PUBLIC

Mitigating the Threat of Ransomware to Business-Critical SAP® Applications

An Introduction to Ransomware for IT Leaders and the Steps You Can Take to Protect Your Systems

December 2021

ONAPSIS

THE BEST RUN SAP

Table of Contents

Introduction

Almost every day, we hear in the news about another case of ransomware. While ransomware is not necessarily a new trend in the world of cybersecurity, in the past year it has quickly elevated its profile to become one of the biggest concerns for chief information security officers around the world.

The FBI defines ransomware as "a type of malicious software, or malware, that prevents you from accessing your computer files, systems, or networks and demands you pay a ransom for their return. Ransomware attacks can cause costly disruptions to operations and the loss of critical information and data."[1]

While the name alone focuses attention on paying a ransom for access to your data, as the FBI notes, there's a whole other set of impacts with these attacks – disruptions to operations, downstream quarterly financial effects, critical data loss, or even human impact.

Most, if not all, ransomware infections rely on two vectors to obtain access to a target system and subsequently exfiltrate and then encrypt files – the exploitation of vulnerabilities (such as the abuse of either unpatched system vulnerabilities or misconfigurations in a service) or the leveraging of valid credentials obtained via stuffing attacks, spear phishing, or underground markets.

Some examples include Lilocked ransomware, which exploits out-of-date versions of the Exim message transfer agent to gain a foothold in a target environment, and Rex ransomware, which tests and exploits vulnerabilities in Drupal, WordPress, Magento, Kerner, Airos, Exagrid, and Jetspeed to gain admin credentials. In essence, much like any other type of malware, attackers simply need **any** access to their targeted system that grants them permissions to write or execute files to potentially perform a ransomware attack.

Throughout the first half of 2021, as more and more reports of ransomware affecting larger organizations populated the headlines, customers of both SAP and Onapsis have inquired around guidance and best practices to help them prepare and protect their business-critical SAP® applications from potential ransomware attacks. These are valid concerns, because with so much relying on these critical systems, any ransomware attack affecting SAP applications could have significant impacts to the business.

This document by Onapsis and SAP is our joint effort to introduce our customers to this topic and summarize steps they can take today to protect their business-critical systems and mitigate this very real threat.

[1] *Ransomware, FBI.*

Preparing for a Ransomware Attack

As the threat of ransomware continues to grow for larger organizations all over the world, it is imperative to focus on some key actions, best practices, and controls that any company should ensure are in place to mitigate the threat of ransomware. These are split into three main categories: preventive, detective, and reactive.

PREVENTIVE CONTROLS

The root causes of any ransomware attack stem from allowing an unauthorized attacker to execute code and read or modify files and data in IT systems. Arguably, if organizations have good security programs and apply basic security hygiene, it helps prevent the initial infection in the first place. Here are 10 preventive controls that should be strongly considered as part of a preventive ransomware strategy.

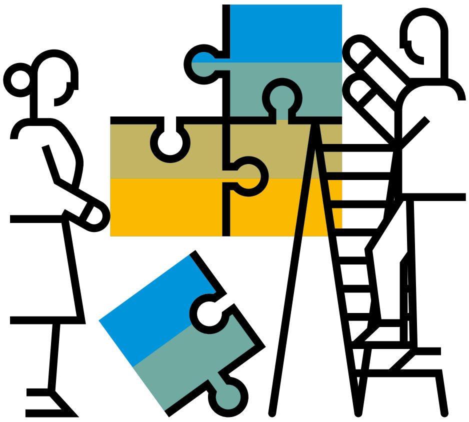
1 Identification of critical assets

For SAP customers, traditionally the entire SAP landscape could be considered critical assets. This might include SAP technology as well as servers, databases, and any other system integrated into the business processes supported by SAP technology. SAP Solution Manager, an IT management solution, provides a good overview of the assets that are connected to it and offers a good starting point for building an inventory. However, other data points, sources, and applications that help identify critical assets and their relationships or connections should be used as well, since it will deliver additional context on top of what SAP Solution Manager provides.

2 Assessment of risks and vulnerabilities in critical assets

The diverse components that build up the SAP application and technology stack should all be assessed to understand their unique and interconnected risks and vulnerabilities. Traditional vulnerability scanners might be good enough for the operating system, but organizations need to build the processes and use more specialized scans to understand what risks and vulnerabilities might affect the different components. (See Appendix 1 for more data about the most critical vulnerabilities commonly exploited by threat actors against SAP systems.)

This should be approached by considering both an external view (for example, by identifying exposed services, leveraging firewall and intrusion detection capabilities, and using external services such as Shodan to properly map exposure) and an internal one (such as taking an active software inventory and tracking changes in the systems).



3 Refinement of business continuity plans

Define, communicate, and test existing business continuity plans (BCPs) to ensure they consider scenarios of business processes and SAP application. Start by mapping existing technology assets, their relationships, and owners into the BCPs, and ensuring they are accounted for in any incident response plan.

Furthermore, ransomware scenarios should consider a diverse set of ransomware attacks, including scenarios that affect key business processes supported by SAP applications, as well as incident response runbooks with backup procedures and protocols and SAP-specific instructions.

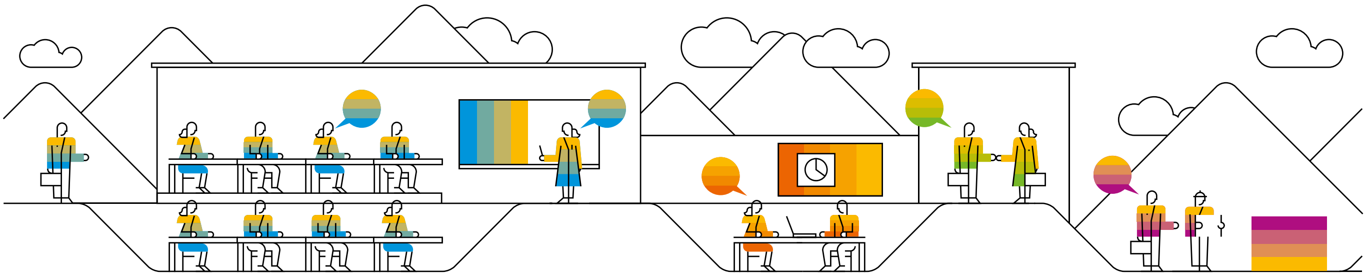
It's important to consider all scenarios when preparing BCPs, and whether teams are appropriately prepared for them. These scenarios include a rebuild of the whole SAP environment and the failure of a critical system restore. You should also consider how long it may take to restore all files affected by a ransomware attack if you had a decryption key.

4 Monitoring for changes in code

Vulnerabilities and compromised code could be introduced into SAP applications by means of malicious activity as well as through unauthorized access. Having the ability to detect malicious changes to custom code and configurations in SAP will help reduce the likelihood of initial infections from outside attackers as well as minimize the risk from potential attackers inside the organization.

5 Operational and user awareness

A lack of user education is partially the problem in a ransomware attack, as the initial infection may come from a variety of attack vectors, and attackers often target higher profile end users through social engineering techniques. It is very important, therefore, to train SAP users on security best practices so they stay alert when visiting public Web sites, and take care when they receive and download something, or execute an action. While IT administrators should leverage multi-factor authentication or secure workstation privileges (among other operational activities), user awareness will complement these activities by potentially reducing the risk of accidental user "collaboration" with infections.



6 Application of the latest security patches

As mentioned in the introduction, ransomware exploits well known vulnerabilities; SAP systems are no exception. It is highly critical to keep systems up to date in terms of security patching. A process to assess, analyze, and prioritize SAP Security Notes should be implemented.

7 Securing the landscape

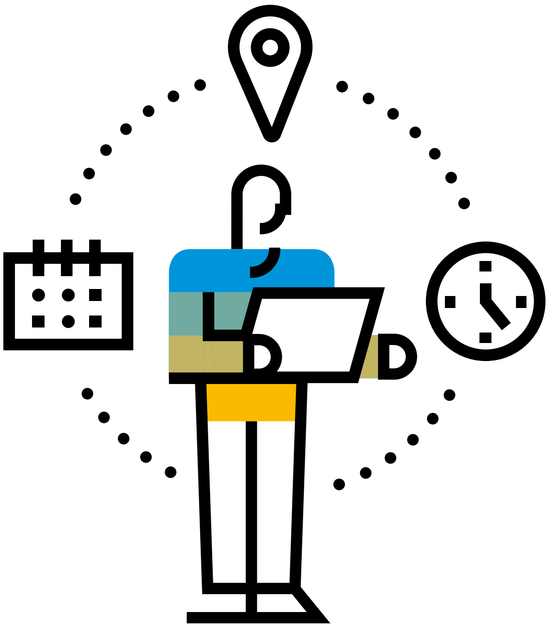
SAP systems operate within an interconnected ecosystem. Different types of systems (development, quality assurance, and production) are all connected to allow for efficiencies in implementing changes according to the proper change management process. Most ransomware has well-articulated and highly effective mechanisms to propagate both vertically and horizontally as well. Organizations need to have the proper processes and the right solutions to secure not just the production systems but the entire SAP landscape.

8 Gaining new visibility and insights with threat intelligence

Timely, impactful threat intelligence programs can provide insightful information about current tactics, techniques, and procedures used by threat actors. They can also provide early alerts about new ransomware campaigns as well as actionable intelligence for security teams responsible for designing and implementing security controls.

9 Building security event monitoring and response capabilities

It is paramount to have the proper tools not only to centralize security events but also to monitor and react to potential threats affecting the SAP landscape. Having up-to-date information from multiple sources such as security logs, traces, and logging information will allow security teams to identify and fix or mitigate security issues faster. Implementing proactive controls and rules to detect malicious behavior could also help reduce the impact of potential unknown vulnerabilities.



10

Implementing a broader “defense-in-depth” model

Since ransomware commonly exploits different vulnerabilities in a system, a layered defense approach to security is recommended as it can significantly reduce the risk of an infection. A layered “defense-in-depth” approach can potentially mitigate, inform, or even block the infection process even if a threat actor bypasses other security measures.

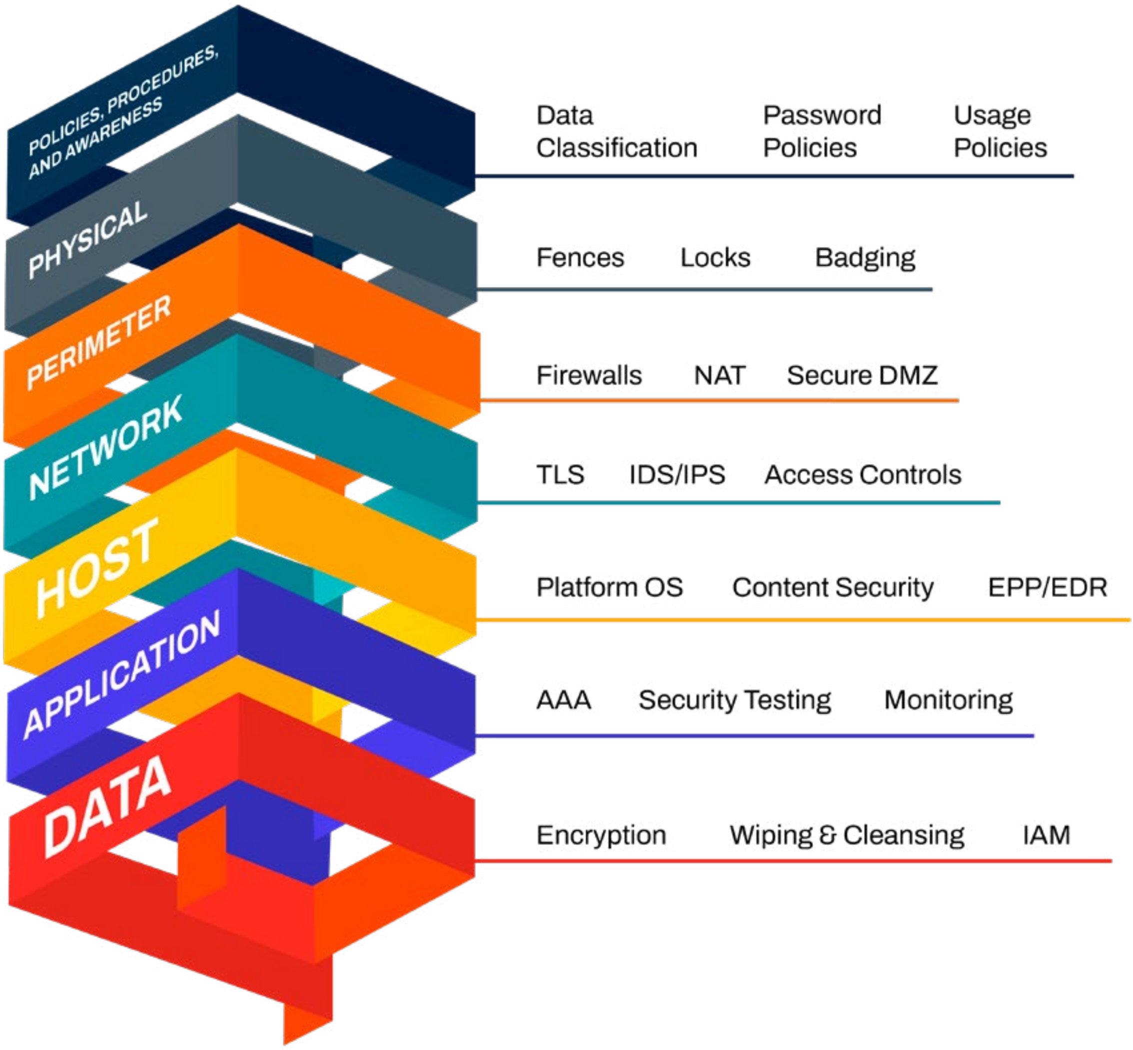


Figure 1: Defense-in-Depth Security Model with Examples

DETECTIVE CONTROLS

Once malicious code is executed by ransomware, it's critical to have endpoint security in place. This control detects the malicious behavior in time (for example, it may identify the number of file read/write data per unit of time) to block that process (the compromise) from executing in the moment. This usually involves endpoint detection and response (EDR) capabilities that, arguably, should be monitoring every asset it can in the organization's IT Landscape.

Some important considerations related to EDR:

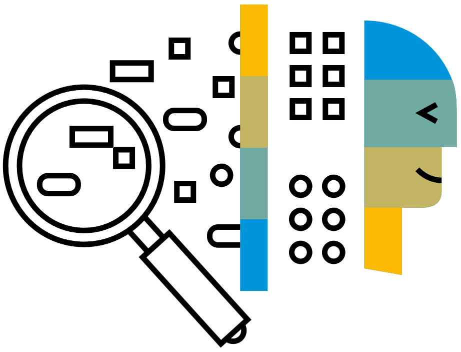
a. EDR is potentially limited based on the operating systems on which it can be installed and deployed. There may be endpoints or components where the operating system is not supported by the EDR technology, rendering them unprotected in some cases.
b. A security monitoring solution integrated with EDR could detect malicious behavior across the network (perhaps by potentially identifying data exfiltration and sudden spikes in data read/write or encryption activities on an endpoint). It could then isolate the process or endpoint that is responsible for that misbehavior, thus preventing greater lateral movement to other critical systems.

It's recommended to have a broad set of endpoint security capabilities (such as endpoint protection and endpoint detection and response) that detect ransomware, mitigate or minimize the impact, or outright prevent the compromise entirely.

While securing all endpoint devices – not only user laptops but also, for example, cloud desktop environments – is critical for detecting the execution of a ransomware file, it's important to note that other solutions deployed in a layered defense model, such as intrusion detection systems and intrusion prevention systems, can also be crucial tools in preventing exploitation.

Since attackers need execution permissions in order to complete a ransomware infection, it's imperative that the right threat intelligence is utilized in conjunction with detective controls. It's also vital that an organization leverages whitelisting for processes and applications to better control what can and can't execute on a system before a ransomware file itself has the opportunity to execute on a system.

Continuous monitoring of SAP activity to detect malicious actions also sheds light on potential ransomware attack risks. Malicious actions include the exploitation of weaknesses, malicious code creation and deployment, and unauthorized access. See Appendix I for more information about the most relevant vulnerabilities exploited by threat actors for SAP applications.



REACTIVE CONTROLS

Backups for critical systems are by far the most important reactive control that an organization has at its disposal when it is the victim of a ransomware attack. They could very well be the difference-maker, saving an organization from having to pay a hefty ransom and minimizing potential downtime from an attack. Backups won't prevent a ransomware incident, but if a backup plan is executed properly, it can significantly reduce an attack's impact and cost.

Backups can be considered the last line of defense, as they provide the ability to restore the systems or information from an older, archived version. There are five things to keep in mind with regards to backups:

1. Ransomware commonly targets Microsoft Windows endpoints. Consider leveraging a different operating system for backups or hardening Windows-based backup servers (by turning off remote desktop protocol) as much as possible to eliminate commonly exploited attack vectors.
2. Maintain at least one backup, or copy of a backup, on a different network – or better yet, on object-based storage – to ensure that your backups aren't compromised by a ransomware attack.
3. Ensure that there is a consistent backup process that runs continuously for the critical assets and systems in the IT landscape.
4. Regularly validate the integrity of backups to ensure they have not been tampered with.
5. Identify that the appropriate time gap between the identification of the compromise and the restoration of the last working backup is acceptable to the business. Verify that the restore process is proven and works across different systems.

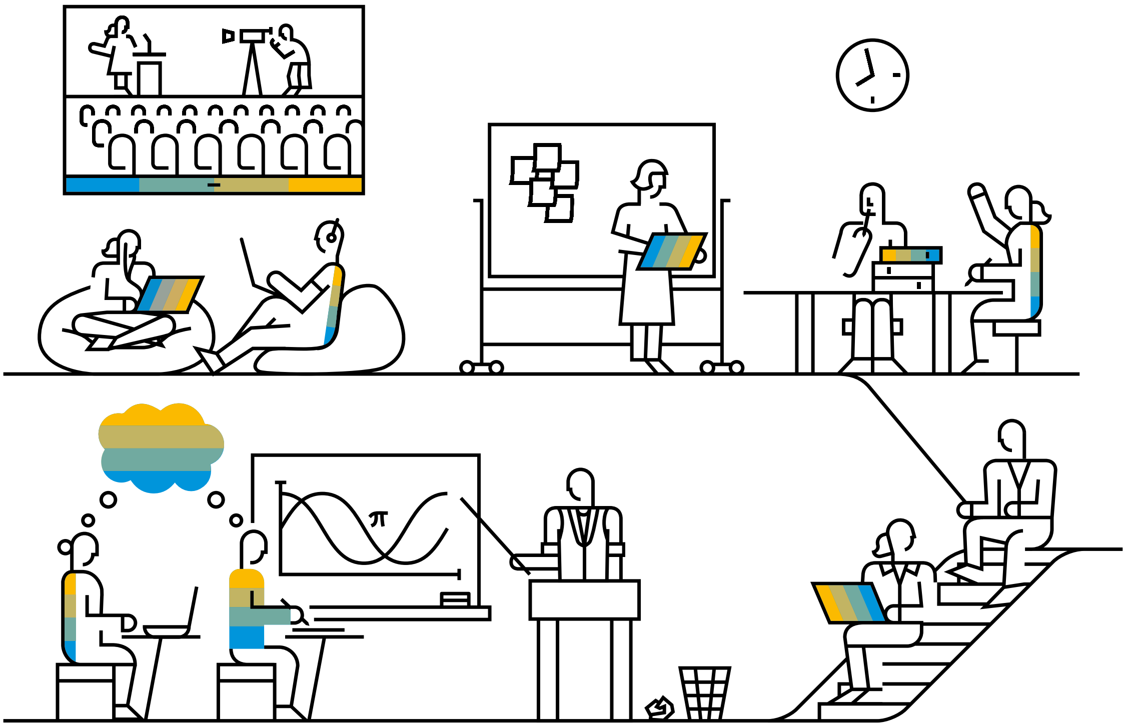
Responding to a Ransomware Attack

If an organization experiences business disruption from what could be a ransomware incident, it's important to follow the BCPs and incident response (IR) runbooks already established.

It's also important that they stay engaged with government agencies, computer emergency response team (CERT) organizations – such as the Cybersecurity and Infrastructure Security Agency (CISA) in the United States or the German Bundesamt für Sicherheit in der Informationstechnik (BSI) – and leading IR firms, especially since these entities frequently see the larger scope of ransomware infections. They can offer knowledge, assistance, and lessons learned from other incidents that they have encountered.

In order to minimize the impact of any attack, time is of the essence, so an organization's incident response plan should be fully vetted beforehand. It should also have a pre-defined, cross-functional response team (consisting of key leaders across different departments such as IT, legal, finance, and communications) as well as scenario runbooks with clear deliverables, incorporating the SAP components of the IT landscape.

An organization should also consider contracting a third-party data recovery specialist or ransomware recovery service team, and have it on standby, should a ransomware event occur. When the time comes for action, an organization's incident response should incorporate, at a minimum, the following steps.



STEPS FOR RESPONDING TO A RANSOMWARE ATTACK

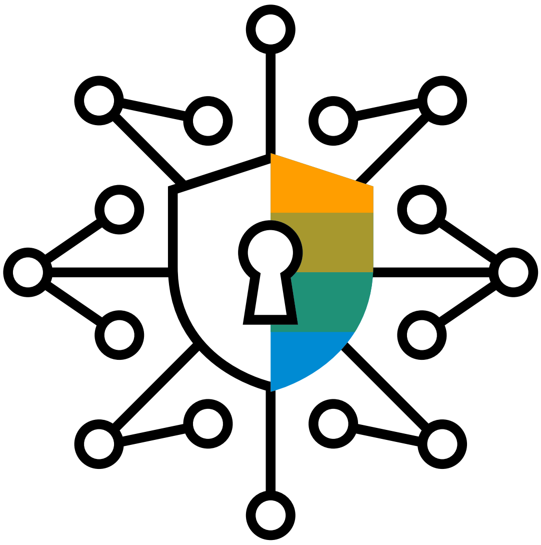
1 Scope to identify which systems were affected to ascertain whether those compromised systems can or cannot be isolated.

   a. If systems can be isolated, then isolate them immediately to prevent incoming and outgoing connections, preventing lateral movement of the initial infection.
   b. If systems cannot be isolated, refer to the BCP that incorporates the business processes supported by the affected systems, fall back to the backup process, and power off the affected systems.

2 Evaluate the affected systems to identify their optimal restoration and recovery processes.

3 Prepare an initial assessment of the facts that were captured during the initial reconnaissance and analysis. Internal and external teams – such as the SAP basis team (responsible for keeping the SAP landscape healthy and up to date), the security operations team, or the third-party incident response team – identified in the BCP should be activated to provide further context and insights into the attack across the IT landscape.

4 If the systems cannot be recovered initially, leverage traditional forensic techniques in order to capture as much system evidence as possible. This should include a system image, a system memory dump, whenever possible, and images or logfiles of affected devices. For SAP applications that are part of scope, organizations must be able to fully assess the history of what happened at the application layer, as it’s vital to consolidate information coming from the diverse application logs as well as from the database itself. Furthermore, this consolidation should also consider the context of SAP applications in order to be impactful and actionable in the event of a response.



Final Recommendations

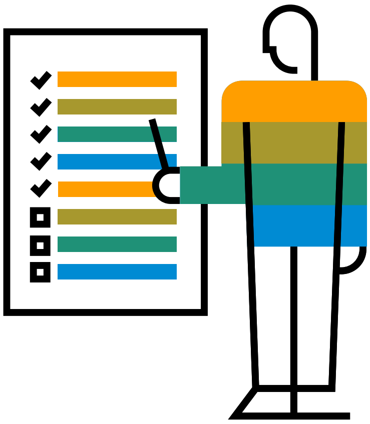
Ransomware is an evolving, lucrative business for threat actor groups. As this topic continues to trend in mainstream conversations and as more affected companies are targeted and subsequently pay ransoms, this threat will only continue to grow.

In this perfect storm, organizations with stagnant budgets and resources as well as lofty digital transformation initiatives often fall victim to attacks from more strategic, more knowledgeable threat actors that are actively targeting unprotected SAP applications[2]. These threat actors have the means and will to exploit critical vulnerabilities, running malicious software through unpatched, unprotected SAP application layers.

Business-critical SAP applications are complex systems made up of multiple software components, application servers, databases, and operating systems. Because of the interconnectedness and overall complexity of these systems, it's imperative that organizations take the appropriate time to prepare accordingly for the threat of a ransomware attack.

In conclusion, ransomware is a continuously evolving threat, with new threat actors, malware, services (for example "ransomware-as-a-service"), and payment models, such as collecting payments from both the enterprise and the victims – also known as "extortionware". To protect your most critical business applications and avoid being the next ransomware victim, SAP and Onapsis recommend that organizations consider a broader scope of controls for good security hygiene that includes all components in the SAP technology and application stack:

1. Maintain an inventory of business processes, components, versions, and assets
2. Apply patches to all components in the technology stack of SAP applications, based on a prioritized list
3. Ensure no vulnerabilities are affecting any component, including software vulnerabilities, misconfigurations, insecure integrations, and insecure authorizations as well as vulnerabilities in any custom-developed code or component
4. Perform regular backups and ensure those backups are properly executed and securely stored, and ideally separated from the network
5. Create a BCP that incorporates SAP applications in incident response runbooks in the event that the organization is the victim of a ransomware attack



[2] *Malicious Cyber Activity Targeting Critical SAP Applications, April 2021, CISA.*

Appendix I: Additional Information and Resources

SAP SECURITY PATCH DAY

Many vulnerabilities are currently being exploited[2] both automatically and manually by threat actors with the objective of, among other things, executing malicious code in unpatched, unprotected SAP applications. It is highly recommended that SAP customers patch their systems when new patches become available. To make this effortless, SAP has launched a regular SAP Security Patch Day, scheduled for the **second Tuesday of every month**; details can be found *here* on this wiki.

GUIDANCE AND RESOURCES:

- *Ransomware: Bedrohungslage, Prävention & Reaktion 2021* (Ransomware: Threat Landscape, Prevention & Response), May 2021, BSI.
- *Ransomware: Erste Hilfe bei einem schweren IT-Sicherheitsvorfall Version 1.1* (Ransomware: First Aid in the Event of a Serious IT Security Incident Version 1.1), January 2021, BSI
- *Ransomware*, FBI.
- Ransomware Guidance and Resources, 2021, CISA.
- *2663467 – Tips to Avoid a Ransomware Situation*, 2020, SAP.
- *2496239 - Ransomware / Malware on Windows*, 2017, SAP.
- *SAP Trust Center* – A single place for all your SAP security information needs.
- *The SAP My Trust Center* – SAP customer/partner site (requires an S-User login).
- *SAP Guides and Best Practices for Security* – How SAP can help you innovate on your path to becoming an Intelligent Enterprise.
- *The Secure Operations Map: Highlights and Best Practices for Securing SAP Solutions*, SAP.

Follow us

www.sap.com/contactsap

Studio SAP | 78247enUS (21/12)

No part of this publication may be reproduced or transmitted in any form or for any purpose without the express permission of Onapsis. The information contained in this document is subject to change without notice. This document is not warranted to be error-free. Complying with all applicable copyright laws is the responsibility of the user.

This content is made available by Onapsis on an "as-is'' and "as-available" basis and without warranties by Onapsis of any kind, express or implied, including warranties of accuracy, non-infringement, fitness for particular purpose or merchantability. Further, the information contained herein is not a commitment, promise, or legal obligation to deliver any capability, code, or functionality. Onapsis assumes no responsibility for your use of the content, and Onapsis shall not be liable for any damages, losses, costs, expenses, claims, liabilities, actions, demands or lawsuits arising out of your use of such content whether based on tort, including negligence, contract or otherwise.

Onapsis may have patents, patent applications, trademarks, copyrights, or other intellectual property rights covering the subject matter in this documentation. Except as expressly provided in any written license agreement from Onapsis, the furnishing of this content does not give you any license to these patents, trademarks, copyrights, or other intellectual property.

Onapsis and other Onapsis products and services mentioned herein as well as their logos and nomenclature are registered trademarks of Onapsis, Inc., and/or its affiliates. All other trademarks are property of their respective owners.

No part of this publication may be reproduced or transmitted in any form or for any purpose without the express permission of SAP SE or an SAP affiliate company.

The information contained herein may be changed without prior notice. Some software products marketed by SAP SE and its distributors contain proprietary software components of other software vendors. National product specifications may vary.

These materials are provided by SAP SE or an SAP affiliate company for informational purposes only, without representation or warranty of any kind, and SAP or its affiliated companies shall not be liable for errors or omissions with respect to the materials. The only warranties for SAP or SAP affiliate company products and services are those that are set forth in the express warranty statements accompanying such products and services, if any. Nothing herein should be construed as constituting an additional warranty.

In particular, SAP SE or its affiliated companies have no obligation to pursue any course of business outlined in this document or any related presentation, or to develop or release any functionality mentioned therein. This document, or any related presentation, and SAP SE's or its affiliated companies' strategy and possible future developments, products, and/or platforms, directions, and functionality are all subject to change and may be changed by SAP SE or its affiliated companies at any time for any reason without notice. The inform ation in this document is not a commitment, promise, or legal obligation to deliver any material, code,or functionality. All forward-looking statements are subject to various risks and uncertainties that could cause actual results to differ materially from expectations. Readers are cautioned not to place undue reliance on these forward-looking statements, and they should not be relied upon in making purchasing decisions.

SAP and other SAP products and services mentioned herein as well as their respective logos are trademarks or registered trademarks of SAP SE (or an SAP affiliate company) in Germany and other countries. All other product and service names mentioned are the trademarks of their respective companies.

See www.sap.com/copyright for additional trademark information and notices.

THE BEST RUN SAP®