CYBERSECURITY

Information Sheet

Cyber Risks

Tags: Cybersecurity, Risk management

365 ARCHITECHS

Threat actors exploit vulnerabilities in technology systems to cause reputational damage, disrupt operations and steal information. This gives rise to a series of cyber risks faced by organisations today, who seek to implement effective cyber defences to protect against these risks.

This information sheet provides a suite of typical cyber risks faced by organisations today.

Understanding these risks can assist governing bodies and management to understand what controls should be implemented to effectively manage the likelihood and consequences of these risks.

Phishing

Hackers often start their approach by phishing for information. This is most commonly done by a phishing email, but equally could be a phone call. Phishing attacks can be elaborate, well-conceived tactics that trick people into providing seemingly benign information to be used against them.

Account breach and password cracking

Bad actors can gain access to systems and information by guessing or bypassing account passwords.

Sophisticated and inexpensive tools are available to automate the process of password cracking. This ultimately means that passwords alone are a relatively weak defence to keep intruders out of your systems.

Data deletion, exfiltration and spillage

Following a system breach, data can be deleted or encrypted so that it is no longer accessible. Information can also be transferred outside the organisation and made available for sale on the dark web.

A loss of data is potentially a significant risk when the information stolen contains personally-identifiable or sensitive data.

Escalation of Privilege

When hackers gain access to systems, they often look for ways to find other easy targets within the network to be able to attack. In this way, they can move laterally around the network, gradually increasing the systems they can access and damage they can do.

Malicious Insiders

Most organisations contain employees and contractors with a variety of personal ethical standards. The pressures of stressful working environments and challenges at home, when combined with opportunity and a high degree of trust, can create the perfect storm for malicious activity of those perhaps least suspected.

Spoofing

Disguising a communication from an illegitimate source masquerading as a trusted source is a hacker technique known as spoofing.

Spoofing can take many forms, including email spoofing where an email is received that looks like it has come from a particular person, but in fact has been sent by a cybercriminal pretending to be someone else.

Website spoofing occurs where a fake website is made to look like a legitimate one, and users are tricked into accessing the wrong site, where they may try to log in using their secret credentials which are inadvertently provided to the hacker.

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 3999 7000 | www.365a.com.au | sales@365a.com.au