CYBERSECURITY

Information Sheet
Vulnerabilities

Tags: Cybersecurity

365 ARCHITECHS

No system is totally impervious to attack. Vulnerabilities are omnipresent in systems, networks, databases, devices and applications. They can be exploited by cybercriminals as they seek to disrupt operations, steal information and harm reputations. Using cyber defences to protect against these threats is critical in managing cyber risks.

This information sheet provides an introduction to the various types of vulnerabilities that may exist in any system.

Attack Surface

The attack surface, is simply the sum of all vulnerabilities. The larger the attack surface, the more opportunity that exists for threat actors to identify vulnerabilities open for exploitation. By reducing your attack surface, you can reduce the risk of a cybersecurity event.

Keep in mind that your attack surface may include:

- Websites
- Servers
- Cloud applications and services
- Internet of Things (IoT) devices
- Wi-fi networks
- Databases
- Networks
- Devices including desktop computers, laptops, notebooks, tablets and smart phones

One way of reducing your attack surface, is to limit the number of applications used. As cloud services become ever-increasingly available, organisational teams may implement applications without any form of centralised approval. This practice is known as **Shadow IT**.

Solutions are available to "discover" cloud applications being used on a network, as well as only allowing approved applications to run.

Patching

Software vendors regularly update their applications to address security vulnerabilities, yet many organisations do not install these updates, known as patches, as soon as they are released. It is critically important that patching is done on all operating systems, devices and applications regularly.

A common issue with patching, is that it can be difficult to know which devices are connecting to computer networks and systems, as well as identifying whether or not they have been patched to the latest versions.

Applications are available to interrogate devices when attempting to connect to systems, and to deny access if they don't meet certain requirements, including if they haven't been patched.

Security Misconfiguration

Security systems are complex. Some available security features may fail to be implemented, or those configured may be implemented with errors. Both of these situations can lead to vulnerabilities open to exploitation.

People

People are both the weakest link and the most import defence in the management of cyber risks.

Strong policies, supervision, insider threat protections, reviews of security audit logs, physical security systems and training may all provide a level of protection against people risks associated with cybersecurity.

About us
365 Architechs is a technology company based in Brisbane, Australia. We deliver solutions to support organisations on their digital transformation including cloud, modern applications, cybersecurity and artificial intelligence to drive profitability, growth and achievement of strategic objectives.
(07) 3393 1186 | www.365a.com.au | sales@365a.com.au