INDIUM

Most Warranted Security: Data Leak Prevention

A Whitepaper

Onboarding security practices are mandatory 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 huge demand and have consolidated the incidents and variants in data vulnerabilities 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. Data sensitivity takes the lead in the contest with volumes. Some more sensitive stats: 90% of data breaches occur within a fraction of a second. The business/organization takes several weeks to identify and fix it. On average, 20% of total revenue is lost due to data breaches 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 organizations via the web, email, and 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 is shared between organizations/competitors. For example, when a user accidentally sends a group mail, they might reveal confidential information such as user credentials, financial data, or sensitive company information appearing in personal blogs.

Weak Passwords:

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

Malicious Attacks:

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

Phishing:

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

Application & Network Vulnerabilities:

A malicious user or hacker is always looking for security flaws in an application or the network. Once they identify the loopholes, 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:

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 our laptops or desktops. The spilling of liquids can cause a short circuit in the electronic components, which causes physical damage that can be hard to recover.

Ransomware:

It is a form of malicious software that prevents legitimate users from accessing the data. The software infects the systems and 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 damage the entire organization, affecting the server, firewalls, and other assets.

Theft:

Today, employees have even turned to their mobile phones and laptops for official work. When these devices are stolen, data is lost.

Disgruntled Employee:

A disgruntled employee can intentionally steal the organization's data or assets for personal benefit. For example, data loss can occur through USB drives, dumpster diving for discarded documents, uncollected printed papers, cameras, and social media.

Business Impact:

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

Key Impacts:

- Lose or compromise your customers' data
- Employees' data at risk
- DDoS attack
- Revenue loss
- Risk of trade secrets
- Risk of malware/virus/threat against organization
- Organization 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 millio-$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 used an open-source framework called Apache Struts for their online web app. This framework was vulnerable to HTTP header attacks, in which a malicious person could inject code and expose sensitive information.

Being Agile with Mendix

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). .

- Proper access control mechanisms should be in place for all internal and external applications.
- Incorporate various encryption/hashing techniques across the organization during data transfer.
- Implement ISO27001 controls, adhering to various security compliance/guidelines, including HIPAA, PCI DSS, SOX audit, etc., as applicable.
- Penetration testing should be carried out for any applications put into production.
- All internal and external applications should be carried 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 leak prevention is to establish 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 with security. Proactively implementing a solid prevention approach can help identify incidents early during the risk modeling 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

INDIUM

About Indium

Indium is an AI-driven digital engineering company that helps enterprises build, scale, and innovate with cutting-edge technology. We specialize in custom solutions, ensuring every engagement is tailored to business needs with a relentless customer-first approach. Our expertise spans Generative AI, Product Engineering, Intelligent Automation, Data & AI, Quality Engineering, and Gaming, delivering high-impact solutions that drive real business impact.

With 5,000+ associates globally, we partner with Fortune 500, Global 2000, and leading technology firms across Financial Services, Healthcare, Manufacturing, Retail, and Technology–driving impact in North America, India, the UK, Singapore, Australia, and Japan to keep businesses ahead in an AI-first world.

USA

Cupertino | Princeton
Toll-free: +1-888-207-5969

INDIA

Chennai | Bengaluru | Mumbai
Hyderabad | Pune

Toll-free: 1800-123-1191

UK

London
Ph: +44 1420 300014

SINGAPORE

Singapore
Ph: +65 6812 7888

www.indium.tech

For Sales Inquiries
sales@indium.tech

For General Inquiries
info@indium.tech