cyberflexx

Preventing Phishing Attempts

1. Monitoring for Suspicious Domain Registrations

DPM continuously monitors for domain registrations that closely resemble your organization's domain. This includes:

- Similar Domain Names: Identifying domains that use typosquatting (e.g., „example.com" instead of „example.com") or variations of your official domain name.
- Keyword Monitoring: Tracking keywords related to your organization, products, or brand names used in new domain registrations.

2. Detection of SSL Certificate Issuance

Phishing websites often use SSL certificates to appear legitimate. DPM not only examines newly registered domain names for potential fakes and look-alikes but also monitors whether these domains obtain SSL certificates, which can be a significant indicator of an impending attack. This involves:

- Certificate Transparency Logs: Monitoring these logs to detect when SSL certificates are issued for domains resembling your own.
- Immediate Alerts: Sending notifications as soon as a suspicious certificate issuance is detected.

3. "Freshness" monitoring

"Freshness" Monitoring DPM checks the freshness of SSL certificates to eliminate false positives from domains registered a long time ago. This feature focuses on newly issued certificates, which are more likely to be used in upcoming phishing attacks. By doing so, it helps prioritize monitoring efforts on domains that pose a more immediate threat.

4. Real-Time Alerts and Notifications

DPM ensures that your security team is promptly informed about potential phishing threats through many different channels. The following are the most common used:

- Email Alerts: Immediate notifications sent to your inbox with details about the suspicious domain and certificate.
- Slack Notifications: Real-time alerts within your Slack workspace for quick team awareness and response.
- Webhooks and API Integrations: Custom notifications integrated with your existing security infrastructure, allowing for automated incident management.

cyberflexx

4. Next Steps

Upon receiving an alert, your security team can take immediate action to mitigate the threat:

- Domain Blocking: Actively block the suspicious domain within your network to prevent access by employees.
- Raising Awareness: Informing the team about the detected phishing attempt to ensure heightened vigilance and caution.
- Phishing Campaign Prevention: Implementing additional security measures such as email filtering and enhanced authentication processes to protect against targeted phishing campaigns.

5. Add-On Services

In addition to benefits provided by DPM, we can also support your organization by provision of: Security Awareness Training: Regularly update and educate employees on recognizing and avoiding phishing attempts.

- Automated VA scanning: We can provide extended monitoring of your external exposure by periodically deploying industry standard scanners (like Nessus Professional) to provide you with a list of potential vulnerabilities.
- Verification of Security Posture / Penetration testing: We can execute penetration testing, security assessment or red-team project, allowing for proactive verification of your organization security posture (external and internal) trying to exploit any potential vulnerabilities.
- AI Chatbot / LLM Security Assessment: Conducting a security audit of AI based Chatbot or LLM for organizations planning to expose such a service externally to customers or partners.

Benefits of Using DPM for Phishing Prevention

- Early Detection: Identify suspicious domain registrations and SSL certificate issuances promptly, allowing for immediate action.
- Real-Time Alerts: Receive instant notifications through multiple channels to ensure quick response and mitigation.
- Proactive Defense: Block phishing domains and raise team awareness to prevent successful phishing campaigns.
- Improved Security Posture: Continuous monitoring and proactive measures enhance overall organizational security.

Conclusion

Preventing phishing attacks is a fundamental aspect of any organization's cybersecurity strategy. With DPM, businesses can detect and respond to phishing attempts in real-time, significantly reducing the risk of data breaches and security incidents. By staying vigilant and proactive, organizations can protect their sensitive information and ensure the safety of their employees.