Webinar Questions and Answers

Best Practices & Vulnerabilities for Privileged Accounts

Webinar guests submitted several questions before and during the **9 July 2015, Best Practices and Vulnerabilities for Privileged Accounts** session. The following responses are provided by the Center for Development of Security Excellence (CDSE):

Question: I am a 0080 and how does this apply to me as security manager.

Answer: As a 0080, in supporting a DoD network, a lot of this is mandated. However, it is important that the Security Administrators, those ISSPs understand what the best practices are and how they relate to the network's security and to work together with the ISSM and other system and network personnel in providing the best protection possible.

Question: Understand DoD policy is to change password every 60 days. Is it acceptable to repeat passwords?

Answer: Yes as long as the password hasn't been used within the last 24 times. In accordance with DoD, password history is configured to 24.

Question: Did OPM adequately protect DoD personnel information in accordance to best practices?

Answer: I would certainly hope so though I cannot say with absolute certainty as I do not know what OPM's practices were.

Question: Are the privileged users consider sensitive-critical or non-sensitive critical?

Answer: This is based on security clearance and/or information technology (IT) level of the assigned information system (IS) and is based on the duty position. I would say to check your PD or appointment orders as it should be annotated there.

Question: Does an ISSO need a cert for a MUSA?

Answer: The regulation does not differentiate whether you're performing duties on a Multi-User Standalone or a networked system. Most often, prior to being hired into a position or within a certain period of time, it is stipulated as to what certifications are required for that position. However, I would refer to the DD254; the language within the contract.

Question: Are Industry Partners eligible to participate in the CDSE training and certification programs?

Answer: The short answer is yes. However, I would say that you should go to CDSE's website for a listing of training courses that are available for Industry and also checkout STEPP for those certifications that are available to Industry.

Webinar Questions and Answers

Question: What shall we advise our employees with clearances who are concerned with the OPM breach?

Answer: I would advise them to be vigilant in monitoring their credit reports and to stay up-to-date with and follow OPM's guidance for those affected. The following is a link to OPM's latest information: https://www.opm.gov/cybersecurity/.

Question: How do you know when a service is using elevated privileges and if they can be downgraded?

Answer: Run "services.msc"; it shows a list of services. If you look in the "Log On As" column, you can see which accounts are controlling which services; could be local system, local service, network service, a local user account, or an Active Directory user account. Ensure that the account is not a built-in Administrator or an Administrator account that was renamed. Also, for more information on this topic, check out https://msdn.microsoft.com.

Question: Will we receive a certificate for today webinar?

Answer: Yes you will.