

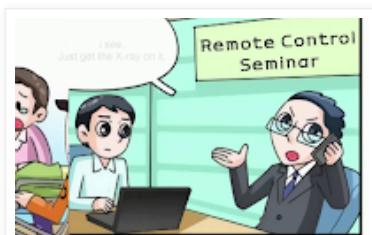
Cybersecurity Blog

Everything about threat intelligence, blue team, red team, pentesting, security audit, security review, testing and assessment.

[Home](#)[MY THOUGHTS FEED](#)[PENTEST TOOLS ARCHIVE](#)[CONTACT ME](#)[DISCLAIMER](#)[ABOUT ME](#)

Sunday, November 24, 2019

Auditing remote access process and procedures



In this article, I am going to share a small checklist that will help auditors and testers to provide assurance on remote access processes and procedures for any company. This is not a technical article but controls defined in this list can be well-reviewed by managers and to be discussed with clients. For each part, if they want to go in-depth, they can.

Administration

- Review policies, procedures and access controls
- Review procedures for remote access including guidelines for receiving access
- Obtain and review documentation of design including DMZ and authentication servers
- Obtain or create a flowchart of traffic flow for remote access

Authorisation and access management

- How Client manages access management and authorization. Are there any procedure that includes:
 - approval by an appropriate department manager
 - approval by IT management
 - Client to verify background checking done for employees of Third Party who are involved in remote access and administrative rights on Client systems
 - a user is a current employee of Third Party

Translate Language

Search

Subscribe via email

Blog Archive

- [2020](#) (2)
- ▼ [2019](#) (6)
 - ▼ [November 24](#) (2)
 - [Guidelines for Corporate Email Audit](#)
 - [Auditing remote access process and procedures](#)
- [September 22](#) (1)
- [September 15](#) (1)
- [May 12](#) (2)
- [2018](#) (4)
- [2017](#) (5)
- [2016](#) (11)
- [2015](#) (4)
- [2014](#) (22)

- duration of remote access given or Remote access can be allowed from any devices on the Internet with valid login credentials?
- account removal upon Third Party's notice to Client if an employee leaves an organization (What if Third Party does not inform Client that the employee left the Third-Party before or not)
- A user must be able to authenticate from the authorized system only
 - does Client has the list of approved Third-Party devices from where remote access is allowed?
- An automatic disconnect of sessions for remote-access technologies after a specific period of inactivity configuration set or not
- Following should be prohibited while accessing data through remote connection:
 - Copying, moving, and storage of data - If allowed by Client, it must be documented and approved in prior; also audit trial of such activity must be logged

Software and hardware used in the remote access process

- Check whether the remote access software is well-known, updated to the latest version and patched against all public vulnerabilities
- Check the type of authentication and encryption being performed with the help of software
- Review the latest encryption standard for the software
- Ensure testing of fail-over devices is performed periodically
- Verify that fail-over tests are performed periodically for VPN authentication devices.

Security

- Management should monitor security incidents and the extent of compliance with information security procedures.
 - Verify through inquiry with the IT Infrastructure Manager that security events such as multiple failed login attempt, username enumeration, numerous failed 2FA/MFA attempts are appropriately identified, investigated, escalated, and resolved after notification.
 - Ensure that audit trails exist, are properly managed and historical data exists.

Posted by Froggy at [11/24/2019](#)



Labels: [access management](#), [administration](#), [authorisation](#), [corporate remote access](#), [encryption](#), [remote](#), [remote access](#), [third party](#), [vpn](#)

No comments:

[Post a Comment](#)

[Newer Post](#)

[Home](#)

[Older Post](#)

