Data Security – An Introduction

When we talk about data security what do we actually mean? Data security means protecting data, such as database, from destructive forces and from the unwanted actions of unauthorised users.

In the UK, the Data Protection Act is used to ensure that personal data is accessible to those whom it concerns, and provides redress to individuals if there are inaccuracies. This is particularly important to ensure individuals are treated fairly, for example for credit checking purposes. The Data Protection Act states that only individuals and companies with legitimate and lawful reasons can process personal information and cannot be shared.

The international standard ISO 27001 covers data and information security. Information security is the practice of defending information from unauthorised access, use, disclosure, disruption, modification, perusal, inspection, recording or destruction. It is a general term that can be used regardless of the form the data may take (e.g. electronic, physical)

So what is Data Security?

- Data is any type of stored digital information.
- Security is about the protection of assets.
- Prevention is the measures taken to protect your assets from being damaged.
- Detection is the measures taken to allow you to detect when an asset has been damaged, how it was damaged and who damaged it.
- Reaction is the measures that allow you to recover your assets.
- Confidentiality ensures that that data is only read by the intended recipients.
- Integrity ensures that all of the data has not been corrupted from its original source.
- Availability guarantees that the data is usable upon demand.
- Accountability is audit information that is kept and protected so that security actions can be traced to the responsible party.
Audit Standards

Data Security is subject to several types of audit standards and verification, the most common are ISO 27001, PCI, ITIL. Security Administrators are responsible for creating and enforcing a policy that conforms to the standards that apply to their business.

IT certification audits are generally carried out by 3rd parties although regular internal audits are recommended. Clients can also carry out audits before they begin doing business with a company to ensure that their clients data is secured to their standards.

Security Policy

A security policy is a comprehensive document that defines a company’s methods for prevention, detection, reaction, classification, accountability of data security practices and enforcement methods. It generally follows industry best practices as defined by ISO 27001, PCI, ITIL or a mix of them. The security policy is the key document in effective security practices. Once it has been defined it must be implemented and modified and include any exceptions that may need to be in place for business continuity. Most importantly all users need to be trained on these best practices with continuing education at regular intervals.

Securing data

Data needs to be classified in the security policy according to its sensitivity. Once this has taken place, the most sensitive data has extra measures in place to safeguard and ensure its integrity and availability.

All access to this sensitive data must be logged. Secure data is usually isolated from other stored data and it is important that controlling physical access to the data centre or area where the data is stored is implemented.

Active Directory for example is used by many companies and is a centralised authentication management system that is used to control and log access to any data on the system.

Encryption of the sensitive data is critical before transmission across public networks. The use of firewalls on all publicly facing WAN connections needs to be in place and also the deployment of VLANs’ to isolate sensitive departments from the rest of the network. It is important to shut down unused switch ports. If Wi-Fi is deployed then it is important to use authentication servers to verify and log the identity of those logging on. Finally the deployment of anti-virus and malicious software protection on all systems.
**Monitoring**

Sometimes you will be surprised what you can find by simply walking around and look for passwords in the open, unattended screens.

Ensure that Event Viewer and Log Files are maintained this provides the audit trail. An Intrusion Detection/ Protection systems (IDS/IPS) to monitor the network and system activities for malicious activities or policy violations. Set up SNMP monitoring servers to monitor and alert for everything as this will alert Administrators to everything from unusual bandwidth usage to hardware failure. It is key to know what's going on with your systems and network.

Documentation is also important, detailed network maps should be available as these maps make it easier to spot security weak points and any flaws in the design that could impact the data security.

You should also consider a network scanner that probes devices to ensure that they are secure. A network scanner will probe and report old out of date software, open ports and the give details on any potential exposures. Networks scans should be scheduled on a regular basis.

**Keep up to date and stay Informed**

Review log files regularly of any publicly facing server to see what types of attacks are being run against your enterprise. Trade publications discuss the latest threats and technologies keeps you updated on the latest attack trends. It is important to understand the technology stack that you are protecting and the technology that is used to attack it.

**User Education**

Something which tends to not be given the required level of importance is user education. All relevant security policies must be clearly explained to the end users. A clear explanation of the consequences for violating these polices must also be explained. The end user needs to sign a document acknowledging that they understand the policies and consequences for violating these policies.

**Enforcement**

Any enforcement must obtain executive authority to enforce the business policies and procedures. This must be based on a systematic approach of warnings and punishments.