Collaborative Discussion 1: Digitalisation – What are the security implications of the digital economy? -> Initial Post -> Peer response

by Gokul Kurunthasalam - Wednesday, 29 June 2022, 7:07 AM

Dear Amit,

I appreciate your post on shifting SMEs to a digital cloud platform and the attendant security challenges and I fully agreed with it. A data breach on a cloud platform can cause data loss or theft as well as harm to the integrity, confidentiality, and availability of data. Causes of cloud data breaches include are Insufficient identity & credential management, Easy registration systems, phishing, pretexting and Insecure APIs. There are a few more common causes of security problems.

- Human mistake
- Excessive permissions granted
- Keeping inactive and inactive accounts
- Leaving default settings in place, such as admin login information and port numbers
- Removing common security measures
- Taking away encryption

In order to reduce vulnerability to cyber threats, SMEs must rearrange their IT infrastructure and business procedures. While adopting cutting-edge technologies like AI, Cloud Computing, and IoT is essential for ongoing success, businesses must exercise extreme caution when choosing service providers. They might choose the Cloud Content Security Platform (CCSP), which offers security services for multi-factor authentication (MFA), endpoint security, next-generation firewalls, and email, web, and endpoint security. This all-encompassing smart perimeter offers simplified architecture, minimises cyberattack vectors, streamlines operations, and enhances firewall intrusion detection while supporting a variety of applications. Additionally, it reduces operating expenses and uniformizes the firms' security infrastructure.

Small and medium-sized businesses (SMEs) must adopt a zero-trust strategy that permits only verified and trusted devices to be connected to the corporate network as cloud computing becomes key to all transformational technologies. With so many endpoints, businesses must set up access controls for two crucial entry points: remote applications and online access. This strategy makes it possible for all systems, endpoints, and internal applications to serve as an extra layer of defence against attackers trying to access enterprise infrastructure, whether it be hosted in the cloud or on-premises.

References:

N. Amara, H. Zhiqui and A. Ali, "Cloud Computing Security Threats and Attacks with Their Mitigation Techniques," 2017 International Conference on Cyber-Enabled Distributed Computing and Knowledge Discovery (CyberC), 2017, pp. 244-251, doi: 10.1109/CyberC.2017.37.

A. Behl, "Emerging security challenges in cloud computing: An insight to cloud security challenges and their mitigation," 2011 World Congress on Information and Communication Technologies, 2011, pp. 217-222, doi: 10.1109/WICT.2011.6141247.

SMEs are going digital, but what about cybersecurity? https://www.dqindia.com/smes-going-digital-cybersecurity/ [Accessed on 28 JUn 2022].