Uyor Chimdi Ebulu

Financial Services - Phishing Attack Compromising Client Accounts

Preparation

Objective: Establish proactive measures to detect, prevent, and respond effectively to phishing attacks.

- Implement **security awareness training** for employees, focusing on phishing attack identification and best practices.
- Enforce **multi-factor authentication (MFA)** for employee and client account access.
- Deploy **email filtering solutions** to block phishing emails.
- Maintain **up-to-date security patches** and endpoint protection solutions.
- Develop an **Incident Response Team (IRT)** with predefined roles and responsibilities.
- Establish **incident reporting channels** for employees and clients.
- Conduct regular **tabletop exercises** and **phishing simulation drills**.

Identification

Objective: Detect and confirm unauthorized access from phishing attacks.

- Monitor for unusual logins, suspicious transactions, and abnormal activity.
- Use Security Information and Event Management [SIEM] tools to analyze and correlate logs.
- Validate compromised accounts via Active Directory and authentication logs.
- Determine the scope of the attack, including affected employees and stolen credentials.
- Immediately notify the Incident Response Team (IRT) and senior management.

Containment

Objective: Minimize impact and prevent further damage.

- Disable affected accounts and enforce password resets.
- Revoke unauthorized sessions and access tokens.
- Freeze compromised client accounts to prevent financial loss.
- Block malicious domains and IPs linked to the attack.
- Alert financial monitoring teams to stop unauthorized transfers.
- Inform employees and clients about the incident and necessary actions.

Eradication

Objective: Eliminate the threat and prevent reinfection.

- Perform **forensic analysis** to find and remove malicious scripts or access points.
- Patch exploited **vulnerabilities** to prevent future attacks.
- Scan systems for **backdoors or malware**.
- Strengthen **security settings** and access controls.
- Re-educate employees on **phishing prevention**.

Recovery

Objective: Securely restore operations and verify system integrity.

- **Re-enable accounts** after validation and password resets.
- **Monitor systems** for lingering threats.
- **Verify fund recovery** if unauthorized transfers occurred.
- **Notify affected clients** and provide fraud protection if needed.
- **Conduct a security audit** before fully resuming operations.

Lessons Learned

Objective: Strengthen security and prevent future incidents.

- **Conduct a post-incident review** with stakeholders.
- **Document findings** on attack methods, response effectiveness, and improvements.
- **Enhance phishing training** with updated tactics.
- **Improve email security** (DMARC, SPF, DKIM).
- **Refine incident response** for faster detection and action.
- **Report the incident** to regulators if required for compliance (PCI DSS, GDPR, GLBA).

Communication Strategy

- **Internal:** Alert **IRT, executives, IT teams, and affected employees** immediately.
- **External:** Inform **clients** via email, SMS, or phone with security steps.
- **Regulatory Compliance:** Report to **financial regulators and law enforcement** if required.
- **Public Relations:** Release a **transparent statement** to maintain trust while preventing panic.

Un grand merci