SLIIT

Discover Your Future

IE2022 – Introduction to Cyber Security

Lecture - 04

Data Loss and Hackers

Mr. Amila Senarathne

Data Loss

Data loss or data exfiltration is when data is intentionally or unintentionally lost, stolen, or leaked to the outside world.

Data is likely to be an organization's most valuable asset. Organizational data can include:

- Research and development data
- Sales data
- Financial data
- Human resource and legal data
- Employee data
- Contractor data
- Customer data.

Data Loss can result in:

- Brand damage and loss of reputation
- Loss of competitive advantage
- Loss of customers
- Loss of revenue
- Litigation/legal action resulting in fines and civil penalties
- Significant cost and effort to notify affected parties and recover from the breach

Vectors of Data Loss

- Unencrypted Devices
- Cloud Storage Devices
- Removable Media
- Hard Copy
- Improper Access Control
- Email
- Social Networking

BYOD (Bring Your Own Device)

- BYOD is the emerging trend of employees using their personal devices, like smartphones, tablets, laptops etc, to remotely access any organizational network to carry out office work.
- Employees can thus access official mail on their smartphone, connect to office and work using their laptop even while they are traveling and use tablets to be part of conferences that happen at their office when they are away.
- BYOD is important today since employees would want to deliver their best in today's competitive world and companies too would want to make the most of the manpower they have at hand.

BYOD Benefits

- Boosts productivity: Employees can always work by accessing work using their personal devices and they can even check emails and update presentations while on vacation or while traveling back home.
- Employees work with devices that they are more comfortable with and are hence happier when they work in places where BYOD is encouraged.
- The money that needs to be invested on buying hardware, software etc. can be utilized for other things even as employees use their own personal devices for work. Thus SMBs can benefit out of BYOD in a very direct manner.
- BYOD helps companies stay abreast of changing technology as employees using personal devices for work would stay up-to-date as regards technology and would use the same for the company as well.

BYOD Drawbacks

- The security threats arise due to the increased number of people who would be accessing a company's data using other devices and also due to the fact that malware could get in through any BYOD device that isn't properly secured.
- Company files and data, which are free to be accessed by employees using their personal devices, could also end up in wrong hands. Such data can be easily seen or stolen by outsiders with malicious intentions.
- BYOD devices might also get stolen or they may get lost, which would also cause data breaches.
- The IT departments in companies where BYOD is practiced would have to undergo tremendous pressure support, managing and securing all BYOD devices.

COPE (Corporate-Owned, Personally Enabled)

- COPE is a business model in which an organization provides its employees with mobile computing devices and allows the employees to use them as if they were personally-owned notebook computers, tablets or smartphones.
- The COPE model provide the organization with greater power to protect the organization's data both technically and legally.
- Corporate-owned device policies provide several benefits, such as:
- The ability to actively manage and control if and when a device can access particular apps, sites, services, networks and solutions.
- The opportunity to wipe a device of any corporate data when an employee loses his or her device or parts ways with the organization.
- The chance to incorporate controls on the device that determine how applications, networks and IT systems can be utilized remotely, and whether specific information can be retrieved in certain scenarios.

Security measures for COPE/BYOD

Mobile Device Management (MDM) features secure, monitor, and manage mobile devices, including corporate-owned devices and employee-owned devices.

- Data Encryption
- PIN enforcement / Strong Authentications Mechnisams
- Remote Date Wipe of stolen/misplaced devices
- Data Loss Prevention (DLP) options
- Jailbreak/Root detection
- Remotely locating devices
- Security assessments (Vulnerability assessments/ Pen testing/ Audits)

The Hacker

Hacker is a common term used to describe a network attacker.

However, the term “hacker” has a variety of meanings:

- A clever programmer capable of developing new programs and coding changes to existing programs to make them more efficient.
- A network professional that uses sophisticated programming skills to ensure that networks are not vulnerable to attack.
- A person who tries to gain unauthorized access to devices on the Internet.
- Individuals who run programs to prevent or slow network access to a large number of users, or corrupt or wipe out data on servers.

White Hat Hackers

- Ethical Hackers Who use their hacking skills for good, ethical and legal purposes
- May perform Security assessments such as vulnerability assessment penetration tests to discover vulnerabilities.
- Security vulnerabilities are reported to developers for them to fix before the vulnerabilities can be exploited.
- Some organizations award prizes or bounties to white hat hackers when they report vulnerabilities

Gray Hat Hackers

These are the individuals who commit crimes and do arguably unethical things, but not for personal gain or cause serious damage.

Example:

- Someone who compromise a system without permission and then disclose the vulnerabilities publically.
- However, by publicizing a vulnerability, the gray hat hacker may give other hackers the opportunity to exploit it.

Black Hat Hackers

- These are unethical criminals who violate computer and network security for personal gain or for malicious reasons.
- Black hat hackers exploit vulnerabilities to compromise computer and network systems.

Modern Hacking Titles

- Script Kiddies
- Vulnerability Brokers
- Cyber Criminals
- Hacktivists
- State-Sponsored Hackers

Script Kiddies

- Inexperienced hackers running existing scripts, tools and exploits developed by skillful hackers to cause harm but typically not for profit.
- It is generally assumed that most script kiddies are juveniles who lack the ability to write sophisticated programs or exploits on their own
- Their objective is to try to impress their friends or gain credit in computer-enthusiast communities.
- However, the term does not relate to the actual age of the participant.

Vulnerability Brokers

- They are usually gray hat hackers who attempt to discover exploits and report them to vendors, sometime for prize or rewards.

Cyber Criminals

- Cyber criminals are black hat hackers with the motive to make money using any means necessary.
- Self employed (working independently) or working for criminal organizations.
- It is estimated that globally, cyber criminals steal billions of dollars from consumers and businesses.
- Cyber criminals operate in an underground economy where they buy, sell, and trade attack toolkits, zero day exploit code, botnet services, banking Trojans, keyloggers, and much more.
- They also buy and sell the private information and intellectual property they steal from victims.
- Cyber criminals target small businesses and consumers, as well as large enterprises and industry verticals.

Hacktivists

- Grey hat hackers who rally and protest against different social and political ideas.
- Hacktivists do not hack for profit, they hack for attention.
- Hacktivists publically protest against organization or governments by posting articles, videos. Leaking sensitive information and performing distributed denial of service attacks.

Examples of hacktivist groups

- Anonymous Hackers
- Syrian Electronic Army.

State-Sponsored Hackers

- These are government-funded and guided attackers.
- State-sponsored hackers create advanced and customized attack code, often using previously undiscovered software vulnerabilities, Steal government secrets , gather intelligence and sabotage networks and systems.
- Their targets are foreign governments, terrorist groups and corporations.
- Most countries in the world participate to some degree in state-sponsored hacking.
- Nations hire the best talent to create the most advanced and stealthy threats.
- **An example** : Stuxnet malware that was created to damage Iran's nuclear enrichment capabilities.

Questions ?

Thank you