CMPE -272 Lab Activity (March 7th)

Team: SJSU ID
-Satwik Upadhyayula: 017423796
-Supriya Vanaparthi: 017464135
- Vineet Samudrala : 017426253
- Shreekar Kolanu : 017406493\

1. Are person-to-person email services like Gmail, Outlook, Yahoo Mail, etc., secure today?

Findings:

a. Encryption : Most major email services use encryption to protect data in transit. Transport Layer Security (TLS) encrypts emails as they travel between servers, preventing interception by third parties.

b. Data Storage: Providers typically store emails on servers, which are secured with various measures such as firewalls, access controls, and encryption at rest.

c. Privacy Policies : Companies like Google and Microsoft outline their privacy practices, including how they handle user data. However, users should review these policies to understand how their information is used.

d. End-to-End Encryption (E2EE) : While some services offer E2EE (e.g., Gmail with its confidential mode), it's not universally applied. E2EE ensures that only the sender and recipient can access the content, but it's not always the default option.

e. Security Measures : These platforms implement security features like two-factor authentication (2FA) to prevent unauthorized access to accounts.

f. Threats : Despite these measures, email services are still vulnerable to phishing attacks, account hijacking, and other security breaches. Users must remain vigilant and adopt best practices to protect their accounts.

Conclusion : While major email services employ various security measures, absolute security is challenging due to evolving threats. Users should enable available security features and remain cautious when sharing sensitive information.

2. Can a company prevent internal email leaks into the public?**

Findings:
a. Data Loss Prevention (DLP) : Companies can implement DLP solutions to monitor, detect, and prevent the unauthorized transmission of sensitive information via email. DLP systems can analyze email content, attachments, and metadata to enforce security policies.

b. Encryption : Encrypting emails, especially those containing sensitive data, can prevent unauthorized access even if they are intercepted or leaked.

c. Access Controls : Limiting access to sensitive information to only authorized personnel reduces the risk of leaks. Role-based access control (RBAC) ensures that employees can only access data necessary for their job roles.

d. Employee Training : Educating employees about the importance of data security, recognizing phishing attempts, and following company policies can mitigate the risk of unintentional data leaks.

e. Monitoring and Auditing : Regularly monitoring email traffic and conducting audits can help identify suspicious activities or policy violations. This allows companies to take proactive measures to prevent leaks.

f. Legal and Compliance Measures : Companies can enforce legal agreements, non-disclosure agreements (NDAs), and compliance regulations to deter employees from leaking sensitive information.

Conclusion : While no system can guarantee 100% prevention of internal email leaks, companies can significantly reduce the risk through a combination of technology solutions, employee training, and policy enforcement. However, maintaining vigilance and adapting to evolving threats are essential.