Chad Ballay

**Week 8**

Relevant Links

<https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-114r1.pdf>

A bucket with just one hole will lose water. No matter how insignificant the size of the hole, it’s very existence is anathema to the job a bucket is supposed to do with regard to holding water. The same holds true for the security of your network. A single hole in your security posture destabilizes much of your network’s safety. We have several tools at our hands to limit the blast radius of the damage but at best you are ceding ground that everything in that compartment is a write off. Telework needs to be done but is also one of the highest risk access mechanisms you’ll have in your network.

Much of the use cases is on BYOD(Bring Your Own Device) items that the employee will supply. The network owner will implement an access mechanism that allows this unmanaged device access to the private network. The crux is how do you allow the friendly barbarian at the gate to come into the city walls without throwing the gates wide for all the unfriendly barbarians to come in as well. I use the combative term intentionally since even at best you have to be overly suspicious to the outside connection. At worst you have to neutralize the connection. Any telework connection is by it’s very definition coming from unknown or untrusted infrastructure.

Some mechanisms for protection:

* VPN – Ipsec or SSL. First secure the tunnel in from the outside. Ensure that no one but the device/user you are connected to can eavesdrop.
* Audit/Process Control – Regular reviews of who has access, what they have access to do, and how often they are using this access is a must.
* Access Limit – At the far end you give the user the ability to connect to an internal system and control it remotely. This way the inputs in can be monitored. At the near end, you limit the access to very clearly defined apps. Does a remote user only need access to Box or Sharepoint? Then that is all that you allow them to have.

Device ownership also plays a key into your security posture. From best to worst:

* Organization – Devices owned/maintained by the network owner. These can be audited and controlled.
* Third Party Controlled – Not as good but at least an interested party is in control.
* BYOD – The employee provides the device and the network owner pre-installs some security controls on it to enforce security policy. Often this is prework is done by having the device be physically onsite and connected to the local network. This is to ensure the device is in fact tied to the specific user.
* Unknown – The least liked option. This is where any device can be used with no pre-installed security control in place before the connection starts.

Once the data leaves your network and is routed to the device you can probably assume that it could be gone forever. Local device encryption and sandbox environments will do much to combat low energy efforts but there comes a point where those checks can be overcome. This doesn’t mean that you shouldn’t make those efforts though. Remote wipe ability, periodic expiration of local storage, etc, etc…. are layers of the onion needed here. The same with enforcing of minimal accepted application version, wireless encryption, etc…. All of these will often give you partial protection but the sum total will add up to a broad coverage.