ENGINEERING WHITEPAPER

Peraton LABS

PROTECTING AGAINST CYBERATTACK’S BIGGEST THREAT VECTOR

SOCIAL ENGINEERING SECURITY ASSESSMENTS TO IMPROVE YOUR CYBERDEFENSE POSTURE

PROBLEM STATEMENT

Commercial enterprises, civil and municipal agencies, and U. S. government entities continue to experience a significant increase in cyberattacks. Ransomware attacks are the subject of daily news articles. Municipalities across the U.S., healthcare institutions, and more recently, critical national infrastructure operators with the Colonial Pipeline attack have become victims. Supply chain attacks similarly have exposed security weaknesses among the contractors and services providers, with hackers using their infrastructure to impersonate and target utility operators. The SolarWinds attack demonstrated the sophistication of recent attacks.

Whether the malicious actors are nation-state sponsored or criminal, most cyberattacks typically begin with unsophisticated social engineering attacks, such as phishing, baiting, pretexting, telephone impersonation, social targeting, and physical site entry. All usually target people.

What Is Social Engineering?

Social engineering is a common technique malicious actors use to gain the trust of employees. By offering valuable lures or using impersonation, malicious actors gain personal information in order to launch deeper cyberattackes, such as inserting malware.

People are an organization's most important business asset, but untrained and uninformed employees can also be its greatest security risk. Human psychology and our social nature make it natural to try to help others, expect goodwill interactions, and want to trust. Attackers try to exploit the good intention of others. They do it in different ways—by phone, in person, via email, via text messaging, and other forms of interaction that involve people. Social engineering is likely the oldest security risk known to mankind. Everyone is susceptible and, because attacks change over time, these masquerades are not readily identified.

Common email social engineering techniques are:

- Phishing—an online scam where malicious actors impersonate legitimate organizations via email, text message, advertisement, or other means to gain access to sensitive information.
- Spear phishing—a highly targeted form of phishing by actors pretending to personally know you or do business with you.
- Whaling—a form of phishing that targets executives or high-ranking individuals that have elevated authority within an organization.

More refined forms of social engineering include business email compromise scams, where the malicious actor, with some knowledge of the target, their work processes, or what will motivate the target, mimics common work functions or adds a sense of urgency to the malicious request. Vishing (aka voice phishing) is used to call targets directly—often impersonating authority figures, including threats, or mimicking tech phishing tactics via text messages. Hackers will use whichever approach or attack vector is easiest and most likely to succeed, and they are always creating new ones.

Ransomware

Ransomware has become the fastest growing cybercrime at an estimated global cost of $20 billion in 2020—a fourfold increase in just three years. Occurring roughly every 14 seconds, no organization is immune from this accelerating threat in which cybercriminals threaten to delete, withhold, or publish business-critical information and sensitive data.

Ransomware attacks tend to follow a model, where the targeted network is first infiltrated using social engineering, usually with phishing methods, then the malicious actor explores, pivots, and moves laterally to exploit critical business systems to deploy the ransomware or exfiltrate sensitive data.

Increasing threats and cyberattacks demonstrate that all requests for information must be evaluated for authenticity as well as the need to know.

- Studies continue to show that social engineering is the No. 1 threat vector for cyberattacks.
- According to a 2019 report, 32% of all data breaches employed some form of social engineering attack.

IMPROVING CYBERSECURITY WITH SOCIAL ENGINEERING ASSESSMENTS

Peraton Labs offers social engineering assessments to identify security risks associated with employee and contractor behavior, poorly implemented personnel security policies, and lack of knowledge of approved procedures, as well as highlighting insufficient or ineffective security awareness training. Peraton Labs' social engineering assessments validate the operational security controls in place, test whether your company policies are understood and practiced, and uncover gaps in both policy and practical implementation.

The goal of Peraton Labs' social engineering security services is to help organizations understand the security awareness of their staff as a fundamental part of people/process/technology security. Our services apply a custom approach to each customer where we test deceptions that are tailored to the their customer's business operation. We help them understand the risks, identify gaps in security awareness, company policies and technologies, and make actionable recommendations.

We create custom social engineering campaigns specific to the organization's business purpose using up to five vectors:

1. Phishing/spear phishing/whaling;
2. Phone-based social engineering;
3. Rogue Wi-Fi network access points;
4. Physical (tailgating, talk your way); and
5. Exploitable portable media.

We perform reconnaissance on the targets, create a custom campaign, and then execute it in a multi-phase fashion.

Email/Telephone Assessment

Peraton Labs conducts phone and email-based social engineering testing against a company's staff to ascertain the susceptibility of its workforce to social engineering attacks.

As an example of Peraton Labs' logical security controls assessment, we would:

- Assess a representative sample of your employees, along with who you identify and provide contact information.
- Develop a relevant storyline for two social engineering scenarios designed to entice targets to 1) run commands on their computer, or 2) open an email and click on a URL (to an external website).
- Register a domain name, set up email, and customer creates a webpage to support the claimed identity.

Physical Site Assessment

During customer site visits, Peraton Labs conducts an external site assessment for physical security controls. We observe the activities at the location, the movement of people and goods, the means to access the building, and the handling of deliveries and contractors.

Approximately 90% of confirmed phishing email attacks took place in environments with Secure Email Gateways, emphasizing that an alert and informed workforce is still the best defense.

The COVID-19 pandemic and government restrictions have fostered an increase in the size of the remote workforce. Employees now rely more on electronic than in-person interactions, which provides even greater opportunity for social engineering attacks.

Increased distractions while working from home can make employees more careless. Employees can easily become desensitized and fall prey to phishing and other social engineering attacks.

In a recent study, 52% of employees said that COVID-19 stress has caused them to make more mistakes.

In this environment, businesses must identify weaknesses in employee behavior and focus their efforts to improve security awareness.

Peraton Labs assesses whether procedures in use comply with your security policies. We plan and execute one or more activities to assess implementation of your company policies and efficacy of training. The goal of these activities is to gain unauthorized physical access to one or more of your facilities.

As an example of Peraton Labs' physical security site assessment, we would examine:

- Signage
- Fences
- Landscaping
- Vehicle barriers
- Lights/motion sensors
- Active monitoring of video surveillance, camera placement, and use of motion sensors
- Building entry controls
- Locks
- Mantraps
- Badging (smart vs. photo only)
- Tailgating
- Alternate entrances, emergency exits, shipping/loading entrances
- Co-location controls
- Shared space for personnel and data equipment
- Security guards
- Screening
- Availability
- Reliability
- Training
- Monitoring and alarming

CASE STUDIES

Case 1

Peraton Labs conducted a phone and email-based social engineering assessment to benchmark the susceptibility of a customer's workforce to a phishing attack. Specifically, we:

- Designed a ruse involving a potential services supplier by registering a convincing email address and website.
- Reached out by phone and email to a cross section of employees in various roles including levels of management.
- Succeeded in enticing almost 40% of the employees to undertake risky action in response.

The results of Peraton Labs' social engineering exercise underscored the need for expanding the employee cybersecurity awareness program and conducting regular cyber testing.

Case 2

Peraton Labs’ assessors performed a physical site assessment, in which we were able to access a sensitive customer facility that was protected by badge access controls. Once in the building, our assessors, not wearing the required employee badges, searched for an empty conference room, connected to an unprotected internal network Ethernet port, and explored the company’s infrastructure undetected for hours. Our team located an open mail relay on the network, launched an email phishing campaign, and successfully obtained valid user credentials to company IT services.

PERATON LABS SOCIAL ENGINEERING ASSESSMENT SERVICES

- Personnel cybersecurity awareness
- Email phishing risk assessment
- Phone phishing risk assessment
- Insider impersonation
- Physical site assessment

360-DEGREE SECURITY CONSULTING SERVICES

Social engineering assessments are part of Peraton Labs’ comprehensive, 360-degree enterprise risk assessment services. Our end-to-end cybersecurity consulting services help measure your cybersecurity posture using the NIST Cybersecurity framework and develop a gap profile to prioritize investments.

Our 360-degree risk assessment approach includes:

- Service/operation criticality analysis
- Threat identification
- People awareness/behavior
- Process and procedures
- 4-Quadrant IT and OT vulnerability assessment
- Physical infrastructure assessment
- Present state enterprise risk profile
- Future state and gap profiles

Our suite of technology security analyses applies our deep and broad experience, and customized methodologies and tools, to the focused needs of the public and commercial sectors to provide customers with a comprehensive view of their security posture, possible solutions to fill gaps, and insights into trends to help prepare for the future.

Our 4-Quadrant vulnerability assessment and penetration testing methodology leverages Peraton Labs' invaluable cybersecurity knowledge and insight. We’ve developed state-of-the-art services, which employ a comprehensive systematic approach that includes network, wireless (radio), management application software, and embedded hardware and firmware. This 4-Quardrant approach provides a holistic, integrated evaluation of security weaknesses across each of the quadrants of a customer’s environment to expose and mitigate critical risks not apparent when looking at one quadrant at a time.

See Vulnerability and risk analysis - Peraton Labs for more information about our cybersecurity services.

Contact us at: info@peratonlabs.com.

Peraton | LABS

Learn more at peratonlabs.com