Chad Ballay

Week 8

Trusting no one is usually good advice with regard to external access. It’s the default behavior you should start from. Generally, the authentication procedure can be summed up as IAA. (Cha14)

1. Identify who you are.
2. Authenticate that you are who you say you are.
3. Authorization is given to you on what you can and cannot do.

In the hypothetical case of an employee trying to remotely access while at a conference they would generally connect using one of these protocols. (Remote authentication protocols, 2020)

* PAP – Password Authentication Protocol
* CHAP – Challenge-Handshake Authentication Protocol
* EAP – Extensible Authentication Protocol
* TACACS – Terminal Access Controller Access-Control System
* XTACACS – Extended TACACS
* TACACS+ – Entirely new protocol implemented to replace TACACS
* Radius – Remote Authentication Dial-In User Service
* Diameter – Evolved from Radius as a replacement

The biggest concern is that by opening your network to remote access you may allow bad actors in who can then exfiltrate data outward or wreak havoc internally. This can be limited by implementing several best practices. The first would be the use of multifactor authentication. (Something you know, you have, and you are.) Another would be implementation of a Policy of Least Privilege. (Do remote users need read/write access to production?) Yet another best practice is to implement a jump host architecture. (A remote desktop that the user then connects to internal resources.)

There is no one true best solution. There are some best practices that supercede the implementations of one protocol over another. Mostly the focus is that your remote access process should be grounded in a suspicious posture. Any and all gates that you open in the city wall are points that will be attacked. The use of these entry points for remote access will require vigilance and revision. Today’s secure design is tomorrow’s zero-day exploitable design. Starting with the abstraction of ensuring you know who is coming in, why they are coming in, and watching what they are doing is a best practice that evolved during the times of city states. It is time tested and will do us well if we translate that into a modern implementation.

# Works Cited

Chapple, M. B. (2014). *Access control, authentication, and public key infrastructure.* Burlington, MA: Jones and Bartlett Publishers, Inc.

*Remote authentication protocols*. (2020, April 5). Retrieved from CryptoWiki: http://cryptowiki.net/index.php?title=Remote\_authentication\_protocols