CYBERSECURITY

Information Sheet

Attack Vectors

Tags: Cybersecurity, Attack Vectors, Threats

365 ARCHITECHS

Attacks are initiated by Threat Actors using Attack Vectors. These are the methods used to penetrate systems to gain access to resources and data to commit cybercriminal activities. They include a range of network threats, host threats, application threats and social engineering.

This information sheet provides an introduction to the various types of cyber threats facing organisations today. These threats are known as Attack Vectors. They can be categorised based on the target being attacked.

Network Threats

Network attacks attempt to gain access to a target computer network. They include active **Man in the Middle** (MITM) attacks, as well as passive **Sniffing** and **Eavesdropping**.

Once a computer network is compromised, attackers can move laterally throughout the network, looking for vulnerabilities in hosts and applications. See Information Sheet: Network Threats.

Host Threats

Hosts are another name for servers and computers, that include all endpoints such as desktop computers, laptops, notebooks, tablets and smartphones.

Threats affecting hosts include **Password** attacks, **Keyloggers** and **Malware**.

Application Threats

Just as entire networks and individual hosts are susceptible to attack, so are the applications running on them.

Websites and databases can be vulnerable to **Injection** and **Cross Site Scripting** (XSS) as well as **Denial of Service** (DoS) attacks.

Social Engineering

People can be the weakest link in organisation's security posture, which is why so many successful attacks include social engineering to gain access to systems to steal information, harm reputations or disrupt operations.

Social engineering involves tricking people into performing actions or divulging information. Human decision-making is influenced by cognitive biases which can be exploited by threat actors seeking to psychologically manipulate individuals.

The principle attack vector for social engineering threats is **Phishing**. See Information Sheet: Phishing Attacks.

However, other forms of social engineering include **Pretexting**, **Waterholing**, **Baiting**, **Quid Pro Quo** and **Tailgaiting**. See Information Sheet: Social Engineering.

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