SECUREDATA
TRUSTED CYBERSECURITY EXPERTS

PHISHING AS A SERVICE

KEY BENEFITS & DELIVERABLES

- **Real-World testing:** Tests conducted by human 'phishers' with 18 years of ethical hacking experience to craft emails deceiving spam-filters and adapt according to user response
- **Vulnerability insight:** Deliver two types of campaign during each quarter, although this can be customised, to assess user's susceptibility to: -
  - o Easy to spot campaign, masquerading as a typical poorly worded phishing attack attempting to deceive users
  - o A more sophisticated campaign designed to closely mirror legitimate communications
- **Targeted training** Tracking usernames of those who followed the social engineering instructions by clicking hyperlinks and opening email attachments
- **Risk prioritisation:** Carry out a risk analysis with business impact on the probability of an attack's success
- **Ongoing assessment:** Engagement with the client to establish a security awareness training schedule whereby at-risk users are enabled to identify and report suspicious emails across varying levels of sophistication
- **Measurable results:** As an ongoing service, organisations are able to track whether response to phishing emails improve

KEY SERVICE COMPONENTS

- Construction and sending of an unsophisticated email lure on a quarterly basis to test user vulnerability to 'simple' social engineering
- Construction and sending of a sophisticated email lure on a quarterly basis to test user vulnerability to more deceptive social engineering
- Performance of various deception techniques for the sophisticated email to bypass spam-filtering mechanisms
- Construction of a controlled website landing page to track user click-through rates
- Construction and embedding of non-malicious email attachments reporting back to our controlled servers to track user click-through rates
- Tracking the user names and email addresses of those falling victim to the phishing test
- Tracking the internet browsers used to open the lure emails from web-mail
- Tracking the operating systems used to open the lure emails
- Tracking the user agents used to open the lure emails
- Conducting a contextual risk analysis of the business impact due to a successful attack & the most successful attack vectors

SERVICE DESCRIPTION

Phishing, as a social engineering exercise, is a form of attack conducted by a malicious actor attempting to gain access to an organisation's infrastructure or information by enticing an employee, contractor, supplier or 3rd party partner to respond to malicious emails.

Phishing has varied goals, including injecting ransomware, host compromise, gaining user credentials and information gathering. These attacks can be conducted via email or instant message and is typically sent to a number of people simultaneously in the hope that at least one user will open the email and click the embedded hyperlink or open the attachment. The hyperlink may redirect to a website, masquerading as a legitimate website, where a username and password is requested.

Phishing is the most prevalent form of attack and is often the cause of major compromises. Phishing targets the organisation's weakest link, the users, who do not have the benefit of IT security awareness. This makes the employee an unwitting ally to a convincing attacker and can cause even the best, multi-layered, well-funded IT security infrastructure to fail at protecting the business's critical assets.

Available as a one-off assessment with a maximum 250 email addresses tested or as a subscription service with no limit on the number of email addresses, SecureData's Phishing as a Service is designed for organisations concerned about their users' security awareness, seeking assurance that their employees are able to identify and report suspicious communications.

Using techniques and methods identical to those employed by malicious actors, either as a limited test where usernames and email addresses are supplied by the client or as an unlimited test against any email addresses discovered from publicly accessible sources, SecureData will provide quarterly assessments of an organisation's employee's susceptibility to social engineering via email.

WHY SECUREDATA

Cybersecurity specialists
SecureData specialises in cybersecurity services and solutions, with a 25-year track record of delivering managed services to some of the largest companies in the world.

Outstanding expertise
Our Managed Firewall service is delivered by our UK-based SOC - delivering immediate, 24x7x365 access to specialists who deal with device health incidents, requested and recommended changes, security optimisation and help ensure continuous availability.

Extensive security insight
SecureData's Threat Intelligence platform processes over 30 billion security events per month, giving us unparalleled access to current and emerging threats. SensePost, our elite consulting arm, is at the forefront of cybersecurity - providing insight into the criminal mind-set. We use this information to ensure our Managed Firewall customers are as secure as they possibly can be.

Vendor insights
Our close partnership with Check Point, Fortinet, Cisco and Palo Alto Networks provides superior access to their technical experts and product roadmaps - keeping our SOC's knowledge ahead of the game.

Complementary services
We offer a broad range of services that complement our Managed Firewall service and strengthen your security posture, including Managed IDS/IPS, Managed Threat Detection, Managed Vulnerability Scanning and Managed Compliance Monitoring.

ABOUT SECUREDATA

SecureData is a leading provider of cybersecurity services and solutions.

SecureData looks beyond point technologies to address cybersecurity as a whole. The company offers a comprehensive set of professional and managed security services across the entire attack continuum.

For over 25 years SecureData has been helping organisations assess risks, detect threats, protect assets and respond to breaches quickly and effectively ensuring essential IT infrastructure always remains secure and available.

SensePost, the consulting arm of SecureData includes some of the world's most preeminent cybersecurity experts. Trusted by both corporate and military organisations across multiple countries, SensePost helps organisations to protect IT infrastructure and stay ahead of evolving cybersecurity threats.

Operating across the UK, South Africa and the USA, SecureData has an enviable track record having delivered cybersecurity services for many business sectors including finance, insurance, retail, property, professional services, technology and government.

@SECUREDATAEUROPE @SECDATAEU WWW.SECDATA.COM

@SENSEPOST @SENSEPOST WWW.SENSEPOST.COM

SENSEPOST

FOR MORE INFORMATION PLEASE CONTACT US
T: +44 (0)1622 723400 | E: info@secdata.com