Preventing zero-day attacks: 5 more tips for greater security

Digital Security
Progress. Protected.

Preventing zero-day attacks: 5 more tips for greater security

After you've taken basic steps to reduce your risk of zero days—for example, reviewing your access policies and implementing regular system updates—here are five more ways to strengthen your protection.

1. Automate as much as possible

In the best-case scenario, your emergency plan can be largely automated. All processes that can be executed autonomously relieve the burden on the administrator. These actions can include, for example, the automatic encapsulation of affected endpoints, where the desktop firewalls cut off all connections except those of remote administration.

2. Pay attention to logging and documentation

It is also important that all actions, whether automatic or manual, include the comprehensive logging and documentation of manual steps. This is the only way to track the infection process retrospectively and adapt the contingency plan accordingly—as far as the closing of possible security gaps, but also human behavior, is concerned.

3. Make regular backups

Whatever has caused the security incident, the ability of companies to recover lost, business-critical data as quickly as possible is crucial. This starts with regular backups. Having a system that automatically backs up your data is a smart choice, as this ensures the task is completed regularly. This also ensures that your employees don't forget to back up their data. Backup copies should be made on at least two external media, and an encrypted version of a backup in the cloud storage should also be considered. Again, backup and recovery systems must be tested regularly.

4. Use an endpoint detection and response (EDR) tool

An EDR tool allows the constant and comprehensive monitoring of all endpoint activities. Suspicious processes can then be analyzed in detail, and IT managers can respond to threats at an early stage. Companies enhance their security measures many times over with the use of EDR technology, especially in the event of zero-day attacks, ransomware, targeted attacks (advanced persistent threats), or violations of internal company policies.

5. Regularly review your contingency plan

Just like fire drills, IT contingency plans must be tested regularly. According to NIST, "Information system contingency planning refers to a coordinated strategy involving plans, procedures, and technical measures that enable the recovery of information systems, operations, and data after a disruption."

Two key takeaways: First, you need to develop an effective plan and make sure every employee is familiar with it. For example, how do they report a security incident? Who is in charge of the response?

Secondly, you must review and test your plan. This allows you to find any weaknesses or flaws in your system and fix them—before a crisis comes along.

80% of successful data breaches are the result of zero-day exploits—*Ponemon Institute, 2020*

Need help protecting against zero-day threats?

CONTACT ESET

Learn more about ESET PROTECT Advanced:

ESET PROTECT ADVANCED