PENETRATION TESTING:

The Why, How & Top Benefits

In March 2016, Verizon Enterprise Solutions suffered a data breach that affected an estimated 1.5 million customers.

In a response related to the breach, the company stated, “Verizon recently discovered and remediated a security vulnerability on our enterprise client portal. Our investigation to date found an attacker obtained basic contact information on a number of our enterprise customers.”

While the number of records and type of information may not be as big as other breaches (e.g., 80 million healthcare-related records in the Anthem breach), this is the type of vulnerability that likely should have been detected.

By virtue of being on the Internet, your company has at least one potential opportunity for attackers, and realistically many more. How can you protect your company, its data and the information your customers have entrusted to you?

schellman
formerly BrightLine

THE VALUE OF A

PENETRATION TEST

A penetration test performed by experienced and trained professionals finds vulnerabilities and exploits vulnerabilities in your systems. While many organizations can perform vulnerability scanning and understand the results, a properly performed penetration test uncovers valuable insight into the effectiveness of your security controls against a skilled, human attacker.

PENETRATION TESTING CAN:

1. Identify vulnerabilities that would be difficult, or potentially impossible to detect using automated penetration testing or vulnerability scanning software.
2. Give you the evidence you need to support greater investment in security technology and personnel.
3. Allow you to assess the magnitude (both business and operational) of any potential successful attacks.

FREQUENTLY ASKED QUESTIONS

ABOUT PENETRATION TESTS

Does My Company Need a Penetration Test?

FOR MOST COMPANIES, THE ANSWER IS YES.

It doesn’t matter how small or large your business is, if your business operates in the cloud or stores and collects customer data, it needs a penetration test. The most common reasons an organization requests a penetration test are: It has a compliance requirement to meet, or a potential client wants to see its pen test report.

> “
>
> Think of it this way: Eventually, someone —a potential customer, an existing customer, a potential partner or the government—is going to ask how you’re storing data, if it’s secure, and probably most importantly, whether you can prove it.

HOW OFTEN SHOULD MY ORGANIZATION GET A PENETRATION TEST?

Many organizations conduct penetration tests in accordance with compliance regulations. A penetration test is required for PCI-DSS compliance, and FedRAMP. While it is not a requirement for HIPAA compliance, the National Institute of Standards and Technology issued a special recommendation for HIPAA that encourages healthcare organizations to...

> “
>
> Conduct penetration testing (where trusted insiders attempt to compromise system security for the sole purpose of testing the effectiveness of security controls), if reasonable and appropriate.

This validates your exposure to actual vulnerabilities.

If your organization doesn’t need to adhere to a penetration test timetable to be in line with compliance regulations, you might wonder how often your company should do one. A penetration test should be done as often as necessary to keep your security risks at a manageable level. Many organizations will test annually; however, major changes to an environment or application could warrant more frequent testing.

WHAT ABOUT USING AUTOMATED PENETRATION TESTING SOFTWARE?

It may be tempting to buy penetration testing software, hand it off to your IT team and consider the penetration test complete. This, however, is not a true penetration test and can lead to missed vulnerabilities within your system. While there are commercial and open source offerings to help expedite aspects of a penetration test, the software should be considered a resource and not the entire solution. Hiring a team of experienced and certified penetration testers can give you insight into vulnerabilities you may not be aware of using just software. For example, an external team can look for and exploit vulnerabilities within functions such as workflows and APIs. These are two examples of functionality that may be overlooked by or not accessible to penetration testing software alone.

HOW TO CHOOSE THE RIGHT PENETRATION TESTING PROVIDER

Given the importance of securing your sensitive data and critical applications, you will want to thoroughly vet a team of penetration testers. These individuals will be providing validation of your company and will potentially have access to your company's sensitive data.

Start by asking your potential penetration testers about their industry experience, focus and certifications. While a team might have a lot of experience, keep in mind that if they don't have experience with or knowledge of your industry, they may not be the right fit for your needs. Your team should be thorough, confident in their methodology, and have a keen eye for detail.

Once the test is complete and you have fixed any vulnerabilities, the penetration testing team should also be able to return and do a retest to ensure everything they found has been rectified.

A SAMPLE ANATOMY OF A PENETRATION TEST

Scope: SaaS-Based Application

TIME FRAME: 2-4 WEEKS

Step One

RECONNAISSANCE

The team does reconnaissance, looking at your website, offering, marketing materials and social presence. The reconnaissance is not meant to try to access your website or social media accounts, but rather to evaluate your company and take stock of your online presence. This can help the team be aware of all the possible ways someone could gain access to private information.

Step Two

TESTING

The team takes reconnaissance information and looks for low-hanging fruit like web pages that should have been removed from the server or error messages being kicked out by an old content management system.

Step Three

GAIN UNAUTHORIZED DATA

The team tests the site from the perspective of an untrusted user and an authenticated user of the application. Vulnerabilities are discovered and exploited with a goal to gain unauthorized access to systems or data.

What sets a team of professional penetration testers apart from automated software options is what they can do in Step 3. While a software tool would find and alert you to easy-to-see vulnerabilities, a team of professionals can take everything a step further and concentrate low-severity vulnerabilities to execute more advanced attacks.

Step Four

DELIVER REPORT

After the team's scope of work is complete, you should receive a testing report personalized to your business and its vulnerabilities. The report should also include instructions on how to fix any vulnerabilities.

ADDING PENETRATION TESTING TO

CURRENT COMPLIANCE INITIATIVES

When selecting a partner to conduct your penetration test, choose one that can leverage your work and can perform multiple assessments simultaneously.

Getting a penetration test done alongside your current compliance initiatives is valuable for several reasons:

1. It allows your company to test the compliance controls you've put in place.
2. The penetration testing report will be fully customized and much more detailed because the provider is immersed in your business and industry.
3. It can save time and money.

While other tests and certifications may give you an added sense of security, only a penetration test will give you a true, real-world sense of how secure your data, networks and business are.

Finding the right single assessor partner can provide you with a thorough test, and it can seamlessly integrate information learned from other assessments into your test documents, saving time and money.

DON'T PUT OFF CONDUCTING A PENETRATION TEST ANY LONGER.

Contact us to meet our expert testers and get started.

schellman
formerly BrightLine