idea LOGICAL

LOGICAL TALK · JULY 2021 EDITION

Why Zero-Day Attacks Are On The Rise

Zero-Day Attacks are the next big concern after ransomware and phishing in the world of cybersecurity.

When a newly discovered software exposure is identified and there is no patch or update available at the time of the discovery is called a Zero-Day vulnerability or a Zero-Day incident. It is referred to as a Zero-Day attack because the developers and the experts have no time, a.k.a has zero days to find a solution in the form of a patch or an update.

Why Are Zero-Day Vulnerabilities Becoming One Of The Highest Cyberattacks Of Concern?

The fear of the unknown is why zero-day vulnerabilities are becoming one of the highest cyberattacks of concern.

Zero-day vulnerabilities are critical yet undisclosed threats or that are only discovered as the result of an attack. The software company or its users do not yet know about the vulnerability. As soon as the zero-day vulnerability is identified, an unofficial race starts between the security team of the software company and the threat actors to either patch the vulnerability or exploit it respectively.

This race causes a lot of uncertainty for third-party service providers or the end-users as the event is out of their control. The outcome solely depends on who wins the race – if the security company wins, there will be a patch or an update to stop vulnerability from doing any damage. If the threat actors win, the level of concern rises as nobody knows how they would exploit the systems.

Most recent attacks like on Microsoft and Kaseya VSA are the most prominent examples of zero-day vulnerabilities.

How Is A Zero-Day Attack Executed?

A zero-day attack is initiated when threat actors exploit a zero-day vulnerability.

First, the threat actors test open-source code and proprietary applications for undetected vulnerabilities. Sometimes, threat actors also turn to black markets to purchase information on vulnerabilities that are not yet public.

Then, the threat actors create a kit, script, or a process that enables them to exploit the discovered vulnerability. Once an exploit is available, attackers begin looking for affected systems. This may involve using automated scanners, bots, or manual probing.

The type of attack that a threat actor wants to accomplish is determined at this step. If an attack is targeted, attackers typically carry out inspections to reduce their chance of being caught and increase the chance of success. For general attacks, criminals are more likely to use phishing campaigns or bots to try to hit as many targets as quickly as possible.

Finally, if a vulnerability requires first infiltrating a system, attackers work to do so before deploying the exploit. However, if a vulnerability can be exploited to gain entry, the exploit is applied directly.

How To Protect Your Business From A Zero-Day Attack?

At the moment, there are minimum controls against zero-day vulnerabilities. However, as a business, you must ensure that all your systems are patched and running on their latest updates. You must also avoid using any outdated/ expired hardware or software that the manufacturers do not support.

Finally, rely on the advice of only your trusted technology partner and let them guide you before, during and after an incident.

It's Time To Say Goodbye To Your On-Premise Server

With the attack on Microsoft Exchange vulnerabilities in March 2021, the theoretical weakness of having an on-premise exchange server came to life.

Idealogical security experts strongly recommend our clients to replace Microsoft Exchange's on-premises deployments with the cloud-based alternative - Microsoft 365. Being in the cloud, M365 is not vulnerable to an attack like Zero-day vulnerabilities or issues caused by bad weather or other outages.

Additionally, the chances are, with the March 2021 zero-day attack on Microsoft exchange, the threat actors may already have gained backdoor access and are ready to exploit targeted systems.

Therefore, this is the right time to transition from Microsoft Exchange to M365 if it is not too late already.

Why Move Your On-Premise Set-up to Cloud

SECURITY
Microsoft Exchange: Data is the most valuable asset of your business. Losing it can be crippling, both for your efficiency and your reputation. The security of your data with on-premises storage is heavily dependent on manual effort. So, if there is a malfunction in the system or a compromised system held for ransom may result in a longer recovery time or, in the worst-case scenario, complete loss of data.

M365: No solution is 100% secure, especially when cyber threats are evolving at lightning speed. M365 is no exception. However, security risks can be highly mitigated with security measures like single sign-on and two-factor authentication.

HARDWARE MAINTENANCE
Microsoft Exchange: With on-premise servers, not only does your backup need to be up-to-date, but you also have to take care of your on-premise hardware. You have to ensure that the hardware is under warranty, kept up-to-date and replaced if required, which adds to the overall maintenance cost.

M365: With M365, there is no additional hardware involved that would need maintenance, upkeep or replacement. The only hardware-related costs that M365 may incur are if your user hardware (laptops, desktops and phone) systems are out of warranty.

RANSOMWARE ATTACK VULNERABILITIES
Microsoft Exchange: The threat actors are aware of the disadvantages of having an on-premise server for a business. Therefore, there are higher chances of businesses with on-premise setups falling victim to ransomware attacks.

While a cloud-based system will keep your data backed up, on-premises storage systems have all the data stored on an internal server, meaning you assume a more significant amount of risk. A best practice for on-premise storage to avoid data loss is to include an off-site backup service that replicates the data to another site or media.

M365: On the other hand, M365 releases the latest version updates of their solutions without needing to handle any complicated manual patches that risk human errors. Microsoft delivers updates, and the cloud providers focus on the reliability and security of the system.

Read the full article online.

Superstar Of The Month - Ria Latchman

I am honoured to be voted Superstar of the Month by my team. The Idealogical family motivates me and it's a joy to come to work every day knowing I am supported and valued.

No matter the day and the challenges, as long as my Idealogical family is there, I know everything will be alright. Thank you, team, for all your support and encouragement. It is a privilege to work with each one of you.