OPEN ACCESS Freely available online

Journal of Defense Management

Commentary

Evolution and Strategies of Defense-in-Depth

Rong Duan*

Department of Defense Management, Jamia Millia Islamia University, Jamia Nagar, Okhla, New Delhi, India

DESCRIPTION

In order to provide additional, redundant defensive measures in the event that a security control fails or a vulnerability is exploited, a defense-in-depth technique is used in information assurance. It takes its name from a military tactic that aims to slow down an attack rather than repel it with a single, effective line of defence.

Defense-in-depth cybersecurity application cases include end-user security, product design, and network security.

Defense in depth's adversary, simplicity-in-security, operates on the presumption that having too many security precautions may result in issues or gaps that attackers may exploit.

Evolution of defense-in-depth

In the past, most companies created defense-in-depth plans based on conventional perimeter-based security models to safeguard on-site IT infrastructure. A traditional defense-in-depth security approach includes a variety of security components, like

Endpoint security solutions: Endpoint Privilege Management (EPM) solutions to govern access to privileged endpoint accounts, antivirus software, and Endpoint Detection and Response (EDR) tools to safeguard against threats coming from PCs, Macs, servers, and mobile devices.

Patch management tools: Maintain the security of endpoints by updating their operating systems and applications, and by addressing known vulnerabilities and exposures (CVEs).

Network security solutions: Protecting traditional enterprise networks and traditional on-premises IT systems using firewalls, VPNs, VLANs, etc.

Intrusion detection/prevention (IDS/IPS) tools: For the purpose of detecting harmful activities and preventing attacks against conventional on-premises IT systems.

User identity and access management solutions: Solutions for lifecycle management, single sign-on, and multi-factor authentication that authenticate and authorise users.

Strategies of defense-in-depth

The digital world is not well suited for traditional perimeter-based IT security methods, which were designed to regulate access to reliable enterprise networks. Today's enterprises use SaaS solutions, corporate data centres, private clouds, and public clouds to create and deploy their applications. Defense-in-depth tactics are increasingly being used by most enterprises to safeguard cloud workloads and counter new threat vectors brought on by digital transformation.

In response, many businesses are changing their security strategies and adopting a Zero Trust "assume-breach" mentality, employing a combination of preventative controls and detection technologies to recognise attackers and prevent them from achieving their objectives once they have gained access to a network. A contemporary defense-in-depth strategy's fundamental principles include

Protect privileged access: Privileged accounts (such as superuser accounts, local and domain administrator accounts, application administrative accounts, etc.) can be accessed by both human and non-human identities. Privileged access management technologies can be used to monitor and protect this access (applications, scripts, bots, etc.).

Lockdown critical endpoints: Utilize cutting-edge endpoint privilege management tools to restrict access across all endpoints, stop lateral movement, and protect against infections such as ransomware.

Enable adaptive multifactor authentication: Employ business rules and contextual data (such as location, time of day, IP address, type of device, etc.) to decide which authentication factors to use for a certain user in a specific scenario.

Secure developer tools: Secure, manage, rotate, and keep an eye on the secrets and other credentials used by applications, automation scripts, and other non-human identities by using secrets management tools

As part of a comprehensive, contemporary defense-in-depth strategy, businesses typically implement privileged access

Correspondence to: Rong Duan, Department of Defense Management, Jamia Millia Islamia University, Jamia Nagar, Okhla, New Delhi, India, E-mail: Duanrong123@yahoo.com

Received: 15-Dec-2022, Manuscript No. JDFM-23-21659; **Editor assigned:** 20-Dec-2022, PreQC No. JDFM-23-21659 (PQ); **Reviewed:** 10-Jan-2023, QC No. JDFM-23-21659; **Revised:** 17-Jan-2023, Manuscript No. JDFM-23-21659 (R); **Published:** 24-Jan-2023, DOI:10.35248/2167-0374.23.13.254.

Citation: Duan R (2023) Evolution and Strategies of Defense-in-Depth. J Defense Manag. 13:254.

management solutions, endpoint privilege management solutions, adaptive multifactor authentication solutions, and secrets management solutions alongside more conventional enterprise security solutions (such as EDRs, firewalls, IDS/IPS, etc.).

CONCLUSION

Defense in Depth (DiD) is a cybersecurity approach that layers numerous security mechanisms to protect critical data and information. When one defence system fails, another springs into action right away to stop an assault. This multi-layered strategy with deliberate redundancy boosts system security overall and counters numerous attack routes. Because it mimics the layered defences of a mediaeval castle, Defense in Depth is sometimes known as the "castle strategy." We must overcome the moat, ramparts, drawbridge, towers, battlements, and other obstacles before they may enter a castle.

The way we live, work, and play has been changed by the digital age. But because there are so many possible attackers in the digital world, we need to make sure we have the proper security measures in place to guard against networks and systems being compromised. Unfortunately, no one strategy can effectively defend against every single form of attack. A defense-in-depth strategy can be used in this situation.