The Cost of a Data Breach (CoDB) and the Impact of AI

Introduction

Data breaches are a vulnerable aspect of cybersecurity, signifying unauthorized access and stolen information. Beyond the theft, it raises questions about the cost and recovery time.

Cost of a data breach

In 2023, the worldwide average expense of a data breach reached USD 4.45 million, marking a 15% rise over the past three years. Following breaches, 51% of companies intend to boost their security spending, focusing on incident response planning and testing, staff training, and implementing threat detection and response tools. Organizations leveraging extensive security AI and automation stand to save an average of USD 1.76 million compared to those not utilizing such technologies.

(Source: Cost of a Data Breach Report 2023)

What are the aspects contributing to a data breach?

Understanding the factors behind a data breach is crucial. In today's tech, hackers have many ways to infiltrate. Rather than focusing on all these ways, let's look at the types and frequencies of attacks. From this perspective, the top two are phishing and credential compromise.

The initial step is to reduce the numbers, focusing on top attack scenarios like phishing and credential compromise. Another concern is the substantial time gap, around 277 days, between a hacker entering the system and the attack being detected. Surprisingly, this duration remains consistent despite technological advancements. Thus, it emphasizes the need to decrease costs and the time taken to identify and contain such breaches.

Recommendations

- **Take action to help prevent breaches**
  Secure the organization by deploying appropriate tools and making essential investments. Develop and implement an incident response plan.
- **Save money and time with AI and automation**
  Consider employing Generative AI as an action item. Statistics reveal that only 28% of organizations extensively utilized security AI, leading to cost reductions and faster containment.
- **Protect data in the hybrid cloud**
  Another vital consideration is the shift of organizations to the cloud. 82% of breaches involved cloud-stored data. It's crucial to seek solutions offering visibility across hybrid environments and safeguard data as it traverses clouds, databases, apps, and services.
- **Uncover risky vulnerabilities**
  Incorporate a zero-trust architecture, integrating security into every software and hardware development stage. As the report highlighted, adopting a DevSecOps approach and conducting penetration and application testing emerge as the most significant cost-saving factor.
- **Know your attack surface and how to protect it**
  Knowing your attack surface isn't enough. You also need an incident response (IR) plan to protect it.

Summary

Generative AI can help protect the assets and help with pre-empting and containing threats before the data breach occurs.

Author: Manish Kumar