DATA STORAGE OR PROCESSING

Sector Overview

When it comes to data storage and processing infrastructure in Australia, we are dealing with a very large and interdependent ecosystem. While many Australians will be familiar with the big global industry players like Amazon Web Services, Microsoft Azure, and Google Cloud which are all locally based in Australia, the rise of data centres and cloud computing has dramatically increased over the last decade.

There are a few ways to slice and dice the types of infrastructure in this sector; however, let's use the assessment from Cloudscene.com given they utilise a global comparative perspective: At the start of 2023, Cloudscene mapped the following types of data storage and processing infrastructure being operated in Australia:

- 21 Network Fabrics
- 294 Data Centres
- 724 Internet Service Providers (ISPs)
- 173 Colocation Providers
- 598 Connectivity Service Providers
- 207 Hosting and Cloud Providers
- 453 Managed Service Providers

Looking ahead, the Australian data centre market alone is anticipated to develop at 7.67% (Compound Annual Growth Rate) between 2022 and 2027. This is important because the attack surface and related threats are also likely to increase over the same period. Government investment, technological advancements, the adoption of high-performance computing (HPC) technologies, and rising data centre investments contribute to the market's considerable growth.

Layering these seven elements on top of the communications sector infrastructure, and you're left with a spaghetti web of interrelated systems. Another consideration is the chokepoints - Australia's international cable connections are particularly noteworthy for concentration risk. The subsea cables that tie the data storage and processing sector together are primarily routed through the Southern Cross Cables, PPC-1, Japan Guam South Cable (Maroochydore & Sydney) and SMW-3 (Perth to Singapore via Jakarta). The majority of all significant east coast underwater cables land in Sydney, which acts as Australia's primary interconnection hub.

Cyber Threats to DSP Sector:

The DSP sector is a rich target for cyber attackers since this infrastructure moves and stores data on a large scale. All major private and public sector organisations in Australia are integrated with and dependent on this sector.

High profile attacks:

Threat actors often seek to exploit exposed remote desktop servers, and an example of this is an attack in 2020 against global tech company Equinix whose internal systems were

compromised by a ransomware attack. The attacker, Netwalker, sought a US$4.5 million ransom payment from Equinix to prevent the company's clients' payroll, accounting, audit, and financial data from being released. The initial access vector was identified as credentials and information on remote desktop servers procured on dark net forums. In 2019, a ransomware attack by REvil (Sodinokibi) on CyrusOne encrypted certain devices in CyrusOne's networks that shut down the managed services of many of its clients.

Cyber criminal motivations to target Data Centres:

Cyber attackers actively seek to exploit weaknesses and gaps in data centre security that can occur because so many technologies and applications run simultaneously and complicate vulnerability management, especially when technology develops rapidly. Hackers are constantly on the lookout for new ways to get around security measures.

Motivations vary, with examples being:

- Retaliation against the company or a party associated with the data centre, hackers may execute a cyberattack on the HVAC systems of a particular data centre location.
- Disruption by state-sponsored hackers may interfere with the power supply of crucial data centre components, which might result in a total shutdown of plant operations and disarray among data centre stakeholders.
- Financial gain by hackers who exfiltrate private information from the data centre and its components and sell it to interested parties on dark web markets and forums.

Main threats for DCs:

DC's are among the most crucial components of an organization's IT infrastructure, and their capacity to function is significantly impacted if activities are disrupted by two main types of threat:

Physical Infrastructure attack:

Compute, storage, and network functions represent three core components of DCs operations, with a DC's availability, performance, and security all impacted by physical attacks. Various physical safeguards against infrastructure attacks are incorporated into DC's during the design phase. Redundancy is used for critical functions to reduce single points of failure and increase uptime. The infrastructure supporting DC's must also be built to deal with natural disasters and terrorist threats that can interfere with operations. These include building security systems, temperature control, fire suppression systems, and uninterruptible power supply (UPS).

Cyberattack:

DDoS:

The most frequent type of cyber-attack on DC's are distributed denial of service (DDoS) attacks. By flooding a DC with too much traffic, hackers try to inhibit the systems using the DC, making applications or websites being run on the infrastructure inaccessible. DC 'uptime' is, therefore a key performance metric that is directly threatened by DDoS attacks. Attackers might also seek to co-opt DC infrastructure to create scaled botnets to launch other attacks and this vector for exploitation increases with the number of insecure IoT-linked devices that a DC might host or operate. DDoS attacks can jeopardise availability, costing a DC money, clients, and reputation. Additionally, attackers can amplify the scope and severity of DDoS attacks by exploiting various application layer techniques.

Ransomware:

Unlike DDoS attacks, the impacts of ransomware can persist long after an initial assault is halted. Restoring data from backups might take a long time if the data is damaged or in an unknown state. Data centres may therefore be unable to operate for several days or even weeks/months following a ransomware attack. For example, a ransomware attack on the South Korean hosting company Nayana caused the servers hosting hundreds of client websites to go offline for many weeks. Even after a $1 million dollar ransom was paid, not all files and services were recovered. One of the biggest providers of on-demand colocation data centres in the world, Equinix, has also been subjected to a ransomware attack due to vulnerabilities in internal systems.

External Access Service:

Numerous stakeholders are usually involved with DC security administration, with external services like cloud access security brokers or external DNS servers frequently targeted by attackers seeking to exploit gaps in these external dependencies to cause harm. NordVPN, a market leader in virtual private network (VPN) services companies use to safeguard sensitive data, acknowledged that one of its data centres had been compromised in 2018 because of the unauthorised installation of a third-party remote access system that created an insecure server.

Application attacks:

Attacks against web or server applications, such as a customer dashboards or control panels, can effectively shut down services by rendering them inaccessible, even though attackers may not directly harm DC services in the process. These types of breaches are possible using brute force methods, which succeed as a result of weak passwords or a lack of multi-factor authentication (MFA). Such attacks are more focused and use less operational bandwidth, yet they still have the potential to disrupt services. For instance, if a data centre or hosting provider offers a control panel application to its clients or users, the availability can be impacted by an attack that causes a program to crash. Likewise, Dropbear SSH DoS or Slowloris Apache HTTP attacks in a concentrated attack can overwhelm protocols.

Vulnerabilities of DC's:

Applications running on data centre infrastructure may use code that is vulnerable to exploitation. This applies to internally created and third-party code imported through libraries and in programs built outside the company.

Remote access tools: Due to the Covid-19 pandemic, remote work became more prevalent, and businesses implemented remote access solutions, including virtual private networks (VPNs) and the remote desktop protocol (RDP). Cybercriminals took advantage of these new entry points, using stolen credentials and unpatched vulnerabilities to infiltrate networks and install malware.

Supply chain vulnerabilities:

Organisations rely on external apps in their environment. Due to the dependence of the data centre on the security of these third-party organisations and technologies, these third-party products may introduce additional, less obvious security vulnerabilities.

Responding to threats against the energy sector in Australia:

Many Data Storage or Processing sector entities won't be able to share 'machine to machine' intelligence, so an industry partner is needed as the enabler/facilitator for cyber threat intelligence (CTI) and collective defence via other means. By taking on the role of the trusted advisor/facilitator for the intelligence exchange, an industry organisation would ensure the overall quality of information flowing through its systems and out to the CI members.

'Forewarned is Forearmed', and by joining a trusted cyber community of Critical Infrastructure owners and operators responsible for protecting their data storage or processing assets, you can join the movement to share contextual intelligence and proactively approach cyber defence. Cyber threat activity shared into the CI-ISAC ecosystem by one member has the potential to help others across the sector and the broader CI community stop similar attacks before they impact operations.

CI-ISAC, as a not-for-profit, member driven organisation, with a mission to serve its members and in turn their customers by building a trusted community and leveraging the best technology in its intelligence platform, and drawing on resources and resilience through its industry peer-to-peer network to anticipate, mitigate, and respond to cyber threats.

More information on CI-ISACs sovereign intelligence-sharing capability can be found on the official website: https://www.ci-isac.com.au , or by emailing info@ci-isac.com.au.

Published: 21st February 2023