



Product Brief

AT&T Consulting Security Penetration Testing

New and rapidly deployed technologies, changing workforces, and additional regulations are increasing the operating complexity within many organizations. Additionally, advances in hacking tools and techniques are forcing your IT staff to defend against increasing threats, while budgetary pressures are often preventing a corresponding increase in available resources.

Organizations such as yours have undertaken various security assessments, including vulnerability scanning and testing. However, one problem with such assessments is that a clear understanding of the risk may not always be apparent, and guidance may not always be followed. It is common for a vulnerability assessment to flag problems that are not addressed until after a significant security incident occurs. When a penetration test is successful, it is a clear demonstration of an inadequacy within a system. A penetration test provides additional details that substantiate the potential for a significant security incident, which can motivate your organization to take action.

Penetration Testing

The AT&T Penetration Test offering can be tailored to meet your specific needs. Testing can be modeled to replicate various types of attackers, from opportunistic Internet threats to the knowledgeable insider.

A Penetration Test performed by AT&T Consulting can be used to evaluate your incident response capabilities, to validate the efficacy of security controls, and to provide management with “real world” attack scenarios that include walk-through of actual compromises.

Solution

Penetration testing is often referred to as “Ethical Hacking” and uses the same tools and techniques that attackers are likely to employ. Unlike a malicious adversary, though, our Penetration Test is performed in accordance with pre-defined rules-of-engagement to minimize the impact of testing on your organization’s systems and infrastructure.

The initial scoping of a Penetration Test determines the size and types of activities required to provide the most value for you, such as the following.

Incident Response Test

A swift and measured response to security events is critical to an organization’s ability to adequately defend itself. AT&T Consulting can employ evasion, diversion and various specialized techniques to replicate different types of attackers, including motivated attackers and other malicious activities. These activities allow you to evaluate your ability to detect and respond to a wide range of penetration attempts.

External Penetration Test

From worms and botnets to motivated attackers, an organization’s public footprint is continuously being probed. An External Penetration Test provides a view of your organization from the attacker’s perspective and can be used to meet many of the regulatory and industry compliance requirements for penetration testing.

Potential Benefits

- Allow organizations to analyze your current “real world” security level
- Rationalize information security investments
- Help reduce security risks
- Measure operational effectiveness of security controls
- Evaluate and address compliance requirements and industry standards

Features

- Incident Response Test
- External Penetration Test
- Internal Penetration Test
- Wireless Penetration Test
- Physical Penetration Test
- War Dialing and PBX Test
- Social Engineering

To learn more about AT&T Security Consulting, visit www.att.com/security-consulting or [have us contact you.](#)

Share this with your peers



Internal Penetration Test

Whether it is the deployment of new collaborative and social networking technologies or changes in an organization's workforce due to mergers and acquisitions and outsourcing, operating environments are becoming more complex. An Internal Penetration Test provides a rigorous stress test of your defense-in-depth capabilities.

Wireless Penetration Test

Wireless access has become ubiquitous. There are point-to-point metro area networks connecting campuses, laptops and PDAs connecting to wireless networks, and Bluetooth devices forming personal area networks. The AT&T Consulting Wireless Penetration Test attempts to bypass the security controls of authorized wireless devices, to introduce unauthorized access points into the environment, and to exploit the weaknesses of any discovered rogue devices.

Physical Penetration Test

Without physical security there is no security and yet physical security controls are less likely to be fully integrated into IT and Security Guards are often outsourced. The separation of physical security controls can create exploitable security boundaries within an organization. The AT&T Consulting Physical Penetration Test attempts to gain unauthorized access to secured resources using various non-destructive entry methods, including bypassing Request-to-Exit controls and lock picking.

War Dialing and PBX Test

Now often forgotten, war dialing and PBX exploitation was once the primary means for an attacker to gain unauthorized remote access. The threat still persists; as organizations become more reliant on VoIP and other IP Telephony services, the risk of interception or Denial of Service to mission-critical applications is becoming greater. Out-of-band access to infrastructure devices and other resources can be critical during an emergency, but such access must be properly secured otherwise, risk being the source of the next security incident.

Social Engineering

Social engineering is the practice of obtaining confidential or sensitive information via manipulation of legitimate users. A social engineer will commonly use the telephone, email, or Internet to deceive employees into revealing information, thereby circumventing established security controls. The AT&T Consulting Social Engineering activities provide a barometer to the effectiveness of your security awareness programs and training.

Penetration Testing Combined with Vulnerability Assessment

Often customers wish to combine Penetration Testing with Vulnerability Assessment services. This enables them to get a comprehensive view of their security posture, as well as to validate the effectiveness of controls in response to a simulated attack from within or outside the enterprise. AT&T Consulting offers several options for combining these services as well as developing customized work scope.

Key Benefits

AT&T Consulting takes a highly-customizable approach to penetration testing. We combine our in-depth knowledge with the use of industry standards, applicable regulatory requirements, business goals, and our experience delivering information security services within the security industry, as well as the retail, financial services, healthcare, government, education, media and entertainment industries.

Security Solutions: Expertise from a Trusted Provider

AT&T provides a unique and world-class portfolio of assessment, compliance and related security services. Our experience, expertise and commitment to open standards have established us as a strategic and trusted advisor with our customers. By leveraging AT&T, you can expect best-in-breed solutions, a global network of proven technology, and a cost-effective program-based approach to meet your security and compliance needs.

Share this with
your peers



For more information contact an AT&T Representative or visit www.att.com/security-consulting.



Scan this code
to learn more.

To learn more about AT&T Security Consulting,
visit www.att.com/security-consulting or [have us contact you.](#)

