Securing Your Critical Infrastructure

Phishing Penetration Test

- ASSESS EMAIL SECURITY ARCHITECTURE
  Determine whether the existing email infrastructure is adequately configured to mitigate probable phishing attack vectors, as well as afford client's sufficient knowledge and notice to adequately respond to any attack.
- ASSESS CLIENT-SIDE SECURITY
  Determine whether servers and systems are appropriately hardened to mitigate phishing attacks.
- ASSESS EXISTING SECURITY AWARENESS & TRAINING
  Analyze whether existing security awareness and training are adequate to prevent phishing or social engineering attacks.
- ANALYZE AND DOCUMENT FINDINGS
  Analysis and documentation, including findings and recommendations at both a technical and procedural level.

relay SECURITY GROUP

Service Offering

Details

Relay Security Group, LLC (Relay) was founded in 2007 by information security professionals with over twenty years of cumulative IT security experience in a wide range of markets. Our mission is to provide our clients—through actual validation of vulnerabilities and with minimal impact on their often-sensitive operations—with the most accurate information about security threats to their environments and their readiness to meet current industry standards and regulations. Relay's validation methodology, processes, and recommendations take into account the complexities of these environments, which translate to recommendations that are both reasonable and actionable.

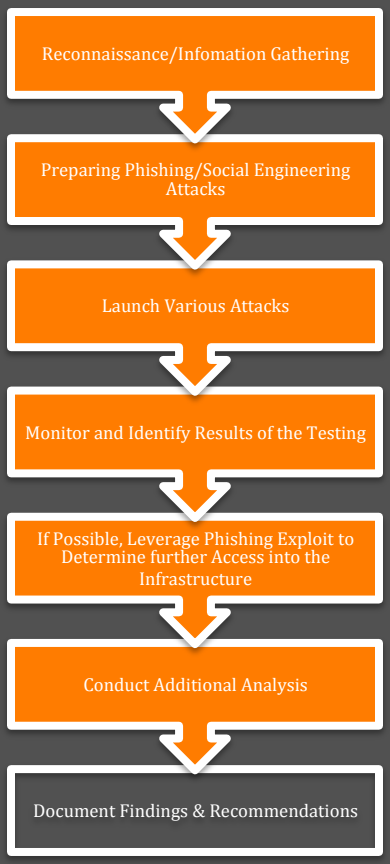
Relay's Phishing Penetration Testing services are based on proven penetration testing and vulnerability assessment methodology, which incorporates the Open Source Security Testing Methodology Manual (OSSTMM) v3.0 in combination with Relay's proprietary techniques that, not only takes into account industry specific requirements, but also provides a detailed review of the client's systems and networks.

Relay's Phishing Penetration Testing services are a specific Social Engineering effort that will assist a client in identifying whether or not their existing email infrastructure and client side environment are poorly configured and if so, what probable attack vectors may be used to either gather information or gain unauthorized access to systems and the infrastructure.

The testing, which is conducted as a cooperative effort can be executed against a general sample size or a key set of users (i.e. Spear Phishing). As part of the testing process, no attempts are made to harm or cause degradation to any application or system, only to demonstrate capabilities of compromise for validation purposes.

Typically, the phishing penetration testing process includes:

1. Identifying and validating specific client scenarios and goals of the testing;
2. Creating/verifying all necessary, DNS, email, and website content;
3. Coordinating management of DNS, email, and website content with the client;
4. Verifying the sampling of users gathered and to be targeted;
5. Conducting the phishing penetration tests against all the responsive users;
6. Based on the goals, escalating client-side and network access; and
7. Conducting an analysis of the data and providing a report outlining the findings and recommendations of the engagement.



3750 Brodie Way Dublin California 94568 ☎ 800.613.0431 ✉ sales@relaysecurity.com WWW.RELAYSECURITY.COM