Video reaction

Cyber Security: Access Control Training Podcast- OPTIONAL

http://www.nist80037rmf.com/cyber-security-access-control-training-podcast

http://convocourses.com

RMF ISSO:

Access Controls documentation(security control)

NIST special publication 800-53(Rev. 4)

Security and privacy control for federal information systems and organizations.

Summary of video

The first part of the video talks about access control documentation such as AC-3 (access enforcement), AC-4 (information flow enforcement), AC-5 (separation of duties), AC-6 (Least Privilege). His on-site guidance nvd.nist.gov/800-53/rev4/ NIST special publication "Control Series", where we can learn more about these access controls. In the second part, he talked about job search websites such as LinkedIn and dice.com.com. He explained how we can fill up the online resume on those sites to get more and more attention of recruiters.

What I have learned

Access control, as it relates to this guide, pertains to granting or denying logical access to a resource, such as data/information or a system. Accession is gained by an individual (a user of the resource),

sometimes individuals are aggregated into groups. It is also possible to have automated system-to-system access, known as system interconnection. Confidentiality, integrity, and availability of information are also an issue when access controls are not properly implemented. If a security breach affects one area of the network, and there are insufficient access controls present to contain or mitigate the breach, its reach may be expanded, affecting additional systems, components, and data. Improperly implemented access controls can result in negative consequences, ranging from a lack of information being available to compromised data integrity and/or lack of confidentiality. There is also a possibility of a negative financial impact due to the response to or recovery from a breach. In addition, due to non-compliance with laws and regulations, legal issues may also occur, leading to warnings, fines, and more access to regulations.

Similarly, access enforcement (AC-3) is the organization's ability to implement access control policies and procedures. The flow of information within and between the system and the control of the interconnected system is information flow enforcement (AC-4). It controls where information is allowed to travel in an information system and between the information systems. Separation of duties (AC-5) distinguishes the duties between the user and the device, without collaboration, to reduce the possibility of malicious behavior. The Least Privilege Principle (AC-6) is the concept of restricting user access rights to the bare minimum permissions necessary to conduct their work. In information system systems, the concept of the least

privilege is often implemented, ensuring that the process operates at the level of privilege no higher than necessary to achieve the organizational mission/business purpose required.

Overall, video was informative and also tutorial on creating resume, searching and applying job using Indeed, LinkedIn, and DICE was helpful.

Reference:

"Cyber Security: Access Control Training (PODCAST)." *ConvoCourses*, 22 Mar. 2020, www.nist80037rmf.com/cyber-security-access-control-training-podcast.

Cyber Security & IT: RMF Access Controls Training - YouTube. www.youtube.com/watch?v=1LkfH1TI3rk.

NVD, nvd.nist.gov/800-53/Rev4.