Cyber Liability

Penetration Testing Explained

Keeping workplace technology up and running is vital to any organization's success. While this task seems feasible, it's growing harder and harder each year as cybercriminals expand their reach. It's not enough to simply protect workplace technology with software and security protocols. It's also critical for your organization to test the overall effectiveness of these protocols on a regular basis. That's where penetration testing can help.

Essentially, penetration testing consists of an IT professional mimicking the actions of a malicious cybercriminal to determine whether an organization's workplace technology possesses any vulnerabilities and can withstand their attack efforts. Conducting a penetration test can help your organization review the effectiveness of workplace cybersecurity measures, identify the most likely avenues for a cyberattack and better understand potential weaknesses. Review this guidance to learn more about what penetration testing is, the benefits of such testing and best practices for carrying out a successful test within your organization.

What Is Penetration Testing?

Put simply, penetration testing refers to the simulation of an actual cyberattack to analyze an organization's cybersecurity strengths and weaknesses. This testing usually targets a specific type of workplace technology, such as the organization's network(s), website, applications, software, security systems or physical assets (e.g., computers and smart devices). Penetration testing can leverage various attack methods, including malware, social engineering, password cracking and network hacking, among others.

Generally speaking, penetration testing is often performed by a professional from a contracted IT firm who is not associated with the organization being assessed in any way. This helps the cyberattack simulation seem as authentic as possible. Penetration testing is typically either external or internal in nature. The primary differences between these forms of testing are as follows:

- External penetration testing requires the IT expert to attack an organization's external-facing workplace technology from an outside perspective. In most cases, the IT professional won't even be permitted to enter the organization's physical establishment during external penetration testing. Rather, they must execute the cyberattack remotely—often from a vehicle or building nearby—to imitate the methods of an actual cybercriminal.
- Internal penetration testing allows the IT expert to attack an organization's internal-facing workplace technology from an inside perspective. This form of testing can help the organization understand the amount of damage that an aggrieved employee could potentially inflict through a cyberattack.

In addition to these testing formats, there are also two distinct types of penetration tests. How much information an organization provides the IT professional prior to the cyberattack simulation will determine the penetration test type. Specifically:

- An open-box test occurs when the IT expert is given some details regarding the organization's workplace technology or cybersecurity protocols before launching the attack.
- A closed-box test occurs when the IT expert is provided with no details other than the organization's name before

conducting the attack.

Ultimately, the penetration testing format and type should be selected based on the particular workplace technology elements or cybersecurity measures that an organization is looking to evaluate.

Benefits of Penetration Testing

Penetration testing can offer numerous advantages to your organization, including:

- Improved cybersecurity evaluations—By simulating realistic cyberattack situations, penetration testing can help your organization more accurately evaluate its varying security strengths and weaknesses—as well as reveal the true costs and of any security concerns.
- Greater detection of potential vulnerabilities—If any of your workplace technology or other cybersecurity protocols fail during a penetration test, you will have a clearer picture of where your organization is most vulnerable. You can then use this information to rectify any security gaps or invest further in certain cyber initiatives.
- Increased compliance capabilities—In some sectors, organizations are legally required to engage in penetration testing. For example, the Payment Card Industry Data Security Standard calls for organizations that accept or process payment transactions to execute routine penetration tests. As such, conducting these tests may help your organization remain compliant and uphold sector-specific expectations.
- Bolstered cybersecurity awareness—Mimicking real-life cyberattack circumstances will highlight the value of having effective prevention measures in place for your employees, thus encouraging them to prioritize workplace cybersecurity protocols.

Penetration Testing Best Practices

Consider these top tips for executing a successful penetration test within your organization:

- Establish goals. It's crucial for you to decide what your organization's goals are regarding the penetration test. In particular, be sure to ask:
  - What is my organization looking to gain or better understand from penetration testing?
  - Which cybersecurity threats and trends are currently most prevalent within my organization or industry? How can these threats and trends be applied to the penetration test?
  - What specific workplace technology elements or cybersecurity protocols will the penetration test target?
- Select a trusted IT professional. Consult an experienced IT expert to assist your organization with the penetration test. Make sure to share your organization's goals with the IT professional to help them understand how to best execute the test.
- Have a plan. Before beginning the penetration test, work with the IT expert to create an appropriate plan. This plan should outline:
  - The general testing timeframe
  - Who will be made aware of the test
  - The test type and format
  - Which regulatory requirements (if any) must be satisfied through the test
  - The boundaries of the test (e.g., which cyberattack simulations can be utilized and what workplace technology can be targeted)
- Document and review the results. Take detailed notes as the penetration test occurs and review test results with the IT expert. Look closely at which cybersecurity tactics were successful during the attack simulation and which measures fell short, as well as the consequences of these shortcomings. Ask the IT professional for suggestions on how to rectify security gaps properly.
- Make changes as needed. Based on penetration test results, make any necessary adjustments to workplace technology or cybersecurity protocols. This may entail updating security software or revising workplace policies.
- Follow a schedule. Conduct penetration testing at least once every year, as well as after implementing any new workplace technology.

For more risk management guidance and insurance solutions, contact us today.