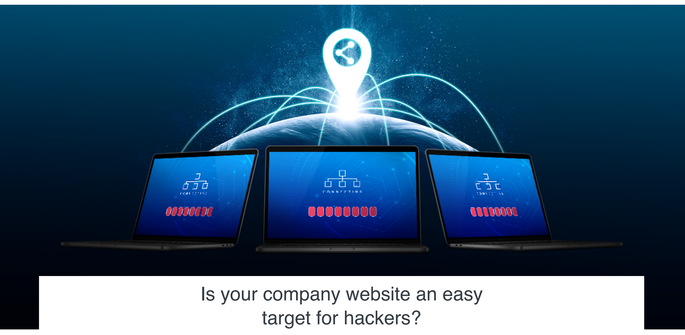

Is your company website an easy target for hackers?

Your company's website is like the store window of a brick-and-mortar shop. Its design is crucial for your customers and partners, and you need to keep it safe. Yet globally, around 30,000 websites are hacked daily. Here's a guide to common types of attacks.

1) DoS and DDoS attack

A denial of service (DoS) is a form of cyberattack in which the perpetrators seek to disrupt or crash a website, network, or other online service **by overloading it with a high volume of fake or junk requests.** Cybercriminals typically use networks of distributed, compromised devices to disrupt systems by targeting one or more of the components necessary to establish a connection to a network resource, making the DoS attack a DDoS – as in distributed denial of service – attack. The most common types are:

- **Volumetric attack** – The oldest type of (D)DoS attack, which employs large volumes of traffic to fill bandwidth capacity between the victim's network and the internet or capacity within the victim's network. The largest volumetric attacks are (currently) measured in terabits per second (Tbps) – the equivalent of roughly 9,000 typical internet connections.

- **Protocol attack** – This type of attack misuses the design of the underlying communication protocol to exhaust the resources of the targeted system. For example, during a SYN flood, the attacker can overwhelm all available ports on a targeted server machine by repeatedly sending initial connection request (SYN) packets, causing the targeted device to respond to legitimate traffic sluggishly or not at all.

- **Application layer attack** – This type of attack targets public-facing applications via a high volume of spoofed or bogus traffic. An example is an HTTP flood attack that floods a specific web server with otherwise legitimate HTTP GET and HTTP POST requests (in tens of millions per second). Even though the server might have enough bandwidth, it is overwhelmed by bogus requests, limiting the ability to process their legitimate counterparts. If the attack continues long enough, the server will run out of processing capacity.

Denial of service (DoS) vs. Distributed denial of service (DDoS)

The difference is in the number of attacking machines. A DoS attack typically utilizes a script or tool, originates from a single device, and targets one specific server or endpoint. In contrast, DDoS attacks are executed by an extensive network of attacker-controlled compromised devices – also known as a botnet – and can be used to overload selected devices, applications, websites, services or even victims' whole networks.

Source: ESET

2) Cross-site scripting attack

Cross-site scripting (XSS) allows attackers to compromise the interactions between users and a vulnerable application. How? According to OWASP, cross-site scripting attacks "are a type of injection, in which **malicious scripts are injected into otherwise benign and trusted websites**." When the malicious code executes inside the victim's browser, the attackers can fully compromise the victim's interaction with the application.

The vulnerability allows attackers to circumvent the same-origin policy designed to differentiate websites from each other. The cybercriminals can impersonate the victims and carry out any actions that the users can perform and, therefore, access any of the users' data. If the victims have privileged access within the application, then the attackers might gain full control over all the application's functionality and data.

3) Injection attacks

- **Code injection** – exploitation of a computer error caused by the processing of invalid data. Attackers usually introduce malicious code into a vulnerable computer program and change the execution flow. Successful code insertion can be disastrous – it enables the spread of malware, and particularly the spread of computer worms in company networks. Attackers can then compromise database integrity and privacy properties, security, and even data correctness.

- **SQL injection (SQLi) attack** – Attackers will try to manipulate the SQL query used in the web application and gain direct access to your data. This is typically done through a web form input field, comment fields, or other places where users interact with your website.

- **Command attack** – Web applications need to call a system command on the web server that runs them from time to time. If user input is not validated and restricted, attackers can insert a command into the system while using the user-level access. The command injection might compromise an application and its data or the entire system with connected servers and infrastructure.

4) Zero-day attack

According to MIT Technology Review, 2021 broke the record for zero-day hacking attacks. A zero-day exploit – **a way to launch a cyberattack via a previously unknown vulnerability** – is just about the most valuable thing a hacker can possess; these exploits can carry price tags north of $1 million on the open market.

A zero-day attack usually starts with a completely unknown security vulnerability in the computer OS or application. A similar, slightly less dangerous case is the n-day: **a vulnerability in the OS or applications for which either the patch has not been released** or the application developers were unaware of or did not have sufficient time to address. In either case, the exploitation happens before everyone (who needs to know) is aware of the vulnerability or before a patch is publicly available. That's why users who trust the source of software patches often never know about the existence of exploits.

Learn more about the recently discovered Log4Shell vulnerability and how to detect it. According to some sources, the results of this flaw could affect hundreds of millions of devices for many years to come.

5) MitM attack

The best-known example of a man-in-the-middle (MitM) attack is active eavesdropping; in this case an **attacker intercepts traffic between two or more victims**. This allows the attacker not only to see the conversation but to alter it with neither victim being aware that the attacker is manipulating the interaction.

This is a particular result of the ability to subvert the authentication protocol. The National Institute of Standards and Technology writes that in the context of authentication, the attacker is usually positioned between claimant and verifier, between registrant and cloud service provider (CSP) during enrollment, or between subscriber and CSP during authenticator binding.

6) Brute-force attack

A brute-force attack uses trial and error to crack passwords, login credentials, or encryption keys to gain unauthorized access to individual accounts and organizations' systems and networks. Often, botnets are used since they're faster due to the high volume of devices making the guess in parallel. Botnets are also harder to block since they include a wide range of IPs.

Motivations for such an attack include **spreading malware, exploiting company ads or activity data, and damaging corporate reputation**. "Many popular websites and services today will block access after 5 to 10 wrong guesses from a specific IP address. A botnet has a better chance to guess the right thing using a range of IPs in a specific geographic region," explains **ESET expert Ondřej Kubovič**.

The hacker tries multiple usernames and passwords, often using a computer to test a wide range of combinations until they find the correct login information. The attacker uses software or at least some code or script that can guess thousands of passwords within a few seconds or minutes.