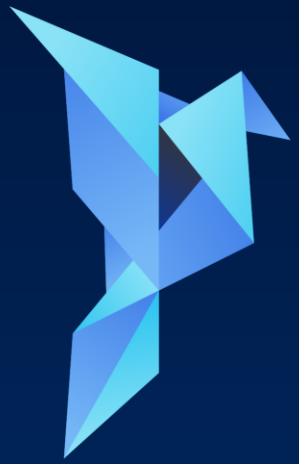


PACIFICA

A NOVENTIQ Company

Internal Threats and Methods for Preventing Information Leakage

Roman GUGNYAK – Cybersecurity Architect

Key Data Security Threats

- **Hacker Attacks:** Database breaches, theft of login credentials and passwords.
- **Phishing and Social Engineering:** Manipulating victims into voluntarily disclosing sensitive information.
- **Insider Leaks:** Mistakes or intentional actions by employees.
- **Insufficient Service Protection:** Weak passwords, lack of encryption.

Who Are Insiders?

An **insider** is an employee, contractor, or partner who has access to corporate information and resources.

Types of insiders:

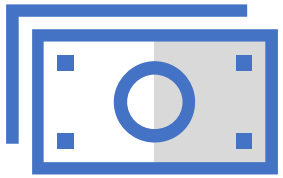
- Malicious
- Unintentional

Main motives:

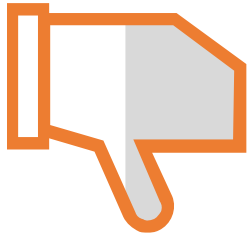
- Financial gain
- Revenge
- Ideological beliefs
- Blackmail
- Mistakes and lack of policy awareness

Why Is This Important?

$4.92M average cost of malicious insider attacks[1]



Expensive fines and penalties



Damaged reputation

Loss of customers and revenue

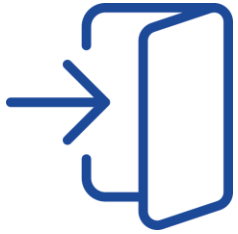
[1]https://www.ibm.com/downloads/documents/us-en/131cf87b20b31c91

Why Are Insiders Dangerous?

Harder to Detect

Variety of Attack Scenarios

Knowledge of Valuable Data



Direct Access to Information Systems

What Can Insiders Do and What Are the Consequences?

Insider Actions


Data theft


Data deletion or corruption


Accidental data leakage


Running unauthorized software, disabling security tools


Sharing account credentials


Connecting unauthorized devices to a PC or network

Consequences


Leakage of trade secrets, loss of competitive advantage


Disruption of business processes, SLA violations, recovery costs


Malware infection across the network


Use of legitimate accounts for attacks


Remote access to the corporate network

Example 1: Terminated Employee

- **Incident:**

A terminated employee retained access and, within 40 minutes, deleted 21 GB of data (20,000 files), including ransomware protection software

- **Damage:**

Loss of critical data and increased security risks

- **Takeaways:**

➢ Immediately revoke access upon termination

➢ Monitor activity in critical systems

Example 2: Coinbase

- **Incident:**

External support agents were bribed, leading to a data leak affecting less than 1% of users (names, accounts, partial SSNs)

- **Damage:**

Attempted extortion of $20 million and reputational risks

- **Takeaways:**

➢ Strict contractor oversight

➢ Zero Trust approach and access limitation

Example 3: Bank Employees Selling Customer Data

- **Incident:**

Employees of major banks were selling customer data via Telegram

- **Damage:**

Massive leaks of personal data and increased fraud activity

- **Takeaways:**

➢ Anomaly and data leak channel monitoring

➢ Improving salaries and employee motivation to reduce risk

Example 4: Dallas City Files Deleted Due to Human Error

- **Incident:**

An employee deleted 22 TB of data (police videos and materials) due to procedural violations

- **Damage:**

Loss of evidence and disruption of investigations

- **Takeaways:**

➢ Staff training

➢ Automation of data transfer processes

Policies and Procedures

Enhancing and maintaining employee loyalty

NDA (Non-Disclosure Agreement)

Corporate resource usage policy

Employee training

Structuring workflows to minimize human error risks

Access control and privilege minimization

Information Security Tools – DLP

- A system that monitors the movement of confidential data within and outside the company.

- **Key Functions:**
  - Locating storage of sensitive information
  - Monitoring and blocking data transfers via channels (email, messengers, cloud services, USB)
  - Controlling printing, copying, and screenshots
  - Content analysis (by keywords, templates, classification)
  - Recording user actions for investigation purposes.

- **How It Prevents Insider Attacks:**
  - Malicious actions: Blocking database exports, copying to USB drives.
  - Negligence: Alerts when sending emails to unintended recipients.

Information Security Tools – SIEM

- A platform for collecting, correlating, and analyzing security events from various sources

- **Key Functions:**
  - Log aggregation (AD, email, VPN, DLP, databases)
  - Event correlation to detect anomalies
  - Real-time response (alerts, automated playbooks)
  - Historical data storage and analysis for investigations

- **How It Prevents Insider Attacks:**
  - Detects abnormal behavior (e.g., mass data export, access during off-hours)
  - Correlates multiple indicators (USB connection + file export + email sending)
  - Integrates with DLP and UEBA for behavioral analysis

Information Security Tools – UEBA

- A technology that analyzes user and system behavior to detect anomalies

- **Key Functions:**
  - Behavioral profiling (normal activity patterns)
  - Anomaly detection (login time, data volume, access to new resources)
  - Risk scoring of user actions
  - Integration with IT, security, and business systems.

- **How It Prevents Insider Attacks:**
  - Detects hidden threats (malicious actions under legitimate accounts)
  - Identifies compromised accounts
  - Reduces false positives through contextual analysis

PACIFICA
A NOVENTIQ Company

Conclusion

Insiders are not only malicious actors but also careless employees

Main risks: data theft and loss, human errors

Consequences: financial losses, reputational damage, legal penalties

Protection requires a comprehensive approach:

- Policies and employee training
- Technical solutions: DLP, SIEM, UEBA
- Access control and Zero Trust principle


PACIFICA
A NOVENTIQ Company