SAP Landscape Security: Three Common Misconceptions

Protect the ERP System at the Heart of Your Organization

Martijn Sprengers MSc and Rick van Galen MSc

SAP is an attractive target for cyber attacks for both malicious insiders and external actors, aiming to attack critical business processes that are facilitated by SAP. Threats to SAP systems go well beyond rogue privileged SAP users, but extend to insiders within the company, corporate spies, cyber criminals and hostile intelligence services or nation states. Given such high-profile threats and a wealth of identified SAP vulnerabilities, it is clear that an integral and thorough approach is desirable to adequately secure your SAP landscape. However, there are still many misconceptions around SAP Landscape protection.

M. Sprengers MSc
is a manager at KPMG Advisory N.V.
sprengers.martijn@kpmg.nl

R. van Galen MSc
is a consultant at KPMG Advisory N.V.
vangalen.rick@kpmg.nl

Introduction

The most critical industrial, financial and core infrastructure systems in the world are controlled by SAP systems. SAP integrates and connects all aspects of your business processes and thereby often stores high value data such as finance, sales and personnel related data.

Traditionally, SAP security was mainly focused on authorization management and the segregation of duties amongst business users. Therefore, many SAP professionals refer to the term "security" as the process of creating and managing roles and profiles to restrict user activities over business information. Of course, these controls are important to the overall level of security within an SAP landscape, but this picture of SAP security is very limited. There are several other security threats that are often not properly addressed, also considering that SAP keeps on adding new functionality such as their future application platform HANA ([Scho15]). Additionally, security vulnerabilities in the technological components of existing SAP infrastructures and inadequate configurations are often not identified by our customers.

SAP is an attractive target for cyber attacks for both malicious insiders and external actors, aiming to attack critical business processes that are facilitated by SAP. Threats to SAP systems go well beyond rogue privileged SAP users,

but extend to insiders within the company, corporate spies, cyber criminals and hostile intelligence services or nation states. Given such high-profile threats and a wealth of identified SAP vulnerabilities, it is clear that an integral and thorough approach is desirable to adequately secure your SAP landscape. However, there are still many misconceptions around SAP Landscape protection. We will discuss the three most common ones.

Common Misconceptions in Protecting the SAP Landscape

Misconception 1: Protection is about systems aka "Securing the systems that actually store the critical data is sufficient"

Many organizations perceive that security is about systems. They reason that if the systems that actually store the data are secured, the risk of unauthorized data modification or confidential information leakage is minimal. A good example of this behavior can be observed in the scope of many financial statement audits. Cyber security firms are usually asked to only assess the adequacy and security of (SAP) systems and related databases that actually process and store financially relevant data. However, to quote SAP itself: "The pace of business is as fast as it has ever been, and it is only continuing to accelerate. To compete and win in today's market reality, companies must fundamentally transform their business models, processes and the IT operations that support both" ([SAP16b]). Therefore, SAP either is or will be at the heart of an organization's business and its most critical processes. As such many non-SAP IT systems, employees and third parties need to have access, creating a myriad of opportunities to misuse any of these logical access paths. Have you ever thought about how many interfaces and connections a single SAP instance could have? It is not about systems, it is about protecting the chain. What is the use of protecting the system that actually holds the data while other, connected, systems that can access that data are insecure? In our experience, it is especially the security of the SAP Solution Manager that is often overlooked, as this particular SAP system can act as a gateway to access any other connected SAP system, including the most critical ones. During our technical assessments, we often see that the Solution Manager can be easily compromised, thereby directly impairing the security of the systems that actually store the data.

A root cause of this problem can be isolated thinking. Traditionally, an important distinction can be observed in administrating and securing SAP systems: the distinction between the SAP Basis and the SAP Security team. In a typical organization that runs SAP, the Basis is responsible for keeping the systems and interfaces running, whereas the Security team deals with access authorizations and Governance, Risk & Compliance (GRC) in the application itself. As a result, neither of the two teams takes responsibility for the security of the operating system, network or database nor do they focus on securing the chain. There needs to be responsibility for connecting all the separate worlds involved in securing the chain and get the specialists thinking about the actual risks in the landscape.

Misconception 2: Security is about compliance, or: "Patch frequently and implement the SAP security baseline to protect against all attacks"

Mid 2014, SAP finally released their security baseline template. A document that they should have developed long before, just like any other large software company or IT vendor. The document is comprehensive and covers almost all aspects of securing a SAP Landscape, the current version (1.9) has 149 pages ([SAP16a]). However, we have not seen a single organization that could implement the entire baseline and have their SAP infrastructure comply with the described controls. The same holds true for the security update process. Again, SAP has released a comprehensive document to describe how to apply patches and individual security notes. But if you need 93 slides to explain a patching process, you cannot expect all organizations to fully implement such a process, let alone to operate it effectively.

Apart from this, no organization can keep up with the pace with which new (security) patches are released, averaging about forty per month ([SAP15]). SAP recognized this as well. If you are not installing each and every individual note, they recommend to at least install the support packages frequently, as these combine multiple critical (security) patches. However, since the component release 610 in 2001, SAP has released 11 other major components and a staggering amount of 287 support package levels. Installing a support package or upgrading to a newer component release often requires thorough testing and days of downtime, which can have a major impact on business continuity. SAP's patch release process simply overwhelms the support teams, allowing critical security holes to remain or be created.

But even if you are able to keep up with the patch frequency and even if your SAP Landscape complies with the baseline, you will still not be protected against one of the most common and prevalent attack types: imper-

The SIEM fallacy: "Let's collect all logs first and then find attackers"

sonation ([Micr14]). During an impersonation attack, (remote) adversaries trick end-users into clicking on a link or installing infected software. Once the computer of the end-user is infected, the adversary can remotely control the system, often without being noticed. If the infected end-user has high privileges in the SAP system (i.e. many organization have implemented Single-Sign On for SAP, or else the adversary just needs to install a keylogger and wait for the victim to login to the SAP GUI), the adversary can modify or obtain unauthorized access to critical data. Even if the infected end-user only has limited privileges, a successful attack can still be launched. With information gathered online, the adversary can identify which users within an organization have specific access rights in the SAP system. For example, to bypass the segregation of duties to modify a bank account number it is required to identify the requester and approver. Then spear phishing attacks are typically used by attackers to both impersonate the requester and approver and have the malicious request approved without consent of the victims. Attack paths such as these are extremely prevalent in practice: because of their valuable data, SAP systems are subject to highly targeted attacks, against which no tenable compliance rules can be created.

Misconception 3: Security and vulnerability monitoring is the holy grail aka "Let's collect all logs and find attackers"

Some organizations have recognized that the threats on infrastructure and application levels are becoming more critical and may provide attackers with unauthorized access to their most valuable data and business processes. Therefore, they consider it imperative to develop a broad, enterprise-wide view on SAP security, including security and threat monitoring of their SAP Landscape. While we encourage this development, we have seen many organizations struggle with implementing a good monitoring strategy and corresponding threat management. For example, the strategy "collect all logs first and then determine which abuse cases to monitor" hardly ever works. Far too often, organizations end up with many false positive alerts, queries to the SIEM system that take ages and standard, vendor provided, use cases that do not detect any sophisticated or targeted attacks. You still end up with your data stolen or your system left out-of-business if you are hit by a carefully planned targeted attack. Monitoring should be implemented based on behavior and scenarios: try not to detect the use of exploits in your SAP environment but focus on attack vectors that revolve around impersonation. Many of the prevalent attacks are not sophisticated at all, but attackers focus on exploiting design weaknesses as these are considered far more reliable (and cheaper) attack vectors than exploiting vulnerabilities ([Abra16]).

And even if you have good monitoring in place, it still acts as a signaling function: only very few monitoring tools will prevent attacks. It is therefore the balance between preventive, detective and responsive measures that organizations should seek. Why spend millions on a detection system if you do not have a communication plan ready?

Conclusion: Improving the Digital Resilience of Your SAP Landscape

The three misconceptions above share a common element: SAP security is a complicated process that may not be covered by focusing on individual aspects or compliance. Although these individual aspects are an attractive way of limiting scope and obtaining a sense of control, all of them on their own only yield a false sense of security. Considering the critical nature of the SAP landscape of any organization that has one, these approaches are just not sufficient.

Securing the SAP landscape can only be done by taking an attacker's perspective. What, exactly, is the organization trying to defend itself against? What type of data is so sensitive that it may not be leaked, and which business processes must be protected from fraud? Which internal and external actors can be identified that present these threats, and what methods do they have at their disposal? With these questions in hand, one may draft a scenario based approach in which an SAP landscape may be assessed from the attacker's perspective, and answer questions about whether the cyber incidents that the organizations is most afraid of can actually happen in practice.

References

[Abra16] J. Abraham, *How to Dramatically Improve Corporate IT Security without Spending Millions*, Praetorian, July 2016.

[Micr14] Microsoft, *Mitigating Pass-the-Hash and Other Credential Theft, version 2*, 2014.

[SAP15] SAP, *Security Patch Process. Implementing SAP Security Notes: Tools and Best Practices*, November 2015.

[SAP16a] SAP, Security Baseline template version 1.9, August 2016.

[SAP16b] SAP, *The Digital Oil and Gas Company*, 2016, go.sap.com/solution/industry/oil-gas.html

[Scho15] T. Schouten and J. *Stölting, Security Challenges Associated With SAP HANA*, Compact 2015/4.

About the Authors

M. Sprengers MSc is a manager at KPMG Advisory N.V. and has more than 7 years of relevant experience with IT Security. He is specialized in security framework reviews, ethical hacking, SAP landscape security, and red teaming. The combination of these aspects allows him to show organizations the real-life scenarios of bypassing security mechanisms, instead of purely theoretical security offense and defense approaches, as well as to construct effective and adequate cyber defense tailored to each organization.

R. van Galen MSc GPEN is an ethical hacker and a cyber security consultant with KPMG. He graduated on the implementation of a cryptographic mobile payments protocol, and joined KPMG in 2014. He acts as a technical specialist on SAP security and mobile security within the cyber security team.