SAP Cloud Security Excellence

A strategy document prepared on behalf of TREND MICRO Germany GmbH

January 2014
Executive Summary

The increasing connectedness and digitalization of business processes changes the character of IT- and especially SAP-landscapes, ranging from closed systems to hybrid IT-environments.

These changes involve entirely new threat scenarios, to which the enterprises must respond within the scope of their security strategy.

The targets are not only large corporations; medium sized companies are affected by cyber-criminals as well. The attacks are becoming more sophisticated, and more often than not, also affect the production- and logistics systems (high-level-incidents) of the businesses.

An integrated security system for SAP-environments, including firewall, intrusion detection and malware protection, combined with standardized reporting, will become increasingly important in the future.

SAP now strengthens its user protection by integrating and certifying security solutions for the SAP NetWeaver platform.

The SAP virus-scan-interface (VSI) provides extensive security services and standardized administration for SAP-environments.

With its “Deep Security” product family, Trend Micro is one of the first certified providers able to offer this integrated protection to SAP users for Linux-based IT- and cloud-environments.
# Table of Contents

3  SAP Cloud Security Design  
5  SAP-Operation 2014  
8  SAP Security in the Cloud  
10 SAP Cloud Security Design  
12 SAP and Trend Micro  
13 SAP Security  
14 Perspective  
15 About Trend Micro  
16 Authors  
17 About CRISP Research  
18 Copyright
For many large and medium sized companies SAP-systems are the informational backbone of the business processes. Regardless whether it is financial- and accounting systems, supplier management or production control - the data on SAP systems is business-critical and therefore it requires special protection.

For many CIOs it has been fairly simple to guarantee this protection up to now, while the SAP-systems were hidden in the back-end of the company-IT system and only marginally connected with the outside world. But the change toward completely digitalized customer relations and business processes requires much stronger openness and connectedness of the SAP-systems with a large variety of cloud-based and mobile applications.

In an effort to provide an ideal “Digital Customer Experience“ to customers and partners, many business processes are now offered as light-weight, user friendly apps and/or cloud services that are not only used on terminals and PCs’ and secure company territory, but also on tablets, notebooks and smartphones. The access to critical company data therefore does no longer only take place in controllable environments, which provides a significantly higher attack potential than in previous years, because networking- and vulnerability levels are closely related in this nice new cloud-world.

Operating SAP-based applications will pose a much higher “Risk Exposure“. SAP has implemented significant changes during the past two years as well, and prepares its software solutions to be “cloud-ready“, in an effort to pave the transition into “digital business for its customers. Not only have new cloud platforms (e.g. SAP HANA Cloud) and a multitude of on-demand services (e.g. Financials, HCM) been developed, but the SAP-portfolio has also been significantly expanded by a wide variety of acquisitions (Success-Factors, Hybris, Ariba). The new cloud solutions are now connected with SAP-core technologies within the scope of a large integration-offensive.
Hybrid SAP-architectures, consisting of a multitude of flexible combination options for solutions and operational concepts are emerging at the end of the journey – from on-premise infrastructures up to public cloud services.

But this newly acquired flexibility in development, provisioning and operations of SAP-based solutions also has a downside; a significantly higher complexity level. It complicates protection of mobile and virtual solutions and renders the classic security management a difficult and expensive task. Without security management automation and virtualization, complex SAP-environments will be difficult to protect in the future.
SAP-Operation 2014
New Models and Strategies

The operation of SAP-systems has changed significantly within the last 24 months. This also applies for developing and testing new SAP solutions. The following trends continue to play a large role in upcoming years as well:

- **01. Unix-Linux-Migration**
- **02. Virtualization**
- **03. Cloud Computing**

**01. Unix-Linux-Migration**
Although many enterprises have migrated their formerly RISC/Itanium-architectures operated SAP-systems, the change to Linux-systems is still an important topic. In 2014 more than 15% of the OS-budgets are still allocated to UNIX.

In comparison to Linux and Microsoft, UNIX, despite several technical advantages, becomes a cost-trap. It will be difficult to justify the administration- and maintenance costs on a median- to long-term basis. Crisp Research anticipates that approximately 25% of the currently installed basic Unix-systems will disappear within 24 months and/or be ported to Linux and Microsoft Windows. Consequently, the remaining Unix-users have to think about how to provide an integrated security management for their SAP-landscapes in the future.

**02. Virtualization**
In addition, the trend for the virtualization of server-, storage and network infrastructures used to operate SAP systems increases. Crisp Research estimates that in Germany only approximately 45% of SAP-systems are operated on virtual infrastructures. This provides room for improvement. Especially medium sized companies still have to carry out the generation-change to virtualized infrastructures and cloud platforms.

However, the effort and complexity of security management with regard to the administration of virtual equipment (VM) and/or equipment-pools is underestimated by many IT-decision makers. Security updates and patches are fre-
quently still performed manually per individual VM and can only be marginally automated. This not only involves security- and compliance risks, but may also influence the TCO of a virtualized operating environment in a sustained negative manner.

03. Cloud Computing

The magic word of past years did not stop at the operation of SAP- systems either, although these business-critical workloads surely are stragglers in the big cloud-hype – which is justified. The requirements with regard to availability, stability, scalability and security could not completely be guaranteed for a long time. Since then, a multitude of service providers have started to offer flexible charges for cloud-environments in managed-, managed private or hybrid operation concepts. The users appreciate this, and Crisp Research anticipates that approximately 35% of the SAP-hosting contract volume in Germany will be allocated to respectively flexible cloud-models in 2014.

In addition, companies also use public cloud platforms such as Amazon AWS for their web-applications docked to SAP, for instance, e-commerce-shops, mobile apps or portals.

OVERVIEW
Cloud-Operation Concepts

MANAGED CLOUD/ CLOUD HOSTING
Managed Service, Shared Infrastructure hosted by Provider, Enterprise-grade SLA

PUBLIC CLOUD
Self Service, Un-managed, Shared Infrastructure hosted by Provider, Pay-as-you-go, standardized SLA

MANAGED PRIVATE CLOUD
Managed Service, Dedicated Infrastructure by Provider, Enterprise-grade SLA

PRIVATE CLOUD
Setup and operations of individual cloud infrastructures within an own data center respectively a colocation

“The Trend toward cloud computing requires an adapted security management for SAP-systems”

Dietmar Lummitsch
Director, IT-Processes and -Systems Jungheinrich AG

SAP Cloud Security Excellence
The operation of SAP-systems increasingly differentiates. New operational options, which can also be combined, are created. Development and testing of new SAP applications is now implemented in part on so called IaaS- and/or PaaS platforms. For example, compute resources on the Amazon AWS-platform, can not only be charged on a pay-as-you-go model but also being provisioned and de-provisioned instantly via a self-service dashboard. Therefore it is essential to coordinate and adapt the internal security management to these new operation- and development models.
It has to be acknowledged that the threat situation for numerous medium sized and large companies in Germany has significantly changed again within the last 24 months. If the majority of attacks on company networks were primarily recruited by avid hackers without a background of organized crime until now, the scenario seems to have reversed. The largest growth rate is currently in specific attacks committed by cyber-criminals.

The attraction and/or vulnerability of the targets (companies, authorities etc.), as well as the easy availability of malware and spyware technologies enable the criminals to profit from their attacks.

The flourishing illegal trade with stolen user data, credit card numbers or patent information through the internet additionally increases the attraction of this type of cybercrime. It is clear that the danger of being singled out by cyber-criminals is no longer limited to internet companies and very large enterprises. Medium sized companies have also become targets of sophisticated cyber attacks that affect the production- and logistics systems in addition to the IT-networks (“High-Level Incidents“).

Based on the estimation by Crisp Research this does not only represent a change from “Low-Level“ to “High Level“
The number and relevance of the attacks on IT-networks have rapidly increased. The attackers also no longer use singular attack tactics, but combine diverse technologies and tactics into so called “multi vector” attacks. For example, DDoS-attacks are combined with SQL-injections. An additional factor is the targeted spying out of victims and exploiting the weakest link in the chain – the human being. Even experienced users are vulnerable to phishing for user data and passwords through social-engineering procedures.

In addition to the targeted attacks, the standardized attacks, using malware still play a large role. The consumerization of IT and the widespread use of social media not only spur the sharing of content and knowledge among colleagues and business partners but also spreads malware and spyware across the organization. Since users place a great amount of trust in the integrity of documents and data located in company-owned SAP systems, viruses and malware can sprawl rapidly.

Numerous companies encounter additional security risks by mobile access to SAP databases, because only if it is guaranteed that no damaging apps or “Man-in-the-Middle“ attacks can be performed with the mobile end-device, unauthorized access to company data can be prevented. It has to be stated that the new mobile cloud-world brings significant advantages for the users. Furthermore the integration of SAP-systems with mobile applications creates an entirely new dimension of flexibility. This however, also corresponds with an equally high security risk – the more connected users and devices are the higher is the potential security threat and risk exposure.

Since SAP-systems are the informational backbone for many companies, they also represent one of the primary targets for cyber-criminals. Protecting SAP-systems in times of cloud-based operational systems should receive the utmost attention.
SAP Cloud Security Design
Strategies, Concepts & Services

Several strategies, concepts and security services are required to operate complex virtual and/or cloud-based SAP-systems securely and according to company compliance regulations. Based on the Crisp Research perspective, the following are the most important aspects for a standardized and efficient SAP Cloud Security Policy:

- **01. Analysis and prioritization**
- **02. Coverage of all operational concepts**
- **03. Integration of diverse security-services**
- **04. Automation of security management**

**01. Analysis and Prioritization**

Facing the new security threats, companies have to increase their IT security budget. In most cases security strategies are being designed and implemented based on standardized procedures and product segments (firewall, content security, virus protection etc.). In times of targeted attacks on certain industries and companies this does not sufficiently meet the potential threats.

In addition, companies must let go of the thought process of having survived numerous years without any incidents. Therefore it is essential to prioritize the applications, data or user groups in need of protection and utilize the available skills and budgets accordingly. SAP-systems should be protected by an adequately high protection factor, because they provide the most valuable business data, but also expose areas where data may be compromised due to increased networking (cf. above)

**02. Coverage of all Operational Concepts (“Hybrid Security“)**

Since SAP-systems are no longer operated on just a central system in the company-owned data center, now and in the future, the system security must be equally guaranteed across all physical, virtual and cloud-based infrastructures.
This applies to the systems internally operated and administered, as well as the outsourced or docked platforms of cloud service providers or hosting partners. If the operational concepts demonstrate a development toward hybrid scenarios, the security solutions must accommodate this trend and cannot stop at the border of a platform or architecture.

**03. Integration of Multiple Security Services**

In an effort to comprehensively protect the SAP-systems, the various security services must be managed with a standardized approach. Only if solutions designed to protect from denial-of-service-attacks, cross-site-scripting, SQL-injections or malware are coordinated, can combined and/or “multi-vector” attacks be prevented successfully.

**04. Automation of Security Management**

The automation of security processes is also an important aspect. Many companies still have a lot to accomplish in this area. For example, firewall updates on virtual machines still need a lot of manual administration work. The manual updating or patching of individual VM or VM-pools not only poses a security risk, but also significantly increases administration of the SAP-system’s virtual operating environments.

Only automated security processes can guarantee the security of virtual environments. Especially when VMs are moved from one platform to another within the framework of complex cloud-environments, more often than not the VMs are not at the most current security level.
In an effort to ensure security and integrity of its customers’ critical business data and protect its technology platforms and software solutions, SAP has relied on close partnerships with leading security providers for numerous years.

**Trend Micro Deep Security - SAP Certified Based on VSI 2.0**

Trend Micro is one of these partners. They are considered one of the most innovative technology providers in the area of integrated security solutions for complex cloud environments.

Trend Micro was recently certified by SAP as one of the first security providers for the integration of its security solutions Deep Security in SAP NetWeaver for versions 2.0 and the SAP virus-scan-interface (“SAP Certified – Integration with SAP NetWeaver“).

The integration of Deep Security in SAP-Systems has two directions of impact. The first is securing the operations infrastructure. In this context, Deep Security protects the hosts used to operate SAP NetWeaver and/or support functions (e.g. databases), via firewall and integrity monitoring.

Secondly, Deep Security 9 provides extensive malware protection for the SAP-NetWeaver-platform. Deep Security uses the SAP Virus Scan Interface (VSI) to search and analyze all types of contents and documents, including integrated graphics and active contents (such as Java Script), in order to identify and isolate damaging contents. This protects users and platform from malware. Furthermore, standardized reporting for administrators is performed, which enables easy adaption of guidelines (“which document types are authorized?”) and it is also made available to SAP-systems via NetWeaver-VSI.

The solution is currently optimized for the operation of Linux-based SAP-systems and supports the platforms listed on the left side.
It can be stated that Trend Micro and SAP have taken a big step toward integrated security management for Linux-based hybrid IT- and cloud-environments by integrating Netweaver und Deep Security (Version 9).

Users operating their SAP-systems in virtual and cloud environments, now have a chance to standardize the majority of their security processes and additionally protect their SAP-systems against new threats, such as Cross-Site-Scripting.

In this context, the high integration and centralization degree of the security management processes can be considered Best Practice. Users are able to significantly reduce administration- and reporting costs (keyword “compliance) when securing their SAP-systems, because no different security products by different manufacturers has to be managed and integrated. Especially the standardization of alert-management and reporting on a single console makes the tasks of security delegates easier and provides the necessary overview of numerous threat-scenarios.

The regulatory requirements can also be met and the security processes are “compliant” in accordance with e.g. PCI DSS 2.0, HIPAA, FISMA/NIST or SSAE-16.
The radical change towards a fully digitized economy will represent the greatest challenge for CIOs’ and IT-decision makers in the years to follow.

In the future, interlocking with all types of cloud-systems will increase rapidly and it will primarily affect the SAP-systems that provide the relevant data at the back end. Securing these hybrid SAP-environments is the utmost priority.

To provide an appropriate protection level in light of the variety and critical aspects of threats and to manage the risks adequately, the IT-security segments (firewall, intrusion prevention, integrity monitoring and malware-protection), have to be interlocked and automated with each other on a higher level. Furthermore, the classic IT-security products have to be adapted to the requirements of the virtual computing world.

The back-up and patching of virtual equipment still poses a great challenge for many IT-administrators. Emergency-patches outside of the scheduled patch cycles can be quite intricate and costly for SAP-systems; not to mention the potential risk factors within the timeframe up to the fully executed patch.

It would surely be beneficial for SAP-users, if an integration of Deep Security and NetWeaver Platform on Microsoft-OS would be possible, since almost one third of the SAP-systems are still operated on Microsoft platforms. This applies for the Unix-based SAP-systems, which also are unable to run integrated security concepts, as well.
About Trend Micro

As a global leader in cloud security, Trend Micro develops Internet content security and threat management solutions that make the world safe for businesses and consumers to exchange digital information. With more than 25 years of experience, we’re recognized as the market leader in server security, virtual security, and small business content security. Trend Micro enables the smart protection of information, with innovative security technology that is simple to deploy and manage, and fits an evolving ecosystem. Our solutions are powered by the cloud-based global threat intelligence of the Trend Micro™ Smart Protection Network™ infrastructure, and are supported by over 1,200 threat experts around the globe.

Additional information is available at:
www.trendmicro.de/deep-security
www.trendmicro.de/sap
In his capacity as an IT Analyst, Carlo Velten has advised renowned technology companies in marketing- and strategy matters for over 15 years. His focus-subjects are Cloud Strategy & Economics, Data Center Innovation and Digital Business Transformation.

Prior to this, he managed the die “Cloud Computing & Innovation Practice” with Steve Janata at the Experton Group and initiated the “Cloud VendorBenchmark”. Previously, Carlo Velten was the Senior Analyst in charge at TechConsult where he was responsible for topics such as, Open Source and Web Computing. Dr. Carlo Velten is a jury member for “Best-in-Cloud-Awards“ and he is affiliated with the industry association BITKOM.

He has appeared as the key-note-speaker and moderator at conferences and events for numerous years. He writes for Computerwoche.de as a contributing editor and supports young startups as a business angel. In addition, he is politically active as the chairman of the manager forum for the Friedrich Ebert Foundation.

Steve manages the research projects for cloud computing, digital customer experience and mobility. He advises and supports IT-users and providers on their journey to a digital economy. Prior to his employment with Crisp Research, Steve was the Senior Advisor and Practice Lead for Cloud Computing & Innovation“ at the Experton Group. He has 15 years of experience as an analyst and strategy consultant in the IT-industry. Within the scope of his consulting career, Steve has worked with companies such as IBM, Microsoft, T-Systems and Telefonica, amongst others.

Steve Janata is author of numerous studies and professional articles. An expert in cloud, channel and digital economy, he is a sought after speaker and moderator at conferences and events. In addition, Mr. Janata is a member of the board at the manager forum Rhine/Main for the Friedrich Ebert Foundation.
About CRISP Research

Crisp Research is a European IT-research and consulting company. With a team of experienced analysts, consultants and software developers, Crisp Research evaluates current and future market trends. Crisp Research supports IT-providers in strategy-, content marketing-, cloud marketing- and sales questions. Cloud computing and digital business transformation are the main focus points at Crisp Research. We have an internal research team in our Crisp Research labs and test current cloud services and products under live-conditions.
Copyright

All rights to the present contents are owned by Crisp Research. The data and information shall remain the property of Crisp Research. Reproduction, including partially, requires the written authorization by Crisp Research.

Weißenburgstraße 10
D-34117 Kassel
TEL +49 561 2207 – 4080
FAX +49 561 2207 – 4081

MAIL info@crisp-research.com
WEB crisp-research.com
TWITTER twitter.com/crisp_research