

Why regular vulnerability scanning is important



Why conduct vulnerability scans?

Every year, Verizon Communications Inc, a multinational telecommunications conglomerate, publishes a report known as the Verizon Data Breach Investigations Report. The report compiles data from over 40,000 security incidents within the last 12 months experienced in a range of public and private sector organisations and uses it to analyse and provide insight into the most common threats in the current landscape

The most recent (2020) report suggests that more than 70% of attacks continue to originate with external sources rather than internal disenfranchised employees. Additionally, 43% of data breaches seen targeted vulnerabilities in web applications, resulting in confirmed data disclosure. The statistics are clear – despite increasing maturity of security controls, external web applications continue to be a lucrative route of exploit for attackers.

Companies who may have experience with penetration testing only in the security testing space can sometimes implement vulnerability scanning on a semi-regular basis, or even just as an annual test. In this article, we'll run through a number of compelling reasons why regular scanning is not just beneficial but essential to delivery on the full potential of vulnerability scanning, and how regular scanning elevates vulnerability scanning to its full potential.

How often should I run scans?

We'd argue - "As often as you can, perhaps weekly, and running partial scans every day".

If you're approaching this article from a background of having performed vulnerability scans or penetration testing perhaps every few quarters, or even just annually, this will seem patently absurd, unmanageable and unnecessary.

But it is an approach based on sound technical underpinnings related to today's modern web applications, threat landscapes, and development practices. Let's run through the various reasons why running your vulnerability scans as often as possible maximises the benefits to you, your business, and your customers.

Reasons to scan more often

Workload Management & Organisational Buy-in

You may be responsible for purchasing, managing or operating the vulnerability scanning solution, but you (or your team) are not an island. Vulnerability detection is only part of a cohesive vulnerability management life-cycle, and buy-in from other technical teams is absolutely essential if vulnerabilities detected are to be remediated in a timely fashion. The results of a vulnerability scan are only as valuable as the willingness of the IT admin to accept the results and act on them – so make it manageable.

Place yourself in the position of a development or operations team managing a service and ask yourself whether you would prefer to receive:

1. One vulnerability finding each week of the year, with a week to fix each; or
2. Fifty-two vulnerability findings on March 2nd, with one week total to fix all of them.

I would expect most people to vote overwhelmingly for Option 1. Having worked in several enterprise organisations, I have observed first-hand how providing fewer findings, more often, prevents frustration and fosters co-operation between teams. “Little and often” makes the vulnerability management process ‘Business As Usual’, rather than an extraordinary demand for resources on an irregular basis. Managers and scrum masters can factor in 5% “fix time” per week or Sprint, and vulnerability management becomes part of the status quo. Providing regular vulnerability reports from frequent scans helps everyone and can make those annual manual tests much easier when they come around.

Chasing the Attack Window

New vulnerabilities in software are published regularly as CVEs. When a new vulnerability is reported, it triggers a race against the clock between the various people involved. From an organisation’s point of view, teams need to roll-out the necessary security patches to rectify the flaw, as soon as the vendor supplies them.


However, at the same time, attackers will start developing exploits with malicious code that can take advantage of the identified weaknesses. The race is on, and the period until you patch is known as the “attack window” during which an attacker can take advantage of the vulnerability on your systems.

If you are only performing vulnerability scanning on a long interval or cycle between scans, it may be months before you are even aware that one of your systems is un-patched and vulnerable. Scanning more regular doesn’t find more vulnerabilities or present a greater burden, but it reduces the timescales between a vulnerability being exposed on your system and you becoming aware of it and patching it, tipping the scales in your favour and against the attacker.

The Continuous Delivery dream and multiple deploys per day

Systems development used to be a slow process with long development cycles. However the advent and adoption of devops and Agile practices within organisations often means that development teams are using Continuous Deployment practices and living up to the dream of minimal diffs and multiple deploys per day. This is great news for product development release, however it means that bad code can be released quicker and more frequently too.

The more Agile your development teams become, the more disconnected an “infrequent scan” approach becomes. If you release code regularly, it makes intuitive sense that you scan the application more frequently too.



"A computer lets you make more mistakes faster than any other invention with the possible exceptions of handguns and Tequila."

Mitch Ratcliffe

Content Management Systems (CMS)

We've already had a crack at developers and system administrators for introducing vulnerabilities, so we might as well have a pop at marketing and content management teams too. Content Management Systems (CMS) such as WordPress allow non-technical teams to manage web presences such as blogs. However, by design many allow the pasting of rich content and links, which are an attractive vector for attackers to seek to introduce vulnerabilities such as Stored Cross Site Scripting (XSS). CMSs can be updated multiple times per week, or even per day – so it makes sense to check these regularly.

Retests

It is important the vulnerability scanning is performed not only to detect vulnerabilities, but critically that follow-up scanning is also performed to verify and provide assurance on claimed fixes. Investigations following Equifax's well-publicised data breach of 2017 appears to suggest that Equifax were aware of the requirement to patch their systems against a known and published vulnerability, but that they failed to retest systems in order to ensure that they had been patched correctly - failure that led directly to the theft of sensitive data relating to 145 million people.

By scanning regularly, you can ensure you follow up on verification that vulnerabilities discovered in previous scans are being remediated in timescales mandated by organisational policy or in line with risk.

Trends & Metrics

Most teams tasked with vulnerability detection and management will at some point either (a) be asked by their senior management to provide some reporting on trends and metrics on vulnerability detection and remediation rates in terms of burn-down and deltas, or else (b) want to provide these metrics themselves.

The more often your vulnerability scans execute, the more granular your reporting is and the more useful they will prove. If you have one data point per year, your metric granularity won't be as good and any trend analysis requested will be much less effective.

Some common misconceptions

Many organisations feel they are protected by their firewall or other forms of external 'wrapper like' defence. The fact is that no matter what defences you have in place you will not be un-hackable (the Dark Web Specialist Dark-beam believes that more than 98% of business have already been hacked-they just aren't aware of it yet). And the landscape is changing every day making it impossible to be ahead of the game. To say that having a firewall will protect you unfortunately just isn't the case. Blue chip companies will spend millions on firewalls but still have data breaches.

It must be mentioned that conducting your ASV PCI scanning is a crucial part of your compliance, however it is an important point to highlight the difference between PCI scanning and vulnerability scanning. If you were to swap your compliance hat with your security hat for just a moment it is fair to point out that passing your ASV PCI scan may give you a false sense of security. Your PCI scan will limit your vulnerability discovery to only find the vulnerabilities within PCI standards which may lead to exploitable vulnerabilities that would not fall within the PCI remit.

Can I conduct year-round scanning in conjunction with an annual test?

Yes, of course and many organisations choose to do so. This way you are finding vulnerabilities year-round but conducting a thorough annual test to give you full confidence in those results.

How can CyberWhite help?

The bottom line is that without performing regular vulnerability scans, you do not have consistent visibility on your vulnerability landscape and are one step behind the hackers. If you would like more information on how we can help, please get in touch.

Keep in touch with CyberWhite

**Mulberry House
3 Defender Court
Sunderland
SR5 3PR**

Tel: 0191 528 3228

Email: info@cyberwhite.co.uk

Website: www.cyberwhite.co.uk

Follow CyberWhite on Social Media



facebook.com/cyberwhite



linkedin.com/company/cyberwhite-ltd



twitter.com/CyberWhiteLtd



twitter.com/CyberWhiteLtd