
          <RFCDEST>NLACCAPP24_NL5_00</RFCDEST>
          <RFCHOST>NLACCAPP</RFCHOST>
          <RFCSYSID>NL5</RFCSYSID>
          <RFCDATABS>NL5</RFCDATABS>
          <RFCDBHOST>NLACCDB20\ACC</RFCDBHOST>
          <RFCDBSYS>MSSQL</RFCDBSYS>
          <RFCSAPRL>702</RFCSAPRL>
          <RFCMACH>562</RFCMACH>
          <RFCOPSYS>Windows NT</RFCOPSYS>
          <RFCTZONE>3600</RFCTZONE>
          <RFCDAYST>X</RFCDAYST>
          <RFCIPADDR>10.215.228.6</RFCIPADDR>
          <RFCKERNRL>720</RFCKERNRL>
          <RFCHOST2>NLACCAPP24</RFCHOST2>
          <RFCSI_RESV />
          <RFCIPV6ADDR>10.215.228.6</RFCIPV6ADDR>
        </RFCSI>
      </rfc:RFC_SYSTEM_INFO.Response>
    </SOAP-ENV:Body>
  </SOAP-ENV:Envelope>
```

Figure 3. **Internet-enabled services (/sap/public/info).**

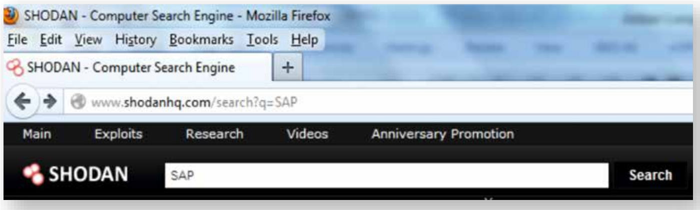

SHODAN - Computer Search Engine - Mozilla Firefox
File Edit View History Bookmarks Tools Help
SHODAN - Computer Search Engine
+
www.shodanhq.com/search?q=SAP
Main
Exploits
Research
Videos
Anniversary Promotion
SHODAN
SAP
Search

Figure 2. **SAP links on the internet.**

[2] login/password_downwards_compatibility

[3] http://www.shodanhq.com

[4] http://scn.sap.com/docs.DOC-17149

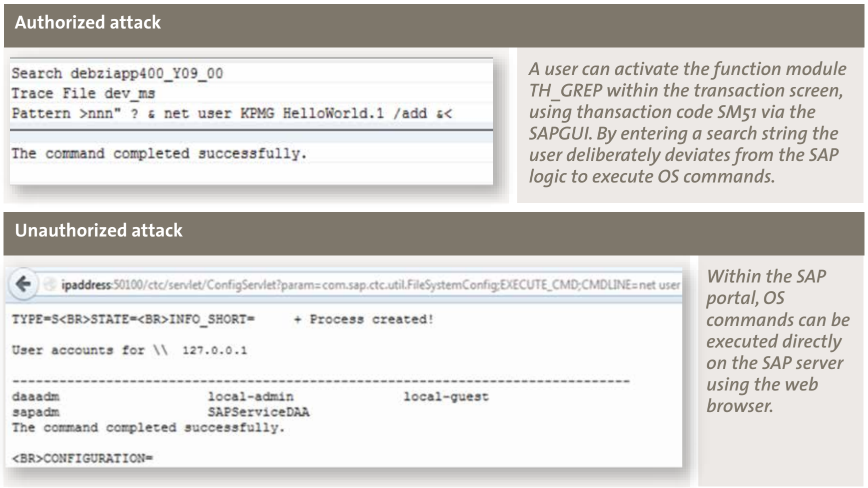
Protecting and auditing the current SAP system is becoming more time-consuming

SAP security notes

Since 2008, the number of security patches – also called 'security notes' – launched by SAP has increased dramatically. Prior to 2008, SAP released only a few patches; but in 2010, 2011 and 2012 an average of 735 security patches were developed each year. Apart from the increase in quantity, the diversity of the discovered vulnerabilities has also grown. This can be explained by the addition of multiple features, components and modules to the old-fashioned SAP R/3 system. Due to the increasing complexity and nature of the risks, protecting and auditing the current SAP system is becoming more time-consuming and requires extensive knowledge of the SAP system.

Note	Description
1097591	Security Scan and XSS Vulnerabilities
1394100	Security note: Access to RFC-enabled modules via SOAP
1141269	Security: XSS vulnerability in SAP GUI for HTML
1177437	Cross Side Scripting issue with Internet Sales
1428117	Security Note: Introducing WSDL security in Java AS 7.20
1415665	SQL injection in Solution Documentation Assistant
1418031	Potential Security Issues in SAP Solution Manager
1445998	Disabling invoker servlet in the portal
1580017	Code injection vulnerability in TH_GREP

Figuur 4. **Examples of SAP security notes.**



Authorized attack

```
Search debziapp400_Y09_00
Trace File dev_ms
Pattern >nnn" ? & net user KPMG HelloWorld.1 /add &<

The command completed successfully.
```

A user can activate the function module TH_GREP within the transaction screen, using thansaction code SM51 via the SAPGUI. By entering a search string the user deliberately deviates from the SAP logic to execute OS commands.

Unauthorized attack

```
ipaddress:50100/ctc/servlet/ConfigServlet?param=com.sap.ctc.util.FileSystemConfig;EXECUTE_CMD;CMDLINE=net user

TYPE=S<BR>STATE=<BR>INFO_SHORT=     + Process created!

User accounts for \\  127.0.0.1

-------------------------------------------------------------------------------
daaadm                   local-admin              local-guest
sapadm                   SAPServiceDAA
The command completed successfully.

<BR>CONFIGURATION=
```

Within the SAP portal, OS commands can be executed directly on the SAP server using the web browser.

Figure 5. **Exploiting security notes 1580017 and 1445998.**

The growing addition of functionalities exposes SAP to inherent vulnerabilities in the underlying technologies. Examples of these adopted technologies include Java, HTTP, SOAP/ XML and open SQL programming languages. This expansion caused an extension of the quantity and diversity of security notes. Figure 4 contains an overview of vulnerabilities in different SAP systems (Solution Manager, Portal) and vulnerabilities inherent in the technologies used, via Cross Site Scripting and SQL injection. Unfortunately, not all organizations are in a position to implement security notes at short notice. The continuity of the SAP system must be guaranteed before implementing a security note. Partly due to the change management process, which involves a variety of acceptance tests, it often takes months for the vulnerabilities to be actually rectified ([Scho13]). Currently, SAP releases security notes on a monthly basis.

The risk description/exposure addressed by SAP within the note's descriptions is often 'high level' and (perhaps) deliberately vague. The screenshots in Figure 5 outline the risk exposure in case security patches are not timely implemented within the SAP system. As demonstrated, malicious users are able to run commands at an operating-system level, as SAP does not validate the accuracy of the user's input.

To perform a risk assessment, organizations have to rely on the categories used by SAP to classify its patches. Among all the security patches launched for each category, we observe a peak, – particularly in 2010/11 – in the number of 'hotnews' patches that were launched. One of the causes for this peak is the attention SAP received within the security community. As of 2010, the number of SAP security conferences grew substantially, for e.g., during Blackhat and Hack in the Box ([Poly12]).

Figure 6 presents the development of different security notes that were launched. As yet, there seem to be considerably fewer patches released by SAP in 2013. On the other hand, vulnerabilities are much more serious in 2013 than in the previous years.

One of the risks identified in different SAP patches concerns vulnerabilities in the SAP gateway (notes 1408081, 1465129, 1531820). The SAP gateway is a technical SAP component, which is deployed as ready to use. This means that security can be added afterwards, but is not activated by default. Technically, this involves the configuration

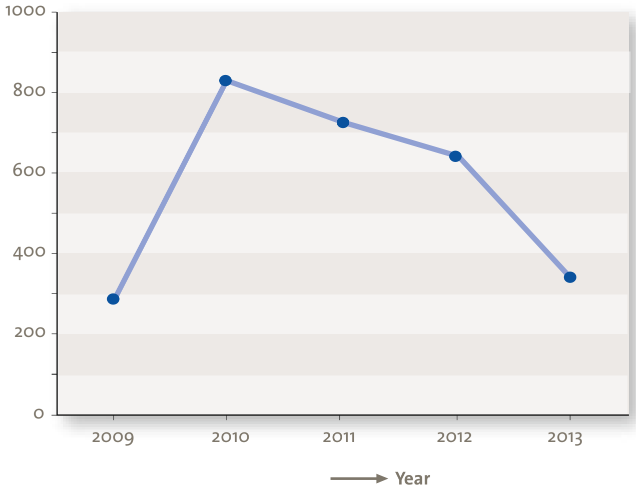
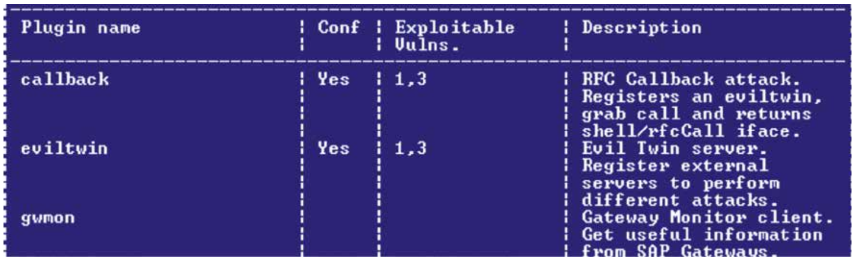


Figure 6. **Released SAP security notes.**



```
------------------------------------------------------------------------
 Plugin name              | Conf | Exploitable    | Description
                          |      | Vulns.         |
------------------------------------------------------------------------
 callback                 | Yes  | 1,3            | RFC Callback attack.
                          |      |                | Registers an eviltwin,
                          |      |                | grab call and returns
                          |      |                | shell/rfcCall iface.
 eviltwin                 | Yes  | 1,3            | Evil Twin server.
                          |      |                | Register external
                          |      |                | servers to perform
                          |      |                | different attacks.
 gwmon                    |      |                | Gateway Monitor client.
                          |      |                | Get useful information
                          |      |                | from SAP Gateways.
```

Figure 7. **SAP penetration-testing suites.**

of the SAP gateway by means of an Access Control List (ACL). The SAP gateway should exclusively communicate with systems within the ACL. If no Access Control has been activated for the SAP gateway, unauthorized persons or systems may access the SAP system, for e.g., by giving operating-system commands. Thus, a default SAP system is deployed from a usability rather than a security perspective.

A current trend within the security community is the adoption of SAP exploits within tooling. For instance, popular penetrating-testing suites, such as Metasploit, Bizploit and Onapsis X1 demonstrate how a SAP system can be targeted easily by a large number of (ignorant) people. Figure 7 shows plug-ins such as 'callback', 'eviltwin' and 'gwmon', which can be used to exploit misconfigurations in the SAP gateway. This results in a complete compromise of the SAP landscape.

Study of SAP vulnerabilities

Various aspects of SAP security issues were outlined in the previous section. To understand the extent and significance of these problems, various issues have been validated in actual practice ([Scho13]). Password hashes, internet services, security notes and scoping issues, among other things, have been addressed during research. This way, the extent to which SAP-related risks are being mitigated by organizations, is made explicit.
All members of the Security Access Management focus group within the VNSG (Association of Dutch-speaking SAP Users) were approached for this study. On 19 September 2012, a security issue questionnaire was submitted to this group. It comprised 21 different questions and was returned by 22 respondents.

The most vital results elaborated in the first three sections are listed below followed by the remaining results.

1. Use of weak password hashes

Unfortunately, we have found that many of our clients utilize a weak password hashing algorithm (such as A, B, D, E, F, G), even though powerful encryption methods exist and have been made available by SAP (such as H/I). This is caused by downward compatibility, on the one hand, and by the number of users that have been defined as 'service' or 'communication' users. These users do not have to comply with the password policy within SAP, and probably their passwords have never been changed afterwards. Only one of the respondents indicated that password complexity was being checked by means of password-cracking tools.

A SAP system can be targeted easily by a large number of (ignorant) people

2. Internet services

The study has shown that of the total respondents, 41 percent deactivated the ICF[5] services. Other respondents indicated that ICF services were not deactivated, or indicated that they did not have knowledge about whether the services were enabled or not.

[5] ICF = Internet Communication Framework

3. Missing SAP security patches

Various security-related incidents and risks can be mitigated by the timely implementation of security patches in SAP. The investigation showed that less than 14 percent of the respondents implemented a security note within one month. Deficient security patches often expose an organization temporarily to all risks outlined in the patch. Unfortunately, a clear risk description/exposure is often not included within the security note, which makes it difficult for organizations to properly assess the risks. The study also showed that access to the SAP gateway was limited for 23 percent of the respondents. This observation is also recognized by many of our clients.

Other findings are:

4. Privilege escalation SAP and OSI

During an IT audit, the Operating System (OS) and Database (DB) layers are usually assessed separately from the application layer. SAP, however, offers the possibility to execute commands on the OS or DB layers directly from the user interface. This enables all SAP users to access other layers within the OSI model (Open Systems Interconnect), namely, OS and DB; although this access may not be mandatory based on the user's work domain. By approaching the OS via SAP, the user can alter the database, bypassing all configured (application) controls within SAP. The risk exists that bank account numbers will be changed intentionally. It is essential, therefore, that ordinary users of the SAP application should have restricted access to the OS/DB level. At the same time, SAP access to the OS and DB should be limited. Research ([Scho13]) has shown that, as a rule, situations such as those described above are not examined during a SAP audit. As a consequence, the organization runs the risk of unauthorized changes being implemented in SAP that cannot be traced back to an individual.

5. Inadequate examination of non-production environments

A SAP landscape involves more than just a production system. As a rule, organizations use DTAP street with separate systems for development, test, acceptance and production. Each of these systems has several clients. From the user's point of view, a client is a separate environment with a user name and separate transactional- and master data. In general, eight to 16 SAP clients can be found within a SAP landscape. In this context, we are only referring to the core component, SAP ECC, leaving aside other products such as CRM or BW. During an IT audit, usually one client (Production) is examined, instead of the entire landscape, despite other systems such as development or acceptance jeopardize the SAP security concept.
The risk exists that unauthorized users from non-production systems or clients logon to the production client by using Remote Function Call (RFC) or client independent transactions. These transactions create the opportunity to access the production client from other systems or clients. In the case of an incoming RFC connection, SAP relies on the authentication and authorization of the other (remote) system. Research ([Scho13]) has shown that IT audits tend to focus primarily on the production client and less on the many other clients or systems in the SAP landscape. It is essential that all systems and clients are examined together and in the same way, due to the interconnected nature of those systems.

Remediation plan

In the previous sections we have explained the issues related to SAP security. We initiated by outlining a number of inherent vulnerabilities in the SAP landscape. Subsequent to that, we examined the extent to which these and other vulnerabilities are mitigated in practice. Below, we have listed several practical solutions and guidelines for system owners to mitigate various SAP security risks.

IT audits tend to focus primarily on the production client and less on the many other clients or systems in the SAP landscape

For practical and technical solutions refer to the Appendix at the end of the article.

Password hashes

1. First and foremost, the use of weak password hashes in SAP must be avoided as much as possible. SAP passwords should be saved in the improved hashing algorithm (CODVN H/I). This can be realized with the help of a SAP NetWeaver upgrade (min. 7.1). In addition, powerful password encryption can be enforced through security parameters.

2. Weak passwords can be identified by using password-cracking tools, such as JTR. Background users in particular are often configured with passwords that might originate from the implementation date of SAP. These passwords need to be changed and measures should be taken to avoid such mistakes.

3. It is said that you are only as strong as your weakest link. This perfectly applies to the Segregation of duties in SAP and is as strong as the weakest password. Various tables and access paths to the password hashes must be restricted by means of authorizations. The possibilities for gaining access to the password hashes must be acknowledged, analyzed and restricted. Password hashes must be regarded as confidential.

Operating System and Database

4. Access to SAP via the Operating System must be strictly limited. Security baselines on OS and DB levels must be designed and implemented. Also, authorizations which allow the execution of OS-commands via SAP must be restricted.

5. Ensure that the SAP user at the OS level is not installed using either root or administrator privileges.

Technical SAP components

6. Technical SAP components should only be able to recognize those systems that are authorized or familiar within the landscape. This way, SAP can be protected against unknown and malicious interfering systems. By implementing Access Control Lists for the SAP router, Oracle, Application Servers and Message Servers, unknown malicious parties are excluded. In this context, SAP systems and servers that are operational should be made explicit, while ensuring that no addresses are overlooked.

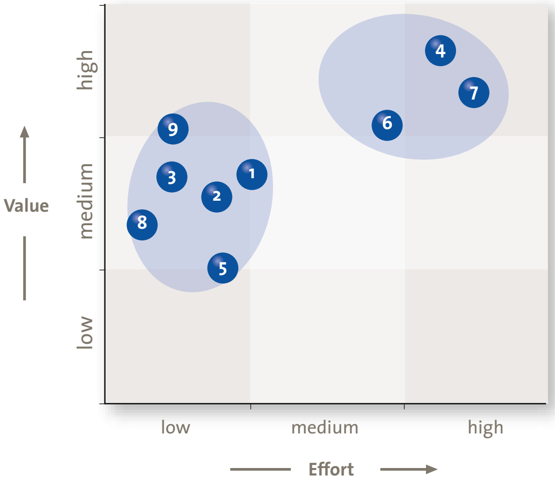


Figure 8. **Remediation plan for SAP security risks.**

SAP security notes

7. Implement the most recent security patches, particularly for the SAP gateway. In addition, the most recent Basis Support package and SAP kernel needs to be implemented. This can be downloaded from the SAP Marketplace. Review Earlywatch/RSECNOTE reports for new patches on a regular basis.

RFC connections and interfaces

8. Investigate all RFC connections from non-production environments and verify the logon & security sections of these connections to prevent, among other things, the remote logon possibility

Services

9. Activate only those services that are essential to the business. Internet services surplus to requirements should be deactivated on the application server wherever possible. If possible, access to critical logfiles within the SAP Management Console should be restricted. The extent to which activities are logged should be decreased (trace level).

The recommendations outlined above can be used as a guide to mitigate various recognized SAP security issues. However, we do not warrant the completeness of the discussed SAP security topics. Other factors that could adversely affect the security of the SAP system include compromised ABAP source code, historical SOD's, table debugging, network sniffing and many others. Also, it should be kept in mind that features such as soft controls and user awareness are preconditions for a secure system. The use of SAP penetration testing software should be

The effect on the regular IT audit is that working programs for SAP need to be adjusted

considered to expose major SAP vulnerabilities. There are various commercial (ESNC) and easy-to-use freeware solutions (such as Bizploit) available on the internet.

Conclusion

Due to the expanse of SAP functionalities and products, organizations are inadvertently increasing the number of access paths to their crown jewels. In addition, SAP embraces technologies such as Java, HTTP, SOAP, XML and open SQL, which exposes SAP to all the security risks inherent to these technologies. The risks involved with the technical security of SAP on the Basis layer, are generally unknown and neglected. Research has shown that, consequently, these risks are only mitigated to a limited degree.

SAP security issues are noticed within the cyber security community. Since 2010, a growing number of SAP security conferences have been organized. Tools to exploit vulnerabilities in SAP have become easy to use and are accessible to a large number of people. Hence, exploiting a SAP system has become easier by the day.

In this article we have addressed risks, vulnerabilities and misconfigurations within SAP. Organizations are often unaware of the risks that they are exposed to by not fixing the neglected vulnerabilities. Fortunately, SAP is increasingly raising the quality of the default security measures in its system.

The effect on the regular IT audit is that working programs for SAP need to be adjusted and the risk analysis has to be revised. A number of the current vulnerabilities within the SAP landscape can be resolved in a relatively easy manner, as indicated in the section entitled ‘Remediation plan’. However, this requires a team possessing knowledge of the application layer and the infrastructure layer.

References

[Edmo11] M. Edmonds (2011), *SAP-Security Audit: The City Should Implement Additional Measures to Effectively Secure Its SAP Enterprise Resource Planning System*, Audit Report.

[Poly10] A. Polyakov (2010), *SAP-security: Attacking SAP Users*, Digital Security Research Group.

[Poly12] A. Polyakov, Tyurin (2012), *SAP-Security in Figures; A Global Survey 2007–2011*, ERPScan.

[Scho13] T. Schouten (2013), *A False Sense of Security; Auditing (Beyond) the SAP Production System*, University of Amsterdam.

[Vree06] A. Vreeke and D. Hallemeesch, “Zoveel functiescheidingsconflicten in SAP – dat kan nooit, en waarom is dat eigenlijk een risico? De complexiteit van het SAP R/3-autorisatieconcept vervolgd” (“So Many Issues Connected with Division of Responsibilities in SAP – That’s Impossible, and Why Is That a Risk Anyway? The Complexity of the SAP R/3 Authorization Concept Continued”), *Compact* 2006/.

Appendix

The technical details listed below can be used as a guideline to mitigate a number of known SAP security issues. The numbers correspond with those in the 'Remediation plan' section.

1.	Parameter login/password_hash_algorithm & login/password_downwards_compatibility	
2.	John –format=sapB hashfile	
3.	Relevant objects:	S_TABU_DIS, S_TABU_NAM
	Relevant tables:	USR02, USH02, USRPWDHISTORY
	Relevant authorization group:	SC, SPWD
	Relevant transactions:	SE16, SE16N, SM49, SM69, DB02, SM30, SM31, N, UASE16N, SE17,CAC_DET_ACCAS_30, CX0A7, CX0A8, KCS5, KEP6, PRP_UNIT
	Relevant programs:	RK_SE16N, UA_SE16N_START
	Monitoring deletion of logfiles:	RKSE16N_CD_SHOW_DELETE, RSTBPDEL, RSLDARCH02
4.	Relevant objects:	S_LOG_COM en S_DEVELOP
	Relevant transactions:	SM49, SM69 (do not allow additional parameters)
5.	N/A	

6.	Oracle – SAP:	tcp.validnode_checking = yes
		tcp.invited_nodes = (locahost, payrolldb, host3)

	SAP Gateway:	<> USER=* HOST=* TP=*
	SAP Message Server:	<> HOST=*
	Implicit deny	D * * *
	Incorrect entry	P * * *
7.	Earlywatch / RSECNOTE Remote OS authentication for the Oracle database instance (sapnote_0000157499, 21/10/2011) SAP management console (sapnote_00001439348, 14/12/2010)	
8.	Relevant transactions:	SM59, SA38 – RSRFCCHK
9.	Relevant transactions:	SICF
	Activated services:	http://127.0.0.1:8001/sap/bc/gui/sap/its/webgui http://127.0.0.1:8001/sap/public/info
	SAP Management Console:	http://<host>:5<instance>13

About the authors

Tom Schouten MSc RE is consultant at KPMG Advisory and is concerned with, among other things, security audits and advisory engagements for a range of organizations. This article is based on his research at the University of Amsterdam within the 'Amsterdam IT Audit Program' programme.

Jeroen Kunis MSc RE is senior manager at KPMG Advisory and is very experienced in control issues with regard to SAP and SAP-supported processes, and the development and implementation of SAP Security tooling.