Investigation Of A Data Breach

Task 1: Incident Analysis

Objective: Investigate the breach origin, its scope, and the timeframe.

Findings:

- **Point of Entry**: An attacker leveraged a phishing email that contained a malicious attachment. The file executed a macro, installing a Remote Access Trojan (RAT) on an employee's system. Using stolen credentials, the attacker gained access to the database server hosting customer data.
- **Scope of Breach**: Database logs revealed unauthorized queries exposing the “Customer Account” table. Sensitive fields included customer names, account numbers, and transaction history. Approximately 15,000 records were accessed.
- **Timeframe**: Using timestamp analysis of database queries, the breach activity was traced to a 10-day period (December 10–20, 2024). The attacker accessed the system intermittently during this time.

Technical Analysis:

1. **Log Reviews**: SIEM solutions (e.g., Splunk) were used to correlate anomalous activities. Unusual logins originated from an ip.
2. **Credential Compromise**: Packet captures using Wireshark detected unencrypted credential transmission during the initial exploit phase.

Challenges Identified:

- Inadequate endpoint security allowing the RAT installation.
- Lack of multi-factor authentication (MFA) for privileged access.

Mitigation Plan:

- Conduct organization-wide credential resets.
- Deploy endpoint detection and response (EDR) tools.
- Roll out MFA to all critical accounts.

Task 2: Forensic Analysis

Objective: Perform forensic analysis to identify malware and collect evidence.

Analysis Process:

1. **Disk Imaging: Forensically sound copies of affected systems were created using FTK Imager. Hash values (SHA-256) ensured integrity.**
2. **Memory Analysis: The Volatility framework was used to inspect RAM dumps. Processes linked to `rat.exe` indicated the presence of a Remote Access Trojan.**
3. **Log Analysis: Logs from the application server showed repeated SQL queries executed by an unauthorized user.**
4. **Malware Reverse Engineering: Dynamic analysis of `rat.exe` in a sandbox revealed that the malware communicated with a Command-and-Control (C2) server at `198.51.100.25` over port 443.**

Evidence Collected:

- **Malicious executable and memory artifacts.**
- **Firewall logs showing outbound connections to the C2 server.**
- **Timestamps and IP addresses from compromised database logs.**

Key Findings:

- **The attacker used privilege escalation techniques to obtain admin-level access.**
- **No evidence of ransomware or data alteration was found.**

Mitigation:

- **Immediate blocking of the C2 server.**
- **Strengthening logging mechanisms to detect anomalous behavior sooner.**

Task 3: Data Recovery

Objective: Quantify exposed data and implement a containment and recovery strategy.

Analysis of Exposed Data:

- **Customer Data Impacted: Names, account numbers, and transaction histories were accessed but not modified. Backup files confirmed the integrity of other tables, including encrypted customer credentials and financial PINs.**
- **Quantity: Out of 50,000 records, 15,000 were compromised based on query execution logs.**

Containment Measures:

1. **System Isolation: Disconnected the compromised server from the network to prevent further exfiltration.**
2. **Vulnerability Patching: Applied patches to close vulnerabilities in the database system and employee endpoints.**
3. **Access Control: Revoked all user credentials and issued temporary login credentials using a one-time password (OTP) mechanism.**

Data Recovery Strategy:

- **Restored customer tables from backups dated December 9, 2024, using SQL scripts validated for data integrity.**
- **Conducted checksums and compared row counts to verify successful recovery.**

Recommendations:

- **Implement database encryption for sensitive fields.**
- **Conduct regular backup verification tests.**

Task 4: Regulatory Compliance

Objective: Ensure compliance with legal requirements and notify relevant authorities.

Regulations Addressed:

- **GDPR (Article 33): Data breaches involving personal information must be reported within 72 hours.**
- **CCPA: Notify affected individuals and authorities within a reasonable timeframe.**

Actions Taken:

1. **Notification to Authorities:**
    - **Submitted a report detailing the breach timeline, exposed data categories, and containment measures to the National Data Protection Authority (NDPA).**
2. **Customer Communication:**
    - **Notified affected customers through secure emails, including details of exposed data and mitigation resources like credit monitoring services.**
3. **Internal Documentation:**
    - **Created an incident log for legal and audit purposes. This included evidence such as log files, forensic analysis reports, and an action timeline.**

Technical Challenges:

- **Ensuring encryption during email notifications to prevent secondary breaches.**

Future Compliance Measures:

- **Regular audits of data storage and handling practices.**
- **Conducting tabletop exercises for breach response.**

Task 5: Communication and Notification

Objective: Develop and execute a communication plan for stakeholders.

Stakeholder Communication:

- **Customers: Drafted clear, jargon-free notifications. Emails included the nature of the breach, actions taken, and recommendations for safeguarding their accounts.**
- **Regulators: Provided detailed compliance reports with technical breakdowns.**
- **Internal Teams: Conducted briefings with IT, legal, and PR departments.**

Notification Content:

- **Subject: “Important Security Notice from ABC SecureBank”**
- **Body:**
  “We regret to inform you that a security breach involving your account occurred between December 10–20, 2024. Exposed data includes your name, account number, and transaction history. We recommend enabling fraud alerts and using our free credit monitoring services. Please contact our helpline for assistance.”

Public Relations Strategy:

- **Published a press release emphasizing transparency and ongoing security upgrades.**
- **Organized a media Q&A session to address public concerns.**

Technical Considerations:

- **Used encrypted email gateways to ensure secure notifications.**
- **Deployed a temporary website section with FAQs for customer queries.**

Task 6: Post-Incident Review

Objective: Conduct a comprehensive review to identify and mitigate weaknesses.

Weaknesses Identified:

1. **Employee Awareness: Lack of phishing awareness led to the initial compromise.**
2. **Access Control: Weak password policies allowed rapid exploitation of user accounts.**
3. **Monitoring Gaps: Anomalous activities were not detected in real-time due to insufficient log monitoring.**

Review Findings:

- **Incident response time was delayed by 48 hours due to manual log analysis.**
- **Network segmentation was insufficient, allowing the attacker to move laterally.**

Recommendations:

1. **Training: Implement bi-annual security training for employees with simulated phishing exercises.**
2. **Zero-Trust Architecture: Segment networks and enforce role-based access controls.**
3. **Automation: Deploy advanced SIEM tools with AI-based anomaly detection to reduce response time.**

Future Plans:

- **Schedule quarterly penetration tests.**
- **Update the incident response plan and perform dry runs with all departments.**
