Group Discussion Report
Microsoft's 38 TB Data Leak Incident

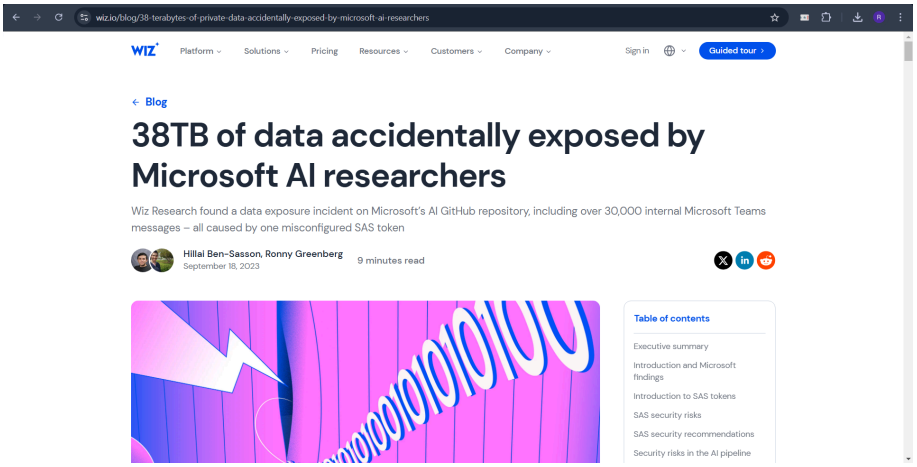
Name : Ritesh Jha
Class : SY_IT (B3)
Roll No : 16010423076

Participants

- Ritesh Jha - 16010423076
- Omkar Dabde - 16010423065
- Vaibhav Dave - 1601042108
- Saksham Varshney - 16010423080

Overview

In June 2023, Microsoft faced a significant data leak when AI researchers accidentally exposed 38 terabytes (TB) of sensitive data due to a misconfigured SAS (Shared Access Signature) token on GitHub. This incident revealed private information like employee data, internal messages, passwords & secret keys, highlighting vulnerabilities in cloud security.



Incident Analysis

The discussion began with **Saksham** explaining the technical details of the incident. He highlighted how a misconfigured SAS token—meant to allow specific access—ended up granting full permissions to an Azure Blob Storage account. This allowed anyone with the URL to access & manipulate sensitive data, leading to an unintended exposure of internal Microsoft resources.

Omkar elaborated on the risks associated with SAS tokens, emphasizing the need for strict access management. He noted that the Microsoft AI team failed to enforce the principle of least privilege, allowing broader access than necessary.

Then **I (Ritesh)** pointed out that the issue went unnoticed by Microsoft for several months & was eventually detected by Wiz, an external cloud security firm. This delay in detection suggested a gap in monitoring & oversight.

Vaibhav shared insights on the consequences of misconfigurations in cloud environments, noting that human error & inadequate training often play a crucial role in such incidents.

Key Discussion Points

Incident Analysis

- Ritesh initiated the discussion by detailing the misconfigured SAS token, which allowed access beyond intended AI research data.
- Omkar emphasized the human error in configuration & the need for stringent access controls.
- Vaibhav discussed Microsoft's delayed detection & reliance on an external firm, Wiz, to discover the breach.
- Saksham pointed out the broader risks of misconfigurations in cloud environments.

Data Impact & Response

- The exposed data contained sensitive employee information & internal tools, posing a security risk despite no evidence of malicious use.
- Microsoft revoked the token, strengthened security audits & issued a public statement to address the breach.

Compliance Violations

- The group identified potential violations of GDPR, CCPA & ISO/IEC 27001 standards, due to improper data protection & risk management.

Root Cause & Lessons Learned

- **Human Error** was cited as the primary cause, with a lack of least privilege access & insufficient monitoring.
- **Lessons** included the need for careful cloud configurations, effective access controls, continuous monitoring & secure data-sharing practices.

Conclusion

The discussion underscored the importance of rigorous cloud security measures, regular audits & proactive monitoring. Proper configurations & compliance with data protection laws are essential to mitigate risks & handle sensitive data securely.