ZERO-DAY VULNERABILITY

WHAT THEY ARE & HOW TO MITIGATE THE THREAT

A ZERO-DAY vulnerability is disclosed when software is found to be at risk but remains unpatched. Hackers take advantage to exploit the vulnerability. This is known as a Zero-Day attack.

Vulnerable software remains susceptible to attack from the time period of disclosure until it's fixed, which means developers must work quickly to provide a patch (a fix) for the vulnerability and close this window of opportunity. Patches are delivered to users in the form of updates.

Every individual user is responsible for installing the update. If we fail to do so, we leave our devices open to exploits, so an update policy is crucial to a cyber security strategy. Enable updates to be applied automatically, for immediate installation of patches.

Ordinarily, security defences protect from most known vulnerabilities, which is why criminals revel in the "window of exposure" offered by unpatched software. A zero-day attack can go unnoticed for a long time.

Should a hacker get onto a business' system through a Zero-Day attack, they can cause a data breach, release malware, and more, resulting in financial loss and reputational damage.

PDSC
POLICE DIGITAL SECURITY CENTRE

www.policedsc.com

To protect against Zero-Day:

- Automatically Update Software and Operating Systems
- Manage User Privileges
- Apply a multi-layered security approach, including installing AntiVirus and a Firewall