indium
Make Technology Work

Most warranted security: Data Leak Prevention

White Paper

www.indiumsoftware.com

Onboarding security practices is a mandatory call out in every enterprise strategy checklist, given the vulnerabilities arising from unintended access, data transfer and malicious targets. The cost of upturn and risk awareness is prominent today, and the time is ripe to get the right security consulting for specialized matters in Security. Indium's security testing experts are addressing data security amid a huge demand and have consolidated the incidents and variants in data vulnerabilities that are weighing down organizations' credibility. Whether you are preparing your next security strategy or gaining awareness through industry stories, this is worth a read!

To begin with, Data Security, as much as it is unfair, is unbiased. Data loss or leaks are tough on small and big organizations equally. Data sensitivity takes lead in contest with volumes. Some more sensitive stats: 90% of data breach occurs within a fraction of seconds. The business/organisation takes several weeks to identify and fix it. On an average, 20% of total revenue is lost due to data breach in any organization.

Desirable Security: Data Leakage Prevention

Data leakage is an unauthorized transfer/loss of data either electronically or physically from within an organization to an external destination. Data leakage typically happens across organization via the web, email, inappropriate access to users, and can happen in random ways (internal/external) as there are no fixed scenarios or steps. Some variants of Data Leakage:

Unintentional Breach:

A data loss / breach can happen inadvertently when information shared between organisations/competitors. For e.g.: when a user sends a group mail accidentally, they might reveal confidential information such as user credentials, financial data, sensitive company information appearing in personal blogs.

Weak Passwords:

People like things to be simple and easy, so they create passwords which are easy to remember, they use default passwords and use same/similar passwords across multiple accounts. These types of passwords are easy to crack and vulnerable to brute force attacks which lead to unauthorised access to sensitive or hidden data.

Malicious Attacks:

When cyber criminals attack a web page to gain access to a system by identifying the vulnerability, they gain access to the database where they can uncover usernames and passwords of the entire account. The hackers harm the data by defacing the website or selling the data to their competitors.

Phishing:

Another form of data loss is by tricking the user to click a link which enforces the user to provide their personal details. Called as phishing attack, this attempts to manipulate targets to click/redirect to fake page/malicious page/replica of the real page to steal user data, including login credentials and credit card numbers.

Application & Network Vulnerabilities:

A malicious user/hacker is in the lookout for security flaws in an application or in the network. Once they identify the loopholes the attackers tend to crawl the application or steal sensitive data.

Virus & Malware:

Computer is affected in numerous ways, one of which is through virus and malware. They cause damages such as corrupting the operating system, damaging the stored data and misusing the internet connection. The main function of the virus is to corrupt the operating system and the files stored within the computer. Malwares act a bit differently wherein they inject a trojan into the system which gives access to the hacker to control the system remotely and as well as gain access to sensitive data.

Power Failure / Damages:
A data loss can happen when there is a sudden increase or drop in voltage which damages the operating system or causes hardware problems like bad sectors or boot failures. Data loss can even happen when we spill coffee, drinks or water on laptop or desktop. The spilling of liquids can cause short circuit to the electronic components which causes physical damages that can be hard to recover.

Ransomware:
It is a form of malicious software which prevents legitimate users from accessing the data. This infects the systems and the servers associated with it. It is a huge threat because the attackers threaten to delete the data or sell it to competitors.

Fire / Explosion:
Gas leakage or fire caused by a flammable liquid can cause damages to the entire organisation, further affecting the server, firewalls and other assets associated with it.

Theft:
In today's world, employees have turned to their mobile phones and laptops even for official work. When these devices are stolen, it leads to a loss of data.

Disgruntled Employee:
A disgruntled employee can intentionally steal the data or the assets of the organisation for personal benefits. For example, a data loss can occur through USB drives, dumpster diving for discarded documents, via uncollected printed papers, cameras and through social media.

Business Impact:

Poor data management leads to security breaches or attacks that severely impact the business. This leads to selling off the data to competitors or it may be used to create a similar product/application.
An IT security breach will lead to unauthorized third parties gaining access to an entire organization's data which will hamper morale and result in the loss of investors/customers' trust.

Key Impacts:
1. Lose or compromise your customers' data
2. Employees' data at risk
3. DDoS attack
4. Revenue loss
5. Risk of trade secrets
6. Risk of malware / virus / threat against organisation
7. Organisation Reputation Loss (Ranking)

Real Time Scenarios:

Who: Digital Ocean
When: May 2020
How: Details of the Hack
Digital Ocean is a web hosting provider. It has recently contacted some of its customers stating that there is a security lapse which has exposed their account details.

The leak occurred due to an internal sensitive document being left online by mistake. This document consisted of customers' personal details such as email ID and their digital ocean account details including technical information such as number of servers owned, bandwidth used and payment details of the customer.

Who: **CTS**
When: **April 2020**
How: **Details of the Hack**

A Ransomware attack affected Cognizant and has resulted in the loss of $50 million-$70 million in revenue. The attack could have happened through the IP addresses associated with Kepstl32.dll, memes.tmp and maze.dll files which are prevalent in earlier maze ransomware attack. The line of attack was initially on the internal server which in turn affected the VDI's and WFH laptops.

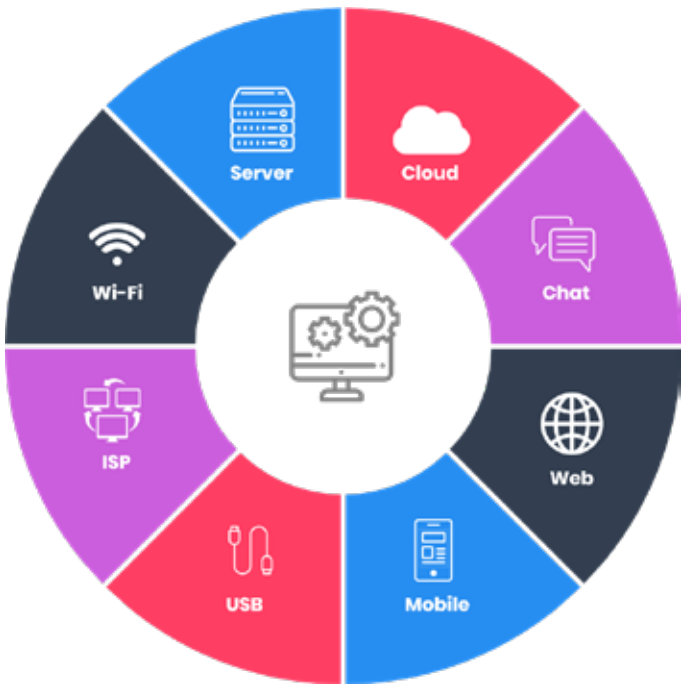
Who: **Equifax**
When: **Mid-May 2017**
How: **Details of the Hack**

They were using an open source framework called Apache struts for their online web app. This framework was vulnerable to HTTP header attack where a malicious person can inject a code and expose sensitive information.

How to Prevent Data Leakage/Loss:

Data leak can be curbed by practising detection and prevention of unauthorized access to data. This can also be used to prevent data being mishandled or accessed illegally on the web application and inside the organisation.

Areas to be Monitored for Data leakage:



There's a huge volume of valuable information available to organisations which needs to be protected and monitored regularly to avoid data leakage while adhering to strict policies to prevent any violation.

Preventive Methods:

There is a range of actions that can be taken to prevent data leakage from an organisation (e.g. alert users to their risky behaviour, quarantine outbound email messages containing sensitive data, block the transfer of data to portable storage media, and locate office equipment in a physically secure environment).

Preventive Steps:

- Proper access control mechanism should be in place for all internal and external applications
- Incorporate various encryption/hashing techniques across the organisation during data transfer.
- Implement ISO27001 controls adhering to various security compliance/guidelines which includes HIPAA, PCI DSS, SOX audit etc as applicable.
- Penetration testing should be carried out for any applications that are put into production.
- All internal and external applications should carry out VAPT that covers the following (not limited),
    - Injection Attacks
    - Malware Protection
    - Application Fuzzing
    - Anti-Skimming attacks
    - Web / Network-Based attacks

Conclusion:

The premise of Data Leaks prevention is establishing a resilience to the dynamic nature of data breaches. Breaking down the areas of focus and understanding data transaction vectors is a tested solution to mitigate loss. There are constantly evolving platforms and devices posing new and unanticipated ways of data leaks and insecurities; documenting a structured approach to the situation alone shall be a fake promise to deal security. Proactive implementation of a solid prevention approach can help identify incidents early during the risk modelling phases. Key Pointers

- Data Flow Maps: Awareness and visibility into data Usage and information Security plug points
- Controls and procedures in data sharing, content control, intelligent firewalls, permissions
- Policies for various platforms and open data destinations
- Tools, guidelines and support from management

INDIA

Chennai | Bengaluru | Mumbai
Toll-free: 1800 123 1191

USA

Cupertino | Princeton
Toll-free: 1 888 207 5969

UK

London

SINGAPORE

+65 9630 7959

Sales Inquiries
sales@indiumsoftware.com

General Inquiries
info@indiumsoftware.com