

Zero-Day Attacks: What They Are and How to Protect Your Business

Secure your business and your customers from cyber attacks with professional prevention, regular maintenance, and rapid response.



Table of Contents


1. What Is a Zero-Day Attack?
2. Why Should You and Your Organization Care About These Types of Attacks?
3. How Often Do Zero-Day Attacks Happen to Small Businesses?
4. What Is the Potential Impact of a Zero-Day Attack?
5. What Is the Typical Impact of a Zero-Day Attack With Proper Response?
- 6-7. Key Steps for Prevention and Response
8. How SMBs Can Maintain Zero-Day Attack Prevention
- 9-10. Benefits of Outsourcing Your Technology Protection and Security

A green warning icon consisting of a triangle with an exclamation mark inside, positioned above a stylized laptop screen.

What Is a Zero-Day Attack?

Zero-day vulnerability is a security vulnerability in a company's IT systems that the company isn't aware of until it is uncovered by cyber criminals. Typically, there is no security patch ready or available to deploy to protect the target.

Zero-day attack is when attackers exploit the zero-day vulnerability, causing damage to or stealing data from the organizations' systems and/or users. Attackers can write malicious code to exploit the vulnerability; they can also utilize phishing techniques to launch their attack.



Why Should You and Your Organization Care About These Types of Attacks?

Out of the myriad cyber attack models, zero-day attacks are especially concerning because if one hits your business it means cyber attackers know something about your systems that you don't. "Zero" often refers to the amount of time you have to patch your vulnerability – zero days – before it is exploited.

An attack like this can cost an organization:

- ✓ Millions of dollars
- ✓ Reputational damage
- ✓ Legal trouble
- ✓ And more.

How Often Do Zero-Day Attacks Happen to Small Businesses?

66

zero-day vulnerabilities have been exploited in 2021¹ - almost doubling the total exploited in 2020, and more than in any other year on record.


43%

of cyber attacks target small businesses.²

Small businesses are especially vulnerable to zero-day attacks because of their typical lack of in-house security expertise which leads to undetected vulnerabilities.

1. <https://www.technologyreview.com/2021/09/23/1036140/2021-record-zero-day-hacks-reasons/>

2. <https://purplesec.us/resources/cyber-security-statistics/>



What Is the Potential Impact of a Zero-Day Attack?

- ✓ **Data theft:** Attackers can exploit a zero-day vulnerability to steal data from your organization and sell it on the dark web, extort customers, or steal money from you.
- ✓ **Unauthorized takeover:** Zero-day exploits can take control of your organization's production machines, technology systems, and communication systems.
- ✓ **Financial Loss:** If any critical system goes offline during the attack, you'll experience costly downtime.
- ✓ **Reputational Damage:** If the attack goes public (which it most likely will), your reputation will take a hit because of poor cyber security practices that did not protect your customers, assets, and systems.

What Is the Typical Impact of a Zero-Day Attack With Proper Response?

A quick response and a strong disaster recovery strategy is key to mitigate the untold damage a zero-day attack can do.

- ✓ A combination of cloud-based and on-site storage helps you back up critical data in a secure location.
- ✓ Limiting access or temporarily shutting down access to your website and/or applications while a patch is developed can limit the damage.
- ✓ Applying a patch immediately will get your organization back on track.






Key Steps for Prevention and Response

Maintain updated systems: Keep your applications up-to-date. Vendors include security patches in their software updates to cover identified vulnerabilities.

Constant monitoring: Being aware of your systems and what's happening in them is always the first step. Use tools like firewalls or antivirus software to minimize your risk.

Identify the scope of attack: Find all of the information available about what was affected by the attack and the level of impact.



Key Steps for Prevention and Response, Part 2

Find mitigation opportunities and act: Shut down access and systems if possible while your team works to come up with a patch for the vulnerability. This will lessen the negative impact.

Close initial point of entry: Patch the vulnerability as fast as possible, so other cyber criminals won't be able to attack you the same way.

Recover back to a prior state: If you have back-ups of your data or systems, restore them after the patch is implemented.

How SMBs Can Maintain Zero-Day Attack Prevention

For a small- or medium-sized business, fielding an entire cyber security team – or even one specialized employee – can sound impossible. Many small organizations outsource their IT security services – you can too. Finding a technology and cyber security partner who can dedicate their time to your security efforts will free up your time to go run your business.



Benefits of Outsourcing Your Technology Protection and Security

- ✓ Let Your Limited Staff Rely on a Network of Dedicated Professionals

Get full-time security help for zero-day attacks without needing to add more people to your payroll.

- ✓ Leverage Proven and Professional Experience

Use specialists with deep knowledge and experience in security vulnerabilities in a variety of contexts and environments.



Benefits of Outsourcing Your Technology Protection and Security, Part 2

- ✓ Maximize Your Limited Budget by Paying Only for What Will Be Most Impactful

If it doesn't make sense to set up a security program, you can bring in a vendor and pay for highly effective protection and security work.

- ✓ Buy Yourself the Time You Need

Just because your people don't have the time, doesn't mean you can't invest in time from an outsourced specialist.

Access One is your trusted technology partner. We focus on your security, prevention, and response, so you can run your business.

Contact Access One to learn how we can help you protect against zero-day attacks.

Ready for Your Own Managed IT Services Success Story?

Whether your IT team is overwhelmed, your security is lacking in the face of new technology, you're ready to make a transition to the cloud, or you just need day-to-day IT help, Access One is here for you. We are the managed IT services provider that will help you achieve your technology goals. When you're ready to reap the benefits of an expert partner, get in touch with Access One.

Email us at info@accessoneinc.com or call 800-804-8333 today.

A laptop is shown from a low angle, with a person's hands typing on the keyboard. The laptop screen displays the Access One logo, which consists of a circular icon with a stylized 'A' and the text 'access one' in a sans-serif font. Below the logo, the tagline 'Technology Solutions, Delivered with Care' is written in a smaller, italicized font. The entire image has a green overlay.

access one
Technology Solutions, Delivered with Care