The Importance of Penetration Testing & Vulnerability Scanning

a bluedog whitepaper

bluedog
SECURITY MONITORING

Executive Summary

Cybersecurity has always been a tough area for most businesses, even for those in technology and IT. The number of threats has grown exponentially year after year. More importantly, threat types have also diversified greatly.

The COVID-19 pandemic brought a whole new level of threats. From the ones that are simple to detect (phishing attacks and scams coming from domain names that contain the word “corona”) to sophisticated network breaches that can paralyze a company’s entire operations.

As businesses all over the world moved online, the number of attacks and their success rate has grown to a level that we’ve never known before. Regardless of how the pandemic will evolve, it’s safe to say that the cybersecurity threats are here to stay.

This whitepaper will discuss the importance of prevention as the best way to mitigate cyber threats and will explain in-depth the two most effective methods of preventing cyber-attacks: penetration testing and vulnerability scanning.

You’ll learn the similarities and the differences between them, as well as which of them suits your company’s needs best.

Finally, we’ll reveal the Bluedog Security Monitoring’s proprietary method of leveraging penetration testing and vulnerability scanning so that you can achieve peace of mind and rest easy knowing that your business assets are always safe.

Table of Contents

The State of Cyber Threats

There is no absolute security. You can't have it on the street or in nature, as the pandemic taught us. And you can't have it online. As soon as a computer starts communicating with others, that computer is exposed to threats.

And by no means are these threats to be neglected.

Our computers aren't safe, especially if they are business devices. Did you know that 85% of people posting photos of puppies are actually trying to scam you[1]? Yes, it's that dire!

The number of attacks and their associated losses increase every year, as revealed by this report in the US:

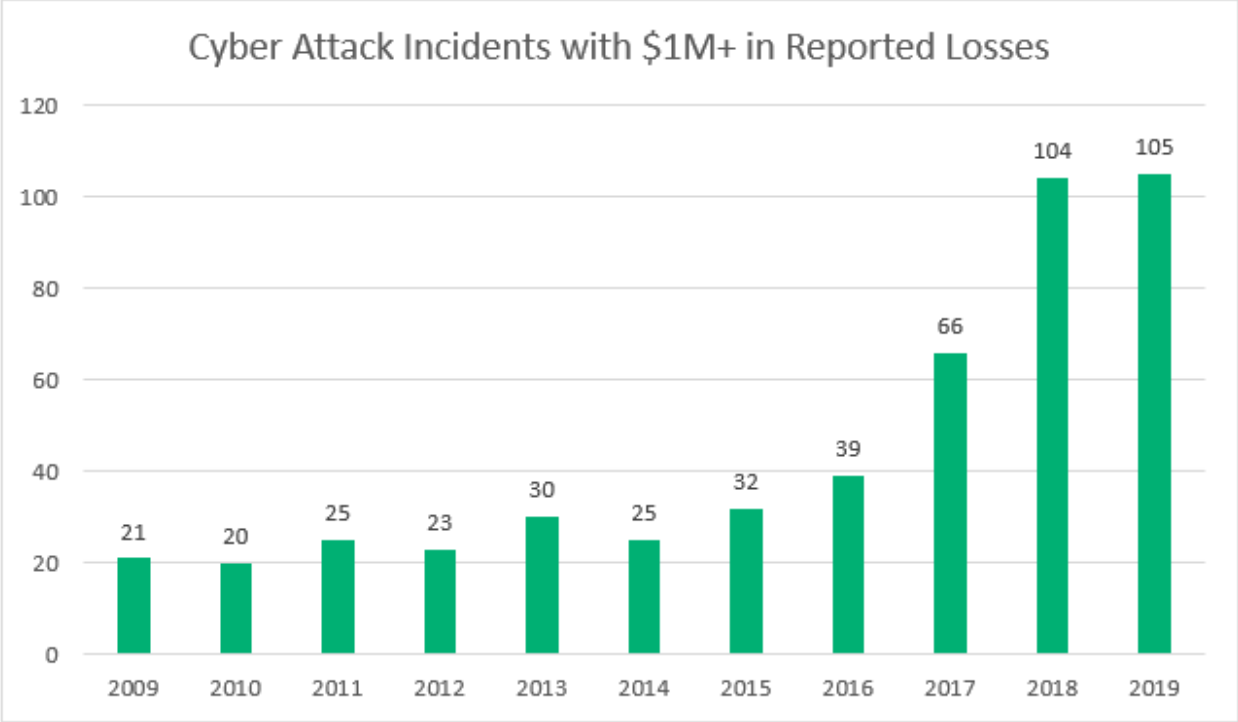

Image via Sectigostore[2]

The Google Transparency Report on Safe Browsing: malware and Phishing paints a similar picture when it comes to the number of websites that can be associated with phishing attempts and malware:

[1] https://www.fintechnews.org/the-2020-cybersecurity-stats-you-need-to-know/, retrieved September 2020
[2] https://sectigostore.com/blog/42-cyber-attack-statistics-by-year-a-look-at-the-last-decade/, retrieved September 2020

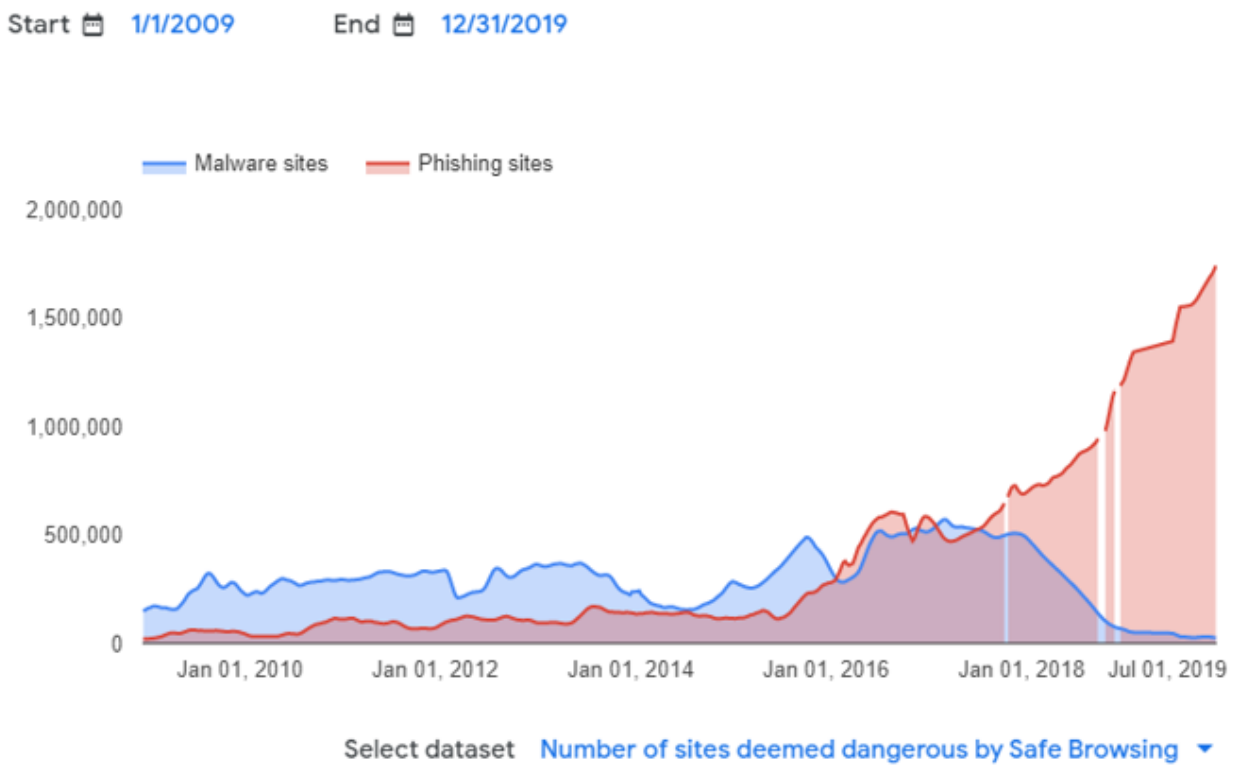

Image via Google[3]

With more than half of businesses hit by a COVID-related cyber-attack[4], security experts are expecting these numbers to grow a lot in the next three years.

While identity thefts and personal data breaches are a major concern for everyone, as a business you have an even bigger responsibility: you are responsible for your own data, that of your employees, and that of your customers and stakeholders.

One of the most famous data breaches was disclosed this year but happened back in 2018. The Marriott data breach exposed more than 500 million guest records! While the company remained vague about the causes of the attack, what we know so far is that the data breach was spotted by a security tool that flagged an unusual database query[5].

---

[3] https://transparencyreport.google.com/safe-browsing/overview?hl=en&unsafe=dataset:1;series:malware,phishing;start:1230768000000;end:1577836799999&lu=warnings_displayed&malware=start:1230768000000;series:attack,compromised;end:1577836799999&warnings_displayed=dataset:users;start:1230768000000;end:1577836799999, retrieved September 2020

[4] https://www.infosecurity-magazine.com/news/businesses-covid-attack/, retrieved September 2020

[5] https://www.csoonline.com/article/3441220/marriott-data-breach-faq-how-did-it-happen-and-what-was-the-impact.html, retrieved September 2020

Which brings us to our security monitoring and testing issue. In 2020 and beyond, companies have two choices: hire a security agency to keep them safe through vulnerability scanning and penetration testing or hire a security agency to clean up the mess left behind by an attack that could have easily been prevented.

Of course, the latter is far more expensive. More and more companies understand the importance of prevention when it comes to their online and network health – just like human health.

Who is responsible when an attack hits a company? A lot of people say it's the CEO[6]. If you've been watching the security news lately, you'll see that it's always the CEO under fire when a data breach happens. It may not be directly their fault, but CEOs are expected to spearhead prevention initiatives.

The most popular of these initiatives (due to their results) are penetration testing and vulnerability scanning,

Think of them as the MRIs and CAT scans of the virtual world. They can save your business (life)!

[6] https://metro.co.uk/2020/06/08/who-responsible-when-cyber-attack-hits-company-people-say-ceo-12820037/, retrieved September 2020

What Is Vulnerability Scanning?

Also known as “vulnerability assessment”, vulnerability scanning is a process that uses automated tools to scan networks, systems, or applications for systematic vulnerabilities or loopholes.

Typically, scan tools rank the vulnerabilities discovered based on their severity: Critical, High, Medium, Low, and Informational. Critical, High, and Medium vulnerabilities should be addressed as soon as possible – within 30 days or less. They indicate that a system can be exploited at any time and that the exploitation can be done relatively easily.

Low and Informational vulnerabilities should also be addressed, ideally before their severity increases and they are upgraded to a higher-risk category.

Vulnerability Scanning Methodology

During a vulnerability scan, the tools will identify all the systems within a company that are connected to a network and do an inventory of them. This includes, but is not limited to: desktop computers, mobile phones, tablets and other mobile devices, laptops, servers, switches, routers, printers, containers, and firewalls.

For each device or system identified, the vulnerability scanner will also attempt to identify its operating system, as well as any other software installed on it. More importantly, the scanner also looks for open ports and user accounts – the usual gateways for cyber-attacks.

After the inventory is completed, the scanner looks in certain databases for known vulnerabilities associated with the devices found or with the software that runs on them. It will also try to login to certain systems to see how they react.

The final result of a vulnerability scan is a list of all the systems and devices along with all the vulnerabilities discovered for each of them, ranked as mentioned above.

Internal vs. External Vulnerability Scans

There are two major types of vulnerability scans: one that is performed from inside the company’s network and another performed from outside of it.

The purpose of the internal vulnerability scan is to replicate the behavior a hacker might have if they manage to breach the external security perimeters.

The aim of the external vulnerability scan is to detect weaknesses in the perimeter defenses. Open ports in the firewall of the network or in that of specialized web apps are the most commonly detected vulnerabilities.

What Is Penetration Testing?

Also known as “ethical hacking” or “pentesting”, penetration testing is a technical test that goes beyond scanning for vulnerabilities. It is performed manually and designed to identify loopholes or vulnerabilities in a network, an application, or a system. Of course, pentesting should also reveal any attempts to exploit those vulnerabilities.

Penetration testing is also called “ethical hacking” because it is, in essence, a simulated cyber-attack on a company’s technologies. Its objective is to give the business decision-makers a chance to see their technologies and the security systems in place the same way a potential hacker sees them.

Better yet, pentesting shows the company the ways in which a hacker can infiltrate their systems and exploit them.

Pentesting Methodology

During a pentest, a cybersecurity specialist tried to exploit a company’s cybersecurity vulnerabilities with the aim of providing an example of what would happen if a real hacker did the same thing.

There are various methodologies and apps, like OWASP[7] to support and automate all or part of the pentest. Their value stems from the fact that there are large communities that contribute to these frameworks and methodologies, so they are always kept up to date on the most recent developments and exploit techniques. Plus, they can provide a structured approach to the test.

However, they aren’t nearly enough to conduct a comprehensive pentest, with real value to a company. Manual testing is the gold standard for any company, irrespective of size and digital assets.

This is because automation tools like Nmap can handle basic network discovery and vulnerability scan engines like Nexpose or Nessus. They can even tackle exploitation frameworks like Metasploit. But it’s manual exploitation that allows the pentester to interpret the findings from the automated tools. The pentester is also the one responsible for manually searching for the vulnerabilities that automated tools usually miss.

[7] https://owasp.org/www-project-top-ten/, retrieved September 2020

And this is the most important part of pentesting. Making sense of the findings, interpreting the vulnerabilities, and addressing them according to priority is something that can only be done manually, by a skilled pentester.

Internal vs External Pentesting

Just like for vulnerability scanning, there are two major types of penetration testing: internal and external.

An internal pentest aims to understand what a malicious attacker could achieve when they gain access to the network. This test is also very efficient for spotting internal threats, like employees who perform malicious activities intentionally or unintentionally.

An external pentest's aim is to gauge the efficiency of the perimeter security in spotting and preventing attacks. Even more, such a test is an excellent way to identify weaknesses in internet-facing assets like FTP servers or mail servers.

The Third Option: Web Application Vulnerability Assessment

A web application vulnerability assessment is, in a way, the brain child of pentesting and vulnerability scanning. The process refers to the scanning of a single website or a single web application.

Unlike vulnerability scanning, it is not 100% automated. It “burrows” the exploitation attempts from pentesting to offer you a more comprehensive overview of your security issues.

Bottom line: web app assessment is more complex than vulnerability scanning but less so than pentesting and it is the ideal compromise solution when you don’t need a complete pentest or you don’t have the budget for it.

Do You Need Both Penetration Testing and Vulnerability Scanning?

As seen above, both solutions are critical for your cybersecurity but in different manners. A vulnerability scan will only discover known vulnerabilities and not attempt to exploit them. It just confirms the existence of vulnerabilities in the system.

A pentest, on the other hand, will attempt to exploit vulnerabilities and see how your defenses hold up.

There are certain organizations regulated by PCI DSS, HIPAA, GLBA/FFIEC, and U.S. Federal Security or the corresponding institutions in non-US countries that are required to perform quarterly vulnerability scans and annual pentests.

Can you forego them if you're not required to perform either?

Yes, if there is no law or regulation forcing you to perform them, you can skip them. However, keep in mind that the average cost of a data breach is $3.9 million[8] and that of an average malware attack on a company is $2.6 million[9].

Can you afford to lose that much money?

If not, then you should definitely consider both vulnerability scans and pentesting.

According to industry standards, vulnerability scans should be performed quarterly or monthly for high-risk or mission-critical assets. Pentests should be performed annually or bi-annually depending on how at-risk your assets are.

It's very important to keep in mind that these recommendations are for companies that have a moderate amount of client records. If, for instance, you are an eCommerce business or a classifieds site like Craigslist, both vulnerability scanning and pentesting should be performed **much more frequently.**

The same goes for whenever you introduce a new service, a new app, or a new piece of software into your network. A pentest before and after the addition is crucial.

More importantly, remember that both these solutions offer a "snapshot" of your systems' health at a certain point in time. You should definitely patch any flaws identified and re-test as soon as the patch is

[8] https://www.ibm.com/security/data-breach, retrieved September 2020
[9] https://www.accenture.com/us-en/insights/security/cost-cybercrime-study, retrieved September 2020

up. And you should keep testing regularly. A one-and-done approach is definitely not enough in a constantly evolving technological landscape.

Let's take a closer look at why pentesting and vulnerability scanning need to work together, not separately by identifying their respective strong and weak points:

Vulnerability Scanning	Penetration Testing
Easy to perform, offers a basic identification of security flaws on systems, devices, and apps.	Harder to perform, involves manual testing.
Identifies well-known vulnerabilities that are already present in various databases	Identifies even new vulnerabilities that haven't been exploited by hackers massively
Does not try to exploit the vulnerabilities it identifies	Tries to exploit vulnerabilities to verify the security of your systems
Provides faster results	Takes more time
Usually can't reveal if your systems have already been compromised	Can reveal if your systems have already been compromised
Offers an inventory of the vulnerabilities found	Offers a human-assisted, business-centric interpretation of each vulnerability + recommendations.
Cannot guarantee your systems will be safe indefinitely	Cannot guarantee your systems will be safe indefinitely

Thus, the answer is always YES, you should perform both vulnerability scans and penetration testing regularly. Just like a doctor's checkup, you will sleep better knowing that everything is in perfect working condition.

More importantly, just like a "human" doctor would tell you, regular scans can't replace best practices. No matter how often you pentest and scan for vulnerabilities, you still have to uphold security measures and re-evaluate them as often as possible.

The Bluedog Security Monitoring Proprietary Solution

There's a famous saying in the cybersecurity industry: *pentesting can tell you if you're insecure but it can't tell you if you are secure.*

At Bluedog Security Monitoring we know every business is unique, with unique needs. So we take a tailor-made approach to the security of each of our clients.

We also know that automated tools aren't enough. They can identify certain types of vulnerabilities, like cross-site scripting, SQL injections, or misconfigurations like incorrectly implemented TLS.

However, they aren't so great at spotting complex vulnerabilities like authentication bypasses or flaws in business logic. They also contain a large number of false positives. This is why human intervention is a must.

Our proprietary solution is **business-centered**. This means that our ultimate goal is to keep your business assets safe. Governed and controlled by skilled experts with dozens of years of experience, our holistic approach to vulnerability scanning and pentesting is the closest thing you can find to being 100% secure.

Our process is the result of decades of cumulated experience:

1. **Scoping**

Our experts work closely with you to identify all your network-facing assets and define the right assessment strategy.

2. **Intelligence gathering**

Our skilled pentesters use the latest techniques for information gathering in order to discover any information that might help them access your network. Just like a real-life attacker would.

3. **Vulnerability scanning and analysis**

Using a mix of automated tools and manual scanning, we identify the biggest security threats to your assets and come up with the best ways to exploit them.

4. **Vulnerability exploitation**

The skilled penetration testers will use all the vulnerabilities to gain access to your network. Everything is done in a perfectly safe and secure manner, with no disruption to your business processes.

5. **Reporting and recommendations**

The final report will outline every issue that we identified. But since this means nothing to you without a solution, we will also offer recommendations on issue patching and further security best practices.

We take care of security issues one by one so you can do what you do best: run your business!

About Bluedog Security Monitoring

Our goal is to provide businesses with a level of network protection typically only afforded by large corporations. We aim to bring high-quality technology, support, and service to the small to medium business, helping protect their business from cyber threats.

Our company is growing quickly, through our simple and affordable end-to-end network monitoring solution. Recently voted one of the Top 10 cybersecurity start-ups of 2019 by Enterprise Security Magazine. Whether you are a small business, or an MSP or IT services reseller or distributor, get in touch and have a chat with us.

20-22 Wenlock Road, London, N1 7GU

info@Bluedogsec.com

+44 20 8819 6254

https://www.bluedog-security.com/