Mitigation Plan for Lookalike Domains

This plan outlines strategies to reduce the risks associated with lookalike domains as part of a comprehensive attack surface management approach.

1. Domain Monitoring and Registration

- Implement continuous monitoring for new domain registrations similar to your brand.
- Proactively register common misspellings and variations of your domain.
- Consider registering your domain across multiple top-level domains (TLDs).

2. Technical Measures

- Implement DMARC, SPF, and DKIM email authentication protocols.
- Use SSL/TLS certificates with Extended Validation (EV) for official websites.
- Employ anti-phishing filters and security headers (e.g., HTTP Strict Transport Security).

3. Takedown Procedures

- Establish relationships with domain registrars and hosting providers.
- Develop a rapid response plan for reporting and taking down malicious lookalike domains.
- Consider engaging a brand protection service for continuous monitoring and takedown assistance.

4. User Education and Awareness

- Conduct regular phishing awareness training for employees.
- Educate customers about how to identify legitimate communications and websites.
- Implement clear communication guidelines for official company emails and websites.

5. Brand Protection Strategies

- Use consistent branding across all official digital properties.

- Clearly communicate official domain names to customers.
- Implement visual security indicators on official websites and emails.

By implementing this comprehensive mitigation plan, organizations can significantly reduce the risks associated with lookalike domains and strengthen their overall security posture.

Revision #1
Created 19 September 2024 16:03:12 by Admin
Updated 19 September 2024 16:04:18 by Admin