ProCircular
SECURITY. PRIVACY. TRUST.

The Attack Path is Paved with Good Intentions:

How cybersecurity solutions create vulnerabilities

By Dawson Medin, Security Engineer II and Lindy Trout, Creative Technical Writer

New talent, technologies, and lucrative targets have led to a recent surge in the cybercrime industry. Skilled criminals are experts at navigating through data to find or create value; and our international dependence on virtual sharing and cloud storage inevitably leaves low-hanging fruit for them to find in the wild. Businesses must be aware of their cyber risks, and security firms are available to help.

Cybersecurity firms have created a booming market for penetration tests, risk assessments, incident response planning workshops, and vulnerability scanning subscriptions to help organizations understand and meet their security goals. Unfortunately, there is no "silver bullet" solution. Firewalls and endpoint protection will not make you impenetrable, security is a layered approach. A reliable security program stems from a security culture that has been fostered and supported from the inside out.

In fact, a misguided focus on cybersecurity can create more problems than solutions. A business' misunderstanding of certain assessments or end-user protection could give them a false sense of security. Overestimating a control measure's capabilities or failing to implement recommendations can create blind spots that attackers are seeking. Business owners with the best intentions could be unwittingly opening holes in their defensive perimeter.

Choosing the Right Penetration Tester

During a penetration test, an ethical hacker is granted legal permission to attack your environment and tasked with finding every way to exploit it. The most thorough penetration tests approach the network from several different perspectives, like a malicious insider, a misguided vendor, or a truly foreign attacker. They use methods like password-spraying, phishing attacks, and input validation exploitation to identify possible entrances for malicious actors. When they are finished exploring, the penetration tester cleans up their path and compiles their findings into a report of prioritized risks and recommendations. Penetration tests can be bundled with social engineering campaigns, web application testing, secure code review, or other add-ons that organizations may require.

Vulnerability assessments or scans are related to penetration tests. In fact, this scanning process is the first step of performing a penetration test. It is a much more passive assessment than a full-scale pen test. During a vulnerability scan, an engineer uses an automated tool(s) to search for potential areas of weakness. The primary advantage of a penetration test over a stand-alone vulnerability scan is that a penetration tester actually attempts to exploit the vulnerabilities they discover. They find vulnerabilities that vulnerability scanners simply cannot. Humans can track down complex, manual attack vectors.
In that light, a penetration test is only as effective as its engineer. If a network needs to be protected against attackers in the wild, then the penetration tester needs to be on par or more skilled than those malicious threats. Ask around, professional recommendations are the best way to find a fair and reputable vendor.

The most important factor in choosing a penetration test is trust. Do your research. Sloppy or cut-rate pen testers can miss important vulnerabilities, create openings that they forget to close, or leave your cybersecurity data in insecure places. These are severe concerns, as they stand out to potential attackers while going unnoticed by general users. Think carefully about the cybersecurity budget. A less expensive but less reputable cybersecurity firm could produce a negative return on investment if they leave exploitable gaps or materials in the network.

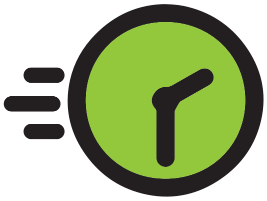
Anecdotally, I have found password lists left by previous testers in client environments. Many of the passwords were still valid. This discovery indicates a two-fold problem. Firstly, the initial pen testers were, for whatever reason, sloppy in their exploration of the client's environment. The client should contact that vendor and let them know of the mistake to prevent it from happening again. Secondly, the passwords had not been updated since they were discovered in the initial penetration test. If a real attacker had accessed that list, they would have been able to infiltrate a user account and impersonate an employee.

Getting the Most from Penetration Testing

As shown in the last example, the penetration test process is not complete at the end of the report delivery meeting. That report will act as a guide to remediating the gaps that were discovered during the assessment. Sometimes, remediation requires a simple patch or update. Other times, a vulnerability may require continuous monitoring or isolating a system from the rest of the network. Occasionally, the cost of remediating a vulnerability is higher than the risk of leaving it, so that risk is accepted and incorporated into future risk management planning. Keep in mind, only low-severity risks should be accepted into business planning. High severity risks must be remediated if they are discovered. Failing to act on these critical vulnerabilities, like neglecting to mandate a password change after several plaintext passwords were discovered, goes against the purpose of the assessment. It would be similar to going to the doctor for a prescription, then neglecting to fill it. The insights and recommendations that come with a penetration test report are valuable, but only insofar as they are used to develop the organization's security posture.

Penetration tests are tidy, self-contained engagements that can indicate to investors and stakeholders that cybersecurity is an organizational priority, but beware of developing a false sense of security. Penetration tests alone will not solve network security. Rather, they work as a tool to identify and prioritize areas of concern. The work that actually increases your defense against cyberattacks may be harder to show to a board of directors. One way is to perform annual, or otherwise recurring, penetration tests and compare the reports from one year to the next. Again, it is necessary to apply the recommendations from the initial penetration test to show improvement in the next one.

Beyond choosing which firm to contract, consider the best time to test your environment. Unfortunately, time and money are scarce, so timing a penetration test takes a little strategy. Performing a penetration test right before a large-scale system migration will not tell you very much about the security of the updated system. A company in those circumstances might choose to have a penetration test after the migration has taken place. This way, they get more relevant information, and they can see gaps they may have unintentionally opened during the transition. However, there are several factors to consider in scheduling a penetration test. Make sure to include IT, C-level executives, and even legal before formalizing the project.



The most important thing to remember is that penetration tests reveal validated, exploitable technical risks and provide prioritized recommendations for protecting the organization. Make sure to test the network(s) or system(s) that would benefit from additional insights and recommendations. Ensure you have the resources to implement the recommendations that will follow. If organizational priorities put security development at the bottom, maybe start by applying generic security best practices. Wait to invest in a penetration test until the resources are available to put the results into action.

Maximize the Value of Security Controls

In 2020, the previous records for highest ransom demand and highest-known ransom paid were both doubled at $30M and $10M, respectively. The cost of ignoring cybersecurity grows higher each day, and businesses are aware. The cybersecurity industry has seen massive growth over the past decade, and new companies are vying for a piece of the pie. It is important for vulnerable organizations to understand exactly how each security measure they implement protects their data's confidentiality, integrity, and availability. Otherwise, they could be losing money by underutilizing tools or risking exposure by leaving blind spots in the defensive strategy.

Starting with the right partner, a penetration test provides actionable insights to make security improvements to the network. Ensure the penetration test vendor is sufficiently reputable and comes with strong professional references. Before scheduling a penetration test, ensure the resources are available to implement the subsequent recommendations. Verify that your systems are in somewhat of a permanent position to prevent the results from being nullified by adjustments shortly after the test.

After the test, organize a plan to implement the recommended updates. Determine which vulnerabilities will be easy fixes, like patches or updates, and which ones will require additional investments. Mending the gaps in the network is an active way to fortify security posture. Plan to have a follow-up penetration test or vulnerability assessment after a good portion of the recommendations have been put into effect.

Lastly, cybersecurity insights are very valuable tools, and it is imperative that they not fall into the wrong hands. Cybersecurity reports and artifacts should be securely stored and protected, but they also must be shared and incorporated into business decisions. The solution is to have dedicated resources, whether that looks like an in-house security team or a representative within the IT department. There should be an assigned resource responsible for orchestrating testing and implementing remediations as they are available. Dispersed or ambiguous responsibilities lead to unresolved issues getting buried in the shuffle.

Cybersecurity affects the data and communication resources that we use every day in the business world. While our dependence on these systems should make their security more important, we can easily take them for granted and neglect to verify their security. The costs of a data breach or ransomware incident are almost always greater than the preventative measures that were initially overlooked. It should be noted, however, that the cost of network security will be greater than what you are invoiced by the firm. An effective penetration test takes months of subsequent remediation activities after the final report is delivered. Cybersecurity is not a product that can be bought or sold. Rather, it is the socialized belief that information storage and access should be controlled. A penetration test can highlight areas where that control is lacking, but resolving the issues requires dedication to the cause.