Know your enemy: Preventing data leakage from insider threats

Mrs. Klorenta Pashaj was named one of 100 Most Influential Women in Europe in Cyber Security and is the first Albanian expert to be accepted by the European Commission into its FUTURIUM Women4Cyber Registry. Klorenta participates in both national and international discussions in cyber security.

Introduction

A right to privacy is not generally recognized on the cyber ecosystem. Cyberspace has emerged as a new area for both public and private operations. The Covid-19 pandemic has altered the way we live and interact on the Internet, including how we spend time. Technology, in particular, has an impact on privacy, from creating extensive records of our online behaviour to affecting democratic processes.

Without strict data protection regulations, the civil society potential of cyberspace will never be realized. However, there are currently no successful standards, legal or otherwise, to limit the collection and use of personal information in cyberspace. The lack of adequate and enforceable data protection standards poses a grave threat to democracies in the new information age. A survey from Oxford University in 2019 (1) showed that privacy concerns are the number one reason people who are not connected to the internet choose not to go online.

The risks of information disclosure

The insider threat that contemporary organisations are most concerned about is data leakage that exposes intellectual property, customer information, and other regulated data. Data loss affects organisations in a variety of ways, and as we constantly see in the news, it can have serious consequences. However, figuring out how to stop data leaks caused by insiders—whether they are careless, malevolent, or compromised—remains a difficulty.

Data leakages can be intentional or unintentional. An intentional data leak is the deliberate act of gathering and revealing confidential information outside of an organisation. Cybercriminals and external threat actors might intentionally target organisations' sensitive data by first breaking into their network or endpoints, then stealing the desired information. Human error was a factor in 85% of cyber security incidents (2).

Data leaks can also be started deliberately by a member of the organisation and these insider threats can be malicious. Insiders frequently handle sensitive data and information in the course of their regular work as employees or other authorised users within an organisation. In this instance, the organisation is intended to suffer harm as a result of the malicious and purposeful data breach.

Insider risks also include unintended data leaks, which are described as the unintentional release of private information outside of a business. These are known as unintentional or careless insider threats. The data leak is assumed to have been inadvertent when an authorised user or system is compromised and doesn't realise the harm they are doing to the business as a result of the behaviour using their access or endpoint, or is careless about it. The majority of insider threats come from careless users, who account for 62% of incidents (3).

Cases of data leakage

Edward Snowden, a former technical assistant for the CIA, is the person in charge of one of the biggest leaks in US political history. For the past four years, Snowden has worked at the National Security Agency as an employee of several outside companies, including Booz Allen and Dell. Along with Bradley Manning and Daniel Ellsberg, Edward Snowden will be remembered as one of the most significant American leakers. He is in charge of turning over information from the NSA, one of the most clandestine organisations in the world (4).

The publication of the salary database for more than 637,138 Albanians in December 2021 is one of the country's biggest scandals, proving that the security systems of the employees that manage the data did not work because of insider threats. It is said that the information includes 630,000 people's monthly wages, job titles, employers' names, and ID numbers from both the public and commercial sectors.

The tax service or the Social Insurance Institute are thought to have leaked the list. This case brought uncertainty about data protection to citizens and highlighted the need for investment in the security of networks and information systems and employees' training.

The prosecution found that the payroll database was removed from the tax system by an insider employee E.Q, who then gave it to her colleague A.A. The latter (A.A) sold the data for 20,000 Albanian lek, which is less than €200. According to official documents of the National Business Center, it turns out that the buyers of the database were the owners of a company that offered loans in Albania from the Russian billionaire Oleg Boikov. The US Senate has categorized the latter (Oleg Boikov) in the list of persons with disturbing ties to the Russian government and intelligence. These links are also reported to be intertwined with organized crime (5).

The Tirana court has blown up the prosecution's investigations, releasing the four arrested who discovered the salaries of over 690,000 Albanian citizens. The four detained for extracting the citizens' data will be investigated under house arrest. In a statement to the media from the DP headquarters, the deputy chairman of the Democratic Party, Enkelejd Alibeaj, says that Rama defended them for the patronage scheme of the citizen's data leaked on April 2021. The court decision about the four detained, says Alibeaj, is clear proof that the authors of the data publication are the Prime Minister and his subordinates (6). The prosecution, so far, has not proven any links to the Russian interest with the publication of the database. Nevertheless, data leakage brought uncertainty, disturbed public opinion and impacted political discourse in Albania.

Preventing data leakage

A data leak might be detected by unusually high system or network activity, the appearance of unexpected software, or anomalous user behavior such as signing in from multiple IP addresses in a short period of time. The time it takes to find, contain, and investigate an event, however, is greatly increased when a team is depending solely on their manual ability to recognize and react to such signs.

To continuously monitor, detect, and prevent data leakage and insider dangers, organizations instead rely on data loss prevention (DLP) technologies. With these technologies in place, businesses may take the required precautions to stop a data breach by getting precursory alerts when a risk is identified or a leak is anticipated.

Some of the best practices to prevent data leakage are:

- Keep track of data access, data migration, and user activities. Understanding which authorised individuals have access to sensitive information and how they utilise it allows organisations to acquire more precise insights into data leakage threats.
- Understand the location of your vital data. Differentiating sensitive data from non-sensitive data allows your security team to be more efficient. Transfer existing

investments in data classification and create new ones using common content detectors across email, cloud, web, and endpoint channels.

- Use data encryption. Data encryption prevents data exfiltration via emails and attachments.
- Use a modern DLP solution. Modern DLP solutions are concerned with connecting individuals and threats to sensitive stuff. It's a people-centric, adaptable method that gives the "who, what, where, and when" of activities, alerts, and events. This enables security teams to detect, prevent, and respond to dangerous users — whether negligent, compromised, or malevolent – before a catastrophic data loss occurs.

The right to be forgotten

If the organizations are not successful in their mission towards preventing data leakage intentionally or unintentionally, then the legacy solution would be “the right to be forgotten”. The GDPR grants people the right to request that businesses remove their personal data, often known as the right to be forgotten. However, organisations are not always required to. Here, we outline the conditions under which the right to be forgotten is valid.

The General Data Protection Regulation (7) establishes requirements for the collection, use, and destruction of personal data. The EU Court of Justice's 2014 ruling on the "right to be forgotten," which drew a lot of media attention, established the basis for the GDPR's right of erasure clause (8).

Given competing interests and the interconnectedness of the Internet, exercising one's right to be forgotten involves considerably more than just asking a company to delete one's personal data. The GDPR's Recitals 65 and 66 and Article 17 both mention the right to be forgotten. It states, “The data subject shall have the right to obtain from the controller the erasure of personal data concerning him or her without undue delay and the controller shall have the obligation to erase personal data without undue delay” if one of a number of conditions applies. A month is deemed to constitute a "undue delay." (9).

Conclusions

Without a doubt, all organisations, whether small, medium, or large, should guarantee that their staff understand the threats or the need for cyberspace protection and assist in lowering their risks. Organizations should include stronger training frameworks to work with in order to reduce the danger of data breaches and data leaks.

Furthermore, failure to comply with data protection regulations would create a situation in which cyber attackers might remove money and other valuable items from personal accounts. They would also endanger people's lives by tampering with personal health information.

It is crucial to know what data is being processed, why it is being processed, and the legal basis for processing in order to verify that the data you are utilising is secure.

References

(1) Hussain, D. (2019, September 9). *Privacy fears put growing numbers of people off using the internet*. Mail Online. https://www.dailymail.co.uk/news/article-7442833/Privacy-fears-risk-widening-digital-divide-study-suggests.html

(2) Verizon. (2021). *2021 Data Breach Investigations Report (DBIR)*. Verizon Enterprise Solutions. https://www.verizon.com/business/resources/reports/2021/2021-data-breach-investigations-report.pdf

(3) Ponemon Institute (2022). *Cost of insider threats*. Verizon. https://www.proofpoint.com/uk/resources/threat-reports/cost-of-insider-threats

(4) Greenwald, G., MacAskill, E., & Poitras, L. (2013, June 11). *Edward Snowden: the whistleblower behind the NSA surveillance revelations*. The Guardian. https://www.theguardian.com/world/2013/jun/09/edward-snowden-nsa-whistleblower-surveillance

(5) *Databaza e pagave u ble nga punonjësi i oligarkut rus me lidhje me Putinin (dokumentet)*. (2022, January 7). Gazeta Express. https://www.gazetaexpress.com/databaza-e-pagave-u-ble-nga-punonjesi-i-oligarkut-rus-me-lidhje-me-putinin-dokumentet/

(6) *Skandali me pagat/ PD për lirimin e 4 punonjësve që nxorën të dhënat sekrete: Rama po mbron krimin për vjedhjen e zgjedhjeve*. (2022, January 10). Lapsi.al. https://lapsi.al/2022/01/10/skandali-me-pagat-pd-per-lirimin-e-4-punonjesve-qe-nxoren-te-dhenat-sekrete-rama-po-mbron-krimin-per-vjedhjen-e-zgjedhjeve/

(7) GDPR. (2019). *GDPR.eu*. GDPR.eu. https://gdpr.eu/

(8) *Court of Justice of the European Union Press release*. (2014, May 13). CVRIA. https://curia.europa.eu/jcms/upload/docs/application/pdf/2014-05/cp140070en.pdf

(9) *Art. 17 GDPR - Right to erasure ("right to be forgotten") - GDPR.eu*. (2018, November 14). GDPR.eu. https://gdpr.eu/article-17-right-to-be-forgotten/