Know and Protect Your Typical SAP Attack Surface

By Christoph Nagy, SecurityBridge

This article exams the typical attack surface for SAP, a world leader in business software.

SAP is the worldwide market leader for business software and the only software manufacturer from Germany that plays a role in the global market. SAP customers generate 87% of the worldwide trade volume. Because business-critical processes run on these systems, they must be protected.

SAP's original concept was to provide standard software for standard processes, but the manufacturer recognized that no two companies are alike. Each SAP system contains an average of two million lines of custom ABAP code. Experience has shown that historically grown user-defined applications include many vulnerabilities. One critical vulnerability per thousand lines of code means a typical SAP system contains no less than 2,000 crucial vulnerabilities!

At its monthly Security Patch Tuesday, SAP provides information about the latest vulnerabilities discovered by the company and its customers, partners, and security experts (as part of bug bounty programs). The associated patches on how to close the gaps are announced simultaneously. From then on, the race between attackers and defenders begins, which the latter can only win if they install the patch quickly enough. No company should rely on these monthly notifications, as good and valuable as SAP Security Patch Day is it's not enough. Because so-called Zero-Days exist under the radar – vulnerabilities that are not yet generally known and for which there is no security update from the manufacturer.

But how can companies effectively tackle the security problem? The basic answer is simple: the better you know your SAP attack surface, the more likely you are to reduce the risk. Companies must assume that every application (and therefore every SAP system) contains serious security vulnerabilities that cannot be closed—because no patch is available. Waiting for the following SAP Security Patch Day cannot be a solution here, as criminals already know about the open gap and can exploit it. Here are ten steps you must take to protect your SAP systems:

Monitor Your Attack Surface

The attack surface is the sum of all possible entry points or attack vectors through which an unauthorized attacker can access a system or application. For example, to extract data or manipulate sensitive information, the smaller the attack surface is, the better it can be protected. In the SAP context, web-based access, for which the Internet Communication Manager (ICM) and the SAP Web Dispatcher are responsible, and the Internet Communication Framework (ICF)—via the SAP transaction SICF—should be particularly monitored and secured. In addition, connecting via the RFC interface (Remote Function Calls) is also vulnerable and can cause data leaks to the outside world.

All exposed services (HTTP, HTTPS, SOAP, WebService, APIs) must be continuously evaluated and inventoried. Any system service that is not used or does not serve a specific SAP business scenario should be disabled to reduce the attack surface. SAP services that do not require authentication should be given special attention. In SAP, they are located in the /public/ namespace (found in transaction SICF). Services such as /public/system_info are the first port of call for attackers to gather information about the SAP system during the reconnaissance phase of an attack.

Take Responsibility for Securing Your Cloud

In the on-premises operation of SAP applications, the company is 100% responsible for the security of its systems. Today, however, applications and services are increasingly moving to the cloud, and hybrid operation is almost the norm. Contrary to popular belief, using a hyperscale cloud does not automatically lead to reduced complexity of the company's security measures. The opposite is true: additional network connections must be secured, other responsibilities must be taken into account (shared responsibility model), and other attack vectors must be anticipated. Furthermore, complete cloud operation does not mean the company no longer has to worry about security in the application stack itself. For example, anyone running SAP on a server in the AWS cloud is still responsible for its security. Even with the application management service model (where the operational aspect is also outsourced), the company's responsibility for cyber security remains.

Anyone dealing with cyber security for the first time, as part of an assessment, is almost always faced with a wall of red lights. The problems seem to be piling up, but which one do companies need to tackle first? You can spend as much money as you want on security, but you will never achieve 100% protection. The solution can only be: Move away from one-time assessments to continuous vulnerability and patch management. The key to this solution is to prioritize and address those issues that pose the most significant risk to the company or are easy to fix.

Know Your Entry Points, Keep Your Attack Surface Small, Continually Patch

Vulnerabilities are constantly changing in complex environments, especially in light of upcoming S/4HANA migrations and SAP's cloud-first approach. The ERP system is not a box whose security can be established by connecting Security Information and Event Management (SIEM). SIEM systems collect log data, alarms, and other messages to evaluate them. In this way, they detect unusual patterns in IT systems and alert them in the event of an attack. SAP's Enterprise Threat Detection can complement conventional SIEM systems. However, SAP is an evolving ecosystem of technical components that are constantly being updated. SAP customers need a dashboard that gives the security, network, and SAP base teams an overview of the current SAP security situation.

Today, SAP users must be prepared for quasi-permanent patching of security vulnerabilities that occur immediately. To do this, they need an up-to-date security mindset to deal with Zero-Days at any time and securely protect SAP databases and applications against attacks. If you know your entry points and keep your attack surface as small as possible, you can achieve much with reduced effort.

Harden the Gateway - For Production And Also Development and QA Systems

The SAP gateway manages the systems allowed to access SAP; by default, it grants access to any host. Unfortunately, this can compromise SAP's underlying operating system (to name just one example). Therefore, access must be limited to those hosts that need to exchange data with the SAP system. Today, the SAP gateway has been hardened in most production systems. However, one still encounters development or QA systems with an unconfigured SAP gateway. These can be misused as stepping stones to other systems, potentially endangering the entire SAP landscape. Therefore, configuring the gateway to restrict access (to internally known hosts) is an essential building block for ensuring SAP security.

Apply Critical Patches

Patches should be implemented soon after SAP patch day; unfortunately, this can be challenging. Apart from the manual effort required for some security patches, it is typical for a system restart or other actions to be necessary that temporarily shut down the SAP system. If production lines are run on this, stopping them is sometimes associated with high costs.

SAP recommends that its customers check their notices and determine whether they apply to any of their systems. Tools such as SAP Security Advisory help with patch analysis. Security monitoring that includes information about SAP security advisories further reduces the risk of unpatched security advisories weakening the SAP security posture.

Track, Manage and Secure All Your RFC Interfaces

Remote Function Call (RFC) interfaces connect SAP systems in an ERP landscape; these connections can be an ideal means for attackers to jump from one system to the next. Therefore, RFC, ERP, and other interfaces must be secured by activating a dialog login that contains names and passwords. The challenge lies in the sheer number of interfaces; administrators often need more visibility, even in just one system. Therefore, a well-documented state of all RFC interfaces is as essential as securing them.

Check Your Internet Connection Services - Do They Need To Be Enabled?

In the whitepaper "Secure Configuration of SAP NetWeaver Application Server using ABAP," SAP lists several internet connection services (essentially ICF web services) that are known to be vulnerable and, therefore, should not be active where avoidable. The document dates back to 2012, but it wasn't until a few years later that SAP took one of the first steps toward "security by default" and disabled the services when installing an SAP system.

Unsecured web services will attract "specialized" SAP hackers, and other attackers who are less familiar with SAP technology will also try to use active ICF services to penetrate SAP. Therefore, SAP users should always check whether these (and other) web services need to be enabled and be highly restrictive.

Secure Your SAP Router, Web Dispatcher, and SAP Gateway

Even if ICF services are disabled, SAP systems should not be exposed to the Internet without security measures. Under S/4HANA and its multiple ways to connect and interact with customers and suppliers, most SAP systems today will be connected to the outside world in one way or another. Therefore, the SAP Router, Web Dispatcher, and SAP Gateway should be hardened as much as possible. It is also advisable to separate the systems so that the outward-facing applications exchange data on a different system than the internal ones.

Encrypt Client Access

Endpoint security is a market unto itself in the cybersecurity industry. Not so with SAP security, which deals with the security of an SAP system. While it's basically "just" the GUI and browser that needs to be secured, these endpoints are also the weakest points in SAP security. Usernames, passwords, vendor or invoice data - a significant amount of information is still entered manually via a terminal. If this data is not encrypted, attackers have an easy time accessing it.

Additionally, if usernames and passwords are affected, this data can cause even more damage to the attacked SAP system. To prevent this, SAP developed its technology for encrypting data exchange between clients and servers, but unfortunately, not all customers use it. Make sure you do.

Control Authorizations Assignments

SAP allows a granular role and authorization concept to adapt SAP systems to incorporate processes. The downside is complexity. Due to numerous possibilities, role and authorization projects are often among the most complex projects in the SAP world.

More importantly, these projects are prone to shortcuts from a security perspective. For example, instead of setting up detailed authorizations for each user, access to specific transactions and processes is often granted generously. The danger of generous permissions and historically established roles are potentially harmful combinations. Therefore, control over roles and authorizations is one of the most critical issues regarding the security of SAP systems. In fact, for some years, it was synonymous with SAP security as a whole.

About the Author

Christoph Nagy has 20 years of working experience within the SAP industry. He has utilized this knowledge as a founding member and CEO at SecurityBridge–a global SAP security provider, serving many of the world's leading brands and now operating in the U.S. Through his efforts, the SecurityBridge Platform for SAP has become renowned as a strategic security solution for automated analysis of SAP security settings, and detection of cyber-attacks in real-time. Prior to SecurityBridge, Nagy applied his skills as an SAP technology consultant at Adidas and Audi.