TRAVA

A COMPREHENSIVE GUIDE TO CYBER INSURANCE

Vulnerability Scan Types

VERSION 1

Grow your business with cyber.

Contents

We live in an increasingly interconnected digital world. Small to medium-sized businesses find themselves at the forefront of cyber threats, making cybersecurity a paramount concern.

Many small business owners assume that they are too inconspicuous to attract cybercriminal attention, however the reality is quite the opposite. As many SMBs handle sensitive customer data, financial information and proprietary business data, they become lucrative targets for malicious actors seeking to exploit vulnerabilities. 43% of cyberattacks aim at small businesses, but only 14% are prepared to defend themselves according to Accenture's Cost of Cybercrime Study[1].

Vulnerability scans play a crucial role in fortifying a company's cybersecurity posture by identifying and addressing potential problems and weaknesses in a company's digital infrastructure.

Trava integrates cyber risk assessment and mitigation into one, convenient cyber risk management platform. We check for vulnerabilities in a company's external and internal environments, predict how malicious actors might get access, and inform how to fix the critical vulnerabilities and up a company's defenses against cyber threats.

This ebook details:

- A description of each vulnerability scan type
- The benefits of performing vulnerability scans
- Recommended frequency for running the scans

Overview of Vulnerability Scan Types

EXTERNAL SCANS	**Port Scan**	Checks for publicly exposed ports on a company's network
	Certificate Scan	Reviews digital certificates used on a company's websites to validate secure communication
	Breach Scan	Scans the web for indications that a company's or its employees' accounts have been compromised in a breach in the past and whether they are accessed on the dark web
	DNS Scan	Scans domains and associated sub-domains for security misconfigurations. Domain Name System (DNS) is the system responsible for connecting domain names to IP addresses, and is essential for emails to work.
	Perimeter Scan	Identifies vulnerabilities on a company's publicly exposed hosts and IP addresses
	Web Application Surface Scan	Assesses the externally accessible components of a web application (e.g., login pages, web forms) for vulnerabilities and possible threats without needing internal access
INTERNAL SCANS	**Cloud Scan**	Analyze a company's public cloud configuration (AWS, Azure or GCP) to identify configuration issues
	MFA Scan	Identify to what extent a company has MFA (Multi-Factor Authentication) enabled throughout their organization
	Web Application Scan	Verifies that a web application, and the components used to develop it, are secure and not exposing security issues/vulnerabilities
	Agent (Endpoint) Scan	Scans remote devices to access a company's network and resources, such as laptops, desktops or servers, for security vulnerabilities
	Internal Vulnerability Scan	Similar to an agent scan. Can expose vulnerabilities on a company's endpoints
	Microsoft 365 Scan	Analyzes a company's Microsoft 365 environment to look for configuration issues that could lead to security vulnerabilities
	WordPress Scan	Analyzes a company's WordPress environments to identify vulnerabilities in the core platform, custom code, and plugins

External Infrastructure and Internal Network Vulnerability Scans provide insights into your cyber security risks and predict how malicious actors might get into your system with the goal to help you build better defenses.

What are these types of scans?

- **External Infrastructure Vulnerability Scans** are performed from outside of a company's network. They target the company's external-facing systems, such as web servers, domain name systems (DNS) and firewalls. These scans simulate attacks from outside the organization and mimic the perspective of potential external hackers. The primary purpose is to identify vulnerabilities, such as open ports, misconfigurations in externally facing servers or unpatched software, that an external attacker could exploit.
- **Internal Network Vulnerability Scans** are performed from a location that has access to a company's internal company network. They focus on evaluating the security of a company's internal network, including its servers, workstations, databases and other devices. Their primary purpose is to identify vulnerabilities that an attacker who has gained internal access might exploit. Internal scans show vulnerabilities at a greater depth as they can "see" more of your company's network compared to external scans.

What are the key insights from external and internal scans?

- External Infrastructure Vulnerability Scans ("External Scans")
    - Weaknesses in your systems that could help avoid a potential incident.
    - Pressing security issues.
    - Changes like services or server setup and whether these changes present any new threats to the organization.
    - Enhancements to the total coverage and surface area of the scanned surface
        - ***Subdomain Enumeration*** - an enhancement that allows our scans to identify all subdomains associated with the provided apex domain (website)
        - ***IP Attribution*** - the ability to determine if an IP address belongs to you or a 3rd party provider for the purposes of remediating vulnerabilities.
    - Internal Network Vulnerability Scans ("Internal Scans")
    - Known vulnerabilities that could compromise your network.
    - Patch trends and missing patches that need attention.
    - Verification that all issues are patched properly and are up to date.

How frequently should you run these scans?
It is critical that you run scans on a continuous basis as new vulnerabilities are constantly being discovered. The frequency depends on several factors, including the company's size, regulatory requirements and the dynamic nature of its IT environment. As a rule of thumb, we recommend that you set up a monthly scanning frequency for external scans, and a weekly scanning frequency for internal scans.

We also recommend that you run scans after significant changes, such as website updates, server configurations, the deployment of new services and after security incidents.

> **Organizations that scan with a steady cadence remediate flaws on average 15.5 days faster.[2]**

External Infrastructure Vulnerability Scans

Port Scans

What is a network port? Network ports are uniquely assigned numbers that serve as communication end-points between a client (i.e. a web browser) and a server (i.e. a website). Trava checks your external surface for open network ports and classifies them into 4 categories:

- Normal ports: standard ports found on web servers. Example: TCP 443.
- Risky ports: ports that are commonly associated with known vulnerable services. These ports should never be open to the Internet unless absolutely necessary. Example: TCP 21.
- Administrative ports: ports that are commonly associated with remote administration services, such as SSH or RDP. These ports should not be open to the Internet unless there is a legitimate business reason. Example: TCP 3389.
- Other ports: ports that Trava identifies as non-standard and should not be open to the Internet. Appearance of these ports could mean that your network gateway or firewall is misconfigured.

What are the key insights from a port scan?

- Discover all open ports on publicly-expose hosts and IP addresses
- Identify rouge ports and devices on your external surface
- Ensure that only authorized ports are available on your external surface

Certificate Scans

What is a digital certificate? A digital certificate is a digital authentication tool that serves two primary functions: A certificate authenticates the identity of the server, and it binds a key pair (public and private) to that server. Certificates are used to provide secure communication to your websites.

- What are the key insights from a certificate scan?
- Discover all the certificates installed across various endpoints in your network and detect known vulnerabilities exposed by your certificates.
- Record certificate location, health, type, days to expiration, and position in the chain of trust.
- Ensure that your certificates are running the most current version.

> **Certificates are used to provide secure communication to your websites.**

Breach Scans

What is a data breach? A data breach is a successful cyber attack in which malicious actors were able to gain access to and steal protected data. Malicious actors can target organizations of any size.

- The common types of data exposed in public breaches include personal information, health information, financial information, intellectual properties, usernames, passwords, and many more.
- Breach scans identify if any of your organization accounts have been compromised through a breach.

What are the key insights from breach scans?

- Find out if any of your company's or employees' accounts have been compromised and are sold or accessed on the dark web.
- Identify other characteristics of the breach that may have a negative impact (date of breach, compromised data types, whether it contains sensitive information)

> **Catching compromised accounts early is critical in preventing unauthorized access to user accounts.**

DNS Scans

What is a DNS? The Domain Name System (DNS) is a system responsible for connecting domain names (i.e. www.travasecurity.com) to IP addresses (i.e. 1.2.3.4) and allowing users on the Internet to browse web sites and resources in an easier way rather than relying on hard-to-remember numbers.

DNS is essential for email to work, as mail servers need to know where to send emails to. Additionally, DNS has features that can be used to prevent emails from being spoofed and protect organizations from phishing attacks.

What are the key insights gained from running DNS scans?

- Misconfigured or missing SPF (Sender Policy Framework) record in a domain's DNS that could lead to emails being spoofed.
- Misconfigured or missing DMARC (Domain-based Message Authentication, Reporting & Conformance) record in a domain's DNS that could lead to emails being spoofed and other deliverability issues.

> **Malicious actors target organizations with missing SPF and DMARC records to use their domains to launch phishing attacks against other entities, most often their customers.**

Perimeter Scans

What is a Perimeter scan? A Perimeter scan, or External IP Address scan, assesses the external attack surface of a company for publicly exposed hosts and IP addresses. Additionally, a Perimeter scan performs further checks on the discovered hosts and IP addresses to identify vulnerabilities that could be exploited by malicious actors.

What are the key insights gained from a Perimeter scan?

- Discover hosts and IP addresses on your external attack surface that are exposed to the Internet
- Identify vulnerabilities on the discovered hosts and IP addresses

Web Application Surface Scans

What is a Web Application Surface scan? This scan assesses the externally accessible components of a web application for vulnerabilities and possible threats without needing internal access. It scrutinizes elements like login pages, web forms, and other user interfaces exposed to all users, authenticated or not.

What are the key insights gained from Web App Surface scan?

- Verification of proper HTTP security header configuration to prevent specific attacks.
- Identification of outdated or vulnerable web server software and third-party components.
- Discovery of potential malicious script injection points that might lead to unauthorized access or data breaches.
- Recognition of scenarios where malicious SQL queries could compromise database security and data integrity.

> **Consistent Web App Surface scans are crucial to promptly identify and rectify vulnerabilities, protecting against data breaches and potential external threats from malicious actors.**

Internal Network Vulnerability Scans

Cloud Scans

What is a Public Cloud? The public cloud is an IT model where on-demand computing services and infrastructure are managed by a third-party provider and shared with multiple organizations using the public internet without buying and maintaining computer hardware. The 3 largest public cloud providers are Amazon Web Services (AWS), Microsoft Azure and Google Cloud Platform (GCP).

With the rapid shift to the cloud that many companies are making, security is often overlooked or misunderstood. A cloud scan analyzes your public cloud configuration to make sure it is set up correctly. It will look for any configuration settings that could expose your data or make you vulnerable to malicious actors. Beyond data exfiltration, malicious actors can also use your cloud environment to launch a variety of criminal activities.

What are the key insights from Cloud scans?

- Verification that your cloud environments are configured in a secure way, or if there are security vulnerabilities in your configurations.
- Ability to identify any of your cloud resources that may be inadvertently exposed to the world.

> **Don’t overlook cloud security. Malicious actors can use your cloud environment to launch a variety of criminal activities.**

MFA Scans

What is MFA? MFA, or Multi-Factor Authentication, refers to the process of verifying a user’s identity by requiring multiple forms of authentication before granting access. This usually means something the user knows (like a password), something the user has (like a smart card or a mobile device), and something the user has (like a fingerprint or facial recognition).

What are the key insights gained from MFA scan?

- Identification of accounts that have not enabled MFA.
- Identification of privileged accounts that do not have MFA enabled as they pose a greater security risk.
- Verification of the strength and efficacy of the authentication methods in use.
- Verification of MFA enforcement at an organizational level.

MFA is a crucial security measure in today’s digital age. Especially with the prevalence of successful attacks using the social engineering vector. The use and enforcement of MFA ensures protection even if a user is compromised.

> **Regular MFA scans are essential for preventing unauthorized access and ensuring all users are protected by multi-factor authentication.**

Web Application Scans

What is a Web Application? A web application provides some kind of web-based service to users or customers. This could include e-commerce sites or other web-based or SaaS (software-as-a-service) applications. If your company hosts its own web application, this can greatly increase your exposure to cyber attacks.

A web application scan will crawl through all of the pages on your web app and look for security vulnerabilities. These vulnerabilities can be the result of poor coding practices or issues with commercial or open-source libraries that are used to develop your application. These vulnerabilities can allow malicious actors to breach your system and access sensitive data or services.

What is the key insight from web application scans?

- Verification that your web application (and the components used to develop it) are secure and not exposing vulnerabilities.
- Web application scanning is an important part of a secure Software Development Life Cycle (SDLC).

> **Web applications are generally exposed to the internet, so vulnerabilities can allow malicious actors to access sensitive data.**

Agent (Endpoint) Scans

What is an Agent or Endpoint? An agent, also called endpoint, is a device used to access your network and other resources, usually a laptop, desktop, or server. In addition to often containing sensitive information and being critical to your businesses operation, endpoints are frequent targets of cyber attacks.

- An agent scan searches an endpoint for any known security vulnerabilities or configuration issues. An endpoint scan is performed by installing a small program on the device that scans for known issues on a periodic basis. Endpoint scans can be run on any Windows, Mac, or Linux computer.

What are the key insights from Agent scans?

- Find out if any of your users have security issues on their computers.
- Expose vulnerabilities in work-from-home environments where devices are not connected to your company's network.
- This is the most effective defense against breaches that could occur due to user errors or careless behavior on local computers. It allows you to keep up with multiple software programs updated at different intervals.

> **Agent scans are critical for exposing vulnerabilities in work-from-home environments where devices are not connected to your company's network.**

Internal Vulnerability Scans

What is an Internal Vulnerability scan? An internal vulnerability scan is similar to an agent scan. However, it's conducted from a centralized appliance positioned inside your internal network instead of individual agents installed on each endpoint.

An internal vulnerability scan is generally faster to deploy, compared to agent scan, because you only need to set up one appliance instead of having to install a scanning agent on all of your devices. An internal vulnerability scan is also advantageous over agent scan for purpose-built devices running on specialized operating systems (for example, network devices such as routers and industrial control devices such as meters, etc.), where scanning agents cannot be installed.

What are the key insights from internal vulnerability scans?

- Similarly to agents scan, an internal vulnerability scan can expose vulnerabilities on your endpoints
- Internal vulnerability scans also expose vulnerabilities on network devices and other specialized-OS devices

Microsoft 365 Scans

What is Microsoft 365? Microsoft 365, formerly Office 365, is a cloud-based SaaS (software-as-a-service) subscription plan that allows use of the Microsoft Office software suite over the life of the subscription for business environments. This scan is specific to Microsoft 365 users.

What are the key insights for Microsoft 365 users from running Microsoft 365 scans?

- Validation of your security patch deployment on applicable system components.
- Detection of known vulnerabilities and security misconfigurations.

> **Cloud environments are a common target for malicious actors to launch a variety of criminal activities.**

WordPress Scans

What is WordPress? WordPress is a free, open-source website creation platform. On a more technical level, WordPress is a content management system (CMS) written in PHP that uses a MySQL database. Known for its ease of use, WordPress is a popular website builder for small and medium-sized businesses. This scan is specific to WordPress users.

What are the key insights for WordPress users from running WordPress scans?

- WordPress scans test for vulnerabilities of a WordPress installation. Checks include WordPress plugins, theme templates, application security, hosting environment, and the web server.
- This scan identifies security holes in your website that can be exploited by malicious actors.
- WordPress sites are regularly updated, and with each update comes potential for a new set of security holes. The number of new vulnerabilities has been increasing steadily since WPScan first started tracking in 2014. In 2022, 1,770 new vulnerabilities were disclosed3.

> **Regular updates can help find changes that you, WordPress, or your website hosting service have made that can leave your website vulnerable to security threats.**

Conclusion

No single scan will fully expose your vulnerabilities, nor will single instances or infrequent scans. In order to protect your company’s and your clients’ data, we recommend that you run the scans on a regular cadence. Prioritize the scans according to the most severe risk level, and take immediate action to resolve vulnerabilities. This is a critical component in a comprehensive cyber risk management strategy.

Trava exists to protect small and medium-sized businesses from the potential damage of cyber threats. By integrating risk assessment and mitigation into one, convenient cyber risk management platform, Trava enables business owners and IT professionals to operate secure, productive businesses without fear of interruption or loss caused by cyber incidents.

solutions for agencies and carriers

Grow your business with cyber.

We get you selling cyber insurance with confidence and securing your clients with actionable data.

TRAVA

travasecurity.com