EPI-USE LABS
value through innovation

SAP SECURITY CHECKLIST

PREVENT THEFT OF EXTERNAL DATA

KEY POINTS TO CHECK

□ Review physical and logical network security, as this is your first line of defence.

□ Close ports on the firewall that are not being used.

□ Ensure that the physical backups are secure, through encryption and/or proper access control.

□ Transport Security: Ensure that remote access is only granted through an encrypted means, like VPN.

□ Cloud security: Ensure that the cloud provider infrastructure setup is secure. Cloud service providers should ensure proper data isolation and logical storage segregation.

□ Systems should be kept up-to-date with vendor security patches. This includes the SAP systems, which are quite often lagging behind in security patches.

□ Use automation where possible to create security baselines that can be replicated across multiple systems.

□ Regularly use SAP-specific vulnerability scanners to find potential weakness in the system configuration.

□ Have a third party conduct independent security testing (penetration tests), where the system is “hacked” on purpose to test for vulnerabilities.

□ Users should not use privileged accounts like Administrator or root to perform their tasks. This is important for security and auditing purposes.

□ Perform regular reviews on audit logs, especially for privileged accounts.

□ Read and act on the security chapter of your SAP Early Watch Alert report and propagate the SAP Security notes through your landscape:

  □ The RSUSR003 report analyses the system for known passwords on standard users. Check this regularly on production and non-production systems alike.

  □ Ensure that debug access is not granted to anyone in Production (except in exceptional circumstances, where emergency access can be granted to certain users, only after approval and for a limited time).

HOW TO TAKE ACTION

□ Consider applying proactive retention periods, either via archiving or via a clean-up service like the one provided by EPI-USE Labs.

□ Remove only the sensitive parts of data on ex-employees or customers, or parts of a business that was divested.

□ Design and institute security programs to ensure continuous secure operations of SAP systems.

□ Encrypt data that is stored and communicated to external systems.

□ Secure communications between systems and parties using encryption so that communication is more difficult to intercept and decipher.

□ Develop a risk assessment and remediation plan, based on industry standards like ISO 27001 and SOC2, while taking into account legislation like GDPR and APP. EPI-USE Labs can help with this.

□ Use automation products to conduct periodic reviews of your system security configuration.

PREVENT THEFT OF INTERNAL DATA

KEY POINTS TO CHECK

□ Data at rest: Use storage encryption and consider preventing the use of USBs. Ensure that archived data is encrypted and backups are secure.

□ Data in motion: set up network segregation/firewalls between systems.

□ Data in use: unencrypted data in memory can be compromised by side-channel attacks from programs running on the same servers, so ensure such data is encrypted.

□ Apply two-factor authentication. This is crucial for users working remotely.

□ Ensure that a security policy is applied to the system, such as changing usernames and passwords. Don't use default usernames or passwords.

□ Segregation of Duties (SoD): locate and prevent gaps in SAP security role design that could allow users to access and exploit all steps of a business process (for example, by being able to both create and issue payment to a Vendor). Products such as Soterion's Access Risk Manager can be used to remove much of the complexity of this task.

□ Users should not use privileged accounts like Administrator or root to perform their tasks. This is important for security and auditing purposes.

□ Prohibit or limit emailing of sensitive data. If using email, ensure that the email technology uses encryption methods during email transmission.

□ Ensure that the non-production environment has the same stringent access controls as the production systems.

□ Ensure that sensitive data is not copied to non-production systems.

HOW TO TAKE ACTION

□ Use a tool such as EPI-USE Labs' Data Secure™ to mask or scramble whole clients or specific data where applicable.

□ Switch off emails in non-production systems. If testing email functionality in non-production systems, ensure that data is scrambled and set to email to specific addresses only.

□ Perform periodic reviews of user accounts to find those that have not logged onto SAP systems over a certain period. Lock or expire such accounts.

□ Perform periodic reviews of accounts to see who has access to which transactions, and to determine whether your users still need to access those transactions.

□ Perform automated code reviews to ensure that custom ABAP code doesn't introduce security vulnerabilities.

□ Implement an internal security awareness and training program.

PREVENT SENSITIVE DATA FROM BEING COMPROMISED OR EXPOSED

KEY POINTS TO CHECK

□ Data classification: Find and categorise all data in your organisation (Public, Sensitive, Private, or Confidential). It is not a good approach to try to protect all data from leakage. Rather prioritise your most sensitive data, find out where it lives, and aim to protect that. Examples are Payroll, Personally Identifiable Information (PII) or Personal Health Information (PHI).

□ Use two-factor authentication where possible, and especially when users are working remotely.

□ Determine where in the world and how your data is being stored. Each country has different laws pertaining to sensitive data, so check that your security policies and data storage architecture comply. If your customer support is outsourced, then consider the relevant laws in that region too.

□ BYOD (Bring Your Own Device) is becoming more popular in the workplace, and brings its own security issues. Set up company policies such as:

  □ Only allow whitelisted devices with the relevant security standards applied.

  □ Only allow authorized, whitelisted applications on BYOD devices.

  □ Devices must be configured to automatically install security updates.

  □ Screensaver passwords must be enabled if the device becomes idle.

  □ Configure app permissions for only the access that is really required.

  □ Keep all OS, firmware, software and apps up to date. Back up device data.

  □ Enroll in 'Find my Device', 'remote wipe' and similar services.

  □ Never store personal financial data on a device.

  □ Run mobile antivirus and scanning tools.

  □ Use Mobile Device Management software.

  □ Data at rest: Encrypt device storage

  □ Data in motion: All connections to the corporate networks and systems should be encrypted.

□ Make sure that SAP user is locked in Production.

□ Educate functional users about which data may be downloaded to MS Excel.

□ Review Data Warehousing feeds to determine whether you need all the sensitive data being extracted.

□ For Database Table Access (SE16), allow only queries or no access at all.

□ Apply appropriate email encryption for email transmissions.

□ Have a third party conduct regular independent assessments.

□ Review interfaces to ensure that sensitive data is not unnecessarily transferred and that transfers are encrypted.

HOW TO TAKE ACTION

□ Perform an audit of roles and access rights.

□ Design and implement secure role designs, taking into account legislation like GDPR and best practices like segregation of duties.

□ Mask or scramble sensitive data and thereby reduce the attack surface or number of places that data can be leaked from, whether accidentally or deliberately. EPI-USE Labs' Data Secure™ can help with this.

□ Apply appropriate encryption technologies.

□ Perform network/firewall and network security penetration testing.

COMPLY WITH LEGISLATION

KEY POINTS TO CHECK

- □ Learn about current regulatory privacy policies.
- □ Be aware that a form of GDPR is coming to Australia soon:
    - □ Read this comparison of GDPR vs Australian Privacy Principles.
    - □ Put policies and procedures in place to specify what data may be kept and for how long.
- □ Proactively remove sensitive personal data that is beyond the retention period state in your policies:
    - □ Train your staff members accordingly.
    - □ Determine which data is being held and where the responsibility for this lies across the company.
    - □ "Ring fence" separate parts of the business for regulatory reasons.

HOW TO TAKE ACTION

- □ Remove any personal data that you do not need to keep, as this increases your risk.
- □ Perform Data Privacy Impact Assessments (DPIA), as required by legislation like GDPR.
- □ Use the proprietary Privacy Comply™ methodology to implement privacy policies, standards and procedures to comply with privacy legislations in multiple jurisdictions.
- □ Implement and regularly test a breach response and notification plan.
- □ Set up policies and procedures similar to those of Production and apply them to non-production systems.
- □ Use a combination of EPI-USE Labs solutions Data Secure™, Data Disclose™ and Data Retain™ where applicable:
    - □ Data Secure replaces sensitive data with anonymous, but fully functional, test data – thereby removing the criminal's 'prize' (your data) and the risk.
    - □ Data Disclose finds, retrieves and presents a subject's data footprint across SAP systems – and as an added benefit, across non-SAP systems as well, if integrated with the former's API.
    - □ Data Retain proactively highlights sensitive subject data suggested for redaction, based on flexible pre-determined business rules, periodically as required by your business.

COMPLY WITH LEGISLATION

KEY POINTS TO CHECK

- □ Ensure that identifiable data in non-production systems is secured, either through applying access control based on role (Segregation of Duties) if the data can't be scrambled, or ideally, through scrambling.
- □ Create a dedicated client (with non-scrambled data) with controlled access given to limited users, and then create another main client and perform a scrambling run on either selected objects or the whole client.
- □ Scramble sensitive data. While your Dev and QA teams require fresh test data, they do not necessarily require access to your sensitive, private or confidential data:
  - □ Scrambling replaces sensitive data with anonymous, but fully functional, test data – thereby removing the criminal's 'prize' (your data) and the risk.
  - □ The quality of test and training data remains the same, without exposing any confidential data.
  - □ The values of fields are changed, while maintaining the integrity of the data and ensuring production-like behaviour.
  - □ At the same time, wider access can be granted to the non-production systems to allow more thorough testing, which will benefit your organisation.
  - □ Access should still be monitored and controlled even in non-production.
- □ Limit access and apply access-control methods to non-production systems. They should have similar control methods to that of production if possible.
- □ Make sure that SAP* user is locked and is only unlocked in certain circumstances (=best practice).
- □ Disable RFC connections back to production.
- □ Keep in mind that anyone with a developer key can read data from other clients in a system. So, for example, if there is a unit test client on DEV, then its data is accessible to developers in the DEV system even if they don't have a log-on for unit test. Third parties off-shore might also come into this category.
- □ Where production data is copied to provision non-production systems, the same controls as in Production should be applied in the non-production systems.

HOW TO TAKE ACTION

- □ Consider a data copy and security solution that can help you to:
  - □ Maintain data compliance by scrambling and anonymising data
  - □ Automate the copy process
  - □ Reduce the footprint when refreshing existing test clients or creating new ones
  - □ Enable you to copy selected data on demand

EPI-USE LABS

value through innovation

HOW EPI-USE LABS CAN HELP YOU GET ON TOP OF SAP SECURITY

Data Secure

Data Disclose

Risk Assessment

Consulting

Penetration testing

CONTACT US:

REQUEST

NAME:

EMAIL:

SUBMIT