NIGC Tech Alert

CYBERSECURITY: DEFENSE IN DEPTH

Defense in Depth -- sometime referred to as the "castle approach" because it mirrors the layered defenses of a medieval castle -- is a strategic approach to cybersecurity that incorporates a progression of layered defensive mechanisms to safeguard data, information, and information systems from successful attacks. Recent cyber-attacks against large organizations across both government and private sectors remind us that having a multi-layered approach with deliberately structured redundancies significantly increases the security of a system. The variable barriers and countermeasures of such systems address different attack vectors. Companies, governments, and organizations are increasingly technology dependent. Cyber related attacks impact organizations, big and small, have increased in recent years, and are not going away. To significantly reduce risk to IT systems, it is prudent for organizations to employ a layered, redundant approach to cybersecurity.

Within the Defense in Depth method to achieve security objectives, there are three critical control layers: physical controls, technical controls, and administrative controls. Physical controls are defense in depth layers implemented to prevent an attacker from gaining physical access into an organization's IT network. They are traditional protections that can be used for anything, from access to the organization's physical site, to protection from specific secured rooms inside an organization. Examples include, but are not limited to, CCTV systems, reinforced fences, and security guards. Technical controls (logical controls) are software and hardware meant to protect an enterprise's system and data assets. They differ from physical controls in the sense that they protect the data of a system rather than the physical system itself. Examples include antivirus software, software or hardware firewalls, disk encryption, authentication controls, and Multi-Factor Authentication. Finally, the concept of administrative controls refers to an organization's IT security policies and procedures. The purpose of this layer of defense is to provide appropriate cybersecurity guidance and to ensure IT regulations are adhered to. Examples include security requirements, data handling procedures, digital code of conduct, confidentiality policies, etc.

The concept of Defense in Depth is not new. Many organizations already employ many of the Defense-in-Depth measures within their IT infrastructure, but some do not apply it across the entire organization. The defense in depth security architecture can help mitigate, but not eliminate cyber risk.

Should assistance be necessary regarding Defense in Depth principles and techniques to reduce the risk of cyber-attack, please reach out to NIGC. The NIGC offers technical assistance, training courses, IT audits and other tools and resources.

For minimum internal control standards, please find the NIGC IT Audit 25 CFR 543.20 Toolkit at

https://www.nigc.gov/images/uploads/training/Toolkit_ITAudit_Rev12_4.pdf

Additional resources detailing information on Defense-In-Depth and related cybersecurity strategies can be found here:

https://csrc.nist.gov/glossary/term/defense_in_depth

Please view the CISA The Department of Homeland Security (DHS)'s National Cybersecurity and Communications Integration Center (NCCIC) document at

https://www.cisa.gov/sites/default/files/recommended_practices/NCCIC_ICS-CERT_Defense_in_Depth_2016_S508C.pdf

September 2023

Division of Technology