Zero-Day and known vulnerabilities: How to protect against them?

Zero-day attacks are increasing every day and are creating problems every day for organizations. The MIT Technology review mentioned that cybercriminals performed 66 zero-day attacks per day in 2021, and 2022 will only see the rise in Zero-day attacks.

A zero-day vulnerability was being exploited back in 2018 against the Windows users in the Middle East Areas.

Can you see the intensity with which zero-day attacks increase and impact the business every day? Attacks due to zero-day vulnerabilities often occur due to a lack of awareness among the company members. But this mistake can cause a hefty amount of loss to the company.

Keep on reading to know everything about zero-day attacks and how you can protect your organization from them.

What is a zero-day vulnerability?

A zero-day vulnerability is a flaw or weakness in firmware, hardware, or software that may have been displayed as disclosed but actually remains unpatched.

When the cybercriminals become successful in attacking the vulnerability and exploit it to perform a cyberattack, it becomes a **zero-day attack or exploits.**

How are zero-day exploits used in a cyberattack?

Here are some of the ways in which threat actors use zero-day exploits to perform a cyberattack.

1. By compromising the security of the network, server, or systems

Cybercriminals use zero-day exploits to penetrate through dictionary attacks or brute force or via inadvertent exposure through the internet. Attackers use malware to perform a cyberattack through this gateway.

2. Exploit kits

Exploit kits involve attacking in succession and using malvertisements and malicious websites which act as a host for zero-day exploits.

Read More: Zero-Day and known vulnerabilities: How to protect against them?