ROSTYSLAV SAVCHUK *Cybersecurity engineer, DATAMI*
https://datami.us/

Datami is a team of highly qualified and experienced WhiteHat hackers. The company has been operating on the market for over 7 years, and it currently has offices in Ukraine, Estonia, and the United States. Datami provides full-cycle cybersecurity services - from diagnosis and treatment to complex penetration tests, IT audits, and other services.

TIP 1. HUMAN FACTOR

Technical protection alone does not ensure that a resource cannot be hacked. Because the most vulnerable link is the human factor. The organisation should train staff members, introduce them to security rules, conduct regular phishing training, and develop written security policies. In most situations, training personnel is a viable way to counter modern threats.

TIP 2. PROTECTION SYSTEMS

You can minimise the risk, but there's no such thing as a fully protected resource, even if you connect a protection (SIEM, IDS/IPS, WAF), or create your own. All software and protection systems, WAF lists, and all system components should always be running the latest stable versions. Be on the lookout for new relevant vulnerabilities, and take precautionary measures to ensure that they are not exploited.

TIP 3. LOGGING

Logs help you detect and respond to attacks faster if you analyse them, and if you have already been hacked, they can help you recover faster. To avoid losing data, logs must constantly be backed up to a third-party server. Make sure that log entries are written correctly, because, at a critical moment, it may turn out that no logs were kept, and there are no records of events.

TIP 4. PENETRATION TESTING

Conduct pentests of the resource on a regular basis (at least once a year). Cyber security specialists simulate attacks to identify weak spots in security postures during a penetration test.

As a result of the pentest, a findings report will be issued and you will be able to patch the security holes, assure customers that their data is protected, and ensure compliance.

TIP 5. COST OF SECURITY SOLUTIONS

Implementing and maintaining cyber security solutions shouldn't exceed the resource cost.

There is no point in setting up a firewall for thousands of dollars on a landing site, the restoration of which will cost hundreds of dollars. To choose the protection system you must take into consideration the industry you are in, IT budget, analyse potential risks and the cost of a potential breach.

TIP 6. WAF (WEB APPLICATION FIREWALL)

A WAF is a special tool that filters and monitors traffic between a web application and the Internet. This tool does not provide 100% protection against hacking, as attackers come up with various ways to bypass such things. Involve a specialist to set up WAF correctly so that there are no false positives and false negatives.

TIP 7. DDOS (DISTRIBUTED DENIAL OF SERVICE) PROTECTION

Moments to go down, hours to recover. DDoS attacks are still one of the most popular; the aim is to make your website and servers unavailable to legitimate users.

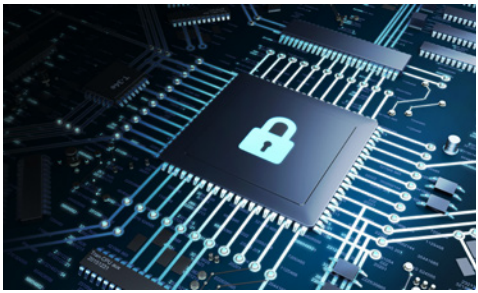
The market is full of solutions to protect against such attacks, so it is important to analyse your requirements and select the right option for you.

TIP 8. SECURITY BY DESIGN

If you are planning to create a website, start thinking about its security right away.

This development principle seeks to minimise design flaws and make the system trustworthy.

For such projects, it's recommended to hire a security consultant, who will lead the project and constantly check its security and consult developers on writing safe functions right away.



TIP 9. INTRUSION PREVENTION SYSTEM

Only an active protection system, such as a firewall or intrusion prevention system, is not sufficient to guarantee maximum security of a resource. The resource should also be protected by its functionality.

For example, exploitation of SQL Injection on the Login page can be prevented with a WAF, but it is better to rewrite this function and make it impenetrable (using data validation), and additionally connect WAF.

TIP 10. NEVER TRUST THE USER

Input is always bad unless proven otherwise. Validate the input before using it, because people will try to make your application fail by adjusting the input. Often vulnerabilities are exploited due to the lack of validation, thus an attacker can enter malicious payloads and break into the system. Always enable white list filtering, block all but a few necessary characters.