MASTERINGSAP
An SAPinsider Company

Mastering SAP Collaborate
22 - 23 May, 2023
Crown Promenade, Melbourne

SAP Security and Data Protection Obligations

Paul Bisby

SAP Security Analyst – Commonwealth Bank

#MasteringSAP #MasteringSAPCollaborate

Who am i?

Paul Bisby

SAP Security Analyst

- Been working in SAP Security for over 23 years
- Worked across private and government organizasations
- Background also in Customer Service and Training
- Will watch and discuss (with or without intelligence) and and all sport. For the best convo start with AFL or Tennis ☺
- Happiest when travelling.

Disclaimer

The information and opinions are my own and are not a reflection of my employer – Commonwealth Bank.

It’s just a little change!

Why is Security Important?

- Security is critical in protecting personal data. This includes personal information of our external customers, our staff, our vendors and their representatives.
- Threats may be internal or external
- Security is everybody's job but for us it is our responsibility to be the expert
- IT'S THE LAW!!!! (OIAC, GDPR – but more about them later)

Three Key Questions

- What data do you have that needs to be protected?
- Who are my users/stakeholders?
- What Security Options do I have?

What data do we need to protect?

- Security is critical in protecting personal data. This includes personal information of external customers, staff, vendors and their representatives. Data that may be held by an organization includes –
- Customer Name
- Address
- Tax File Number
- Identification details (passport, drivers license)
- Date of birth
- Medical Records
- Gender/sexual orientation
- Financial or Transaction history
- Any and all data that is unique and personal to an individual or organisation

Data Classification

Once you know what data you have it is important to classify the data.

Some example classifications may be

1. Highly Protected / Critical – This may be data that if known could result in a severe impact to your Organisation. Eg Market Sensitive data, Merger and Acquisition.
2. Customer and Personal – Any personal information about Customers, Vendors, Employees etc.
3. Confidential – Information internal to your organisation but may only be available to a subset of people in the organisation
4. Group Use – Data accessible to all Group staff and contractors and customers
5. Public – All other data.

After classifying data you can then make decisions on how data will be protected or where data may be transmitted or stored – eg sharepoint, teams, email, network drives etc

What are the consequences of not protecting data?

For an individual or Organization impacted by a data breach

- Identity Theft
- Fraud

For an Individual or Organization responsible for the data breach

- Fines and other penalties
- Reputational Damage

We are all aware of recent media around significant Australian Companies that have had major data breaches.

Let’s not add your organization to that list ☺

Regulatory requirements

The Office of the Australian Information Commissioner (OAIC)

Established in 2010, this is the federal authority for governing the laws and policy around privacy, freedom of information and government information policy.

The General Data Protection Regulation (GDPR)

In 2016, the EU adopted the General Data Protection Regulation (GDPR), one of its greatest achievements in recent years. It replaces the 1995 Data Protection Directive which was adopted at a time when the internet was in its infancy.

If an organization has a presence in the EU or holds data related to EU residents they may have obligations under GDPR.

For breaching these obligations penalties may be significant

Debit/Credit Card Requirements

PCI-DSS – Payment Card Industry - Data Security Standard

Card providers (MasterCard, Visa etc) created the standard to better control cardholder data and reduce credit card fraud and the standard is administered by Payment Card Industry Security Standards Council.

The intentions of each provider were roughly similar: to create an additional level of protection for card issuers by ensuring that merchants meet minimum levels of security when they store, process, and transmit cardholder data.

In version 3.2.1 of the PCI DSS, the twelve requirements are:

1. Install and maintain a firewall system to protect cardholder data.
2. Avoid vendor-supplied defaults for system passwords and other security parameters.
3. Protect stored cardholder data.
4. Encrypt transmission of cardholder data on open, public networks.
5. Protect all systems against malware and update anti-virus software or programs.
6. Develop and maintain secure systems and applications.
7. Restrict access to cardholder data by business need to know.
8. Identify and authenticate access to system components.
9. Restrict physical access to cardholder data.
10. Track and monitor access to network resources and cardholder data.
11. Regularly test security systems and processes.
12. Maintain an information security policy which addresses information security for all personnel.

Security Objects and hints and tips

Every SAP Instance is different, and you will need to assess what data you hold that requires protection. Below I will focus on your likely items to consider for Customer Specific data.

- Customer data
  - Transaction BP
  - Object B_BUPA_FDG
- Table access
  - Perhaps more risky than transactions – SE16, SE11 etc
  - Objects S_TABU_DIS, S_TABU_NAM
- Download Data Access
  - Object S_GUI

- If you are unsure then use your trace options during build and design to help you restrict your access.

SAP Security and Data Protection Tips.

Know your data

What data does my system contain? Does your organization already have a data classification policy?

Know your users

Who needs to see or change protected data?

Know your systems

Are we up to date with our system patching, virus protection, threat detection etc?

Know your security

What critical transactions and functions do I need to ensure are protected?

Useful Links.

The Office of the Australian Information Commissioner (OAIC)

https://www.oaic.gov.au/

The General Data Protection Regulation (GDPR)

https://gdpr.eu/

US Data Protection

https://www.whitecase.com/insight-our-thinking/us-data-privacy-guide

https://www.forbes.com/sites/conormurray/2023/04/21/us-data-privacy-protection-laws-a-comprehensive-guide/?sh=5bb041235f92

https://www.auditboard.com/blog/updates-to-us-state-data-privacy-laws/

Payment Card Industry Data Security Standard (PCI DSS)

https://listings.pcisecuritystandards.org/documents/PCI_DSS-QRG-v3_2_1.pdf

Questions

How to Connect with Me

M: +61 412 572 717

Li: www.linkedin.com/in/paul-bisby-sapsecurity

MASTERINGSAP

An SAPinsider Company

#MasteringSAP
#MasteringSAPCollaborate