Research Report 5: Ransomware Recovery

What did you do?

I first prepared the inventory of network devices by referring to 'Research Report 1: Managing My Network'. Here I was able to obtain the devices from the chosen network and identify which of these are vital/critical and must be recovered first. The process of identifying was weighing which devices held the most important information that would have the biggest impact if lost. I created a table with two columns: the first being the name of the device and the second being whether this device was identified as vital/critical and needs to be recovered first. I also added a column to specify whether each device needs to be updated at this time. I went through the devices to check for any updates/outdated technology. This is referred to as Table 1 in the results. Not only are the devices identified as such, but I also put together a table that recognizes the servers of the network and which ones need to be backed up and recovered first, like the inventory of network devices.

Next, I used the assignment 'Vulnerability Scanning with Shields Up and Nessus' to determine which components of the network need to be updated. From this assignment, there were two medium vulnerabilities reported from Nessus. With the results from Nessus, the software provided which steps needed to be taken to fix these vulnerabilities and not lead to exploitation in the future. I created Table 3, found in the results, to present what these vulnerabilities are and the action that needs to take place.

From the Ransomware Protection Best Practices by Rick Vanover and Edwin Weijdema, they stated that forced password resets are encouraged by "management [implementing] a sweeping force change on passwords on a regular basis" because it "will reduce the threat propagation surface area" (Page 27). With that being said, it is important to ensure that passwords are regularly changed even if there are multiple passwords within a network. Created in Table 4 in the results, is a table that lists the roles of each password within the network that need to be regularly updated and backed up. Not only is there a table for passwords, but I have also created Table 5 to list the network's backups that need to be prepared and maintained.

Lastly, taking all the tables so far into consideration, I have created Table 6 to list the prioritized list of components for recovery. I combined the devices listed as vital from Table 1, all servers from Table 2, all passwords from Table 4, and all backups from Table 5. All these components play their own critical role when it comes to recovery of the network.

What were the results?

Table 1: Inventory of Network Devices

Device	**Vital, Critical, Recovered First (Yes or No)**	**Need to be Updated? (Yes or No)**
Router	Yes	No
Cables	No	No
Printer	No	Yes
Laptop 1	Yes	Yes

Laptop 2	Yes	Yes
Laptop 3	Yes	No
Laptop 4	Yes	No
TV 1	No	No
TV 2	No	No
TV 3	No	No
TV 4	No	No
Ring Doorbell	No	Yes
Mobile device 1	Yes	Yes
Mobile device 2	Yes	Yes
Mobile device 3	Yes	No
Google home speaker	No	No
Monitor 1	No	No
Monitor 2	No	No
Keyboard	No	No
Mouse	No	No

Table 2: Servers

Server	**Vital, Critical, Recovered First (Yes or No)**
Home server	Yes

Table 3: Vulnerabilities That Need to be Updated

Vulnerability	**Action Taken/Action Needed**
SMB Signing not required	Enforce message signing in the host's configuration
SSL Certificate Cannot Be Trusted	Obtain a verified certificate

Table 4: Passwords (Roles)

Passwords (Roles)
Admin on Laptop 1
Admin on Laptop 2
Admin on Laptop 3
Admin on Laptop 4
Owner on mobile device 1
Owner on mobile device 2
Owner on mobile device 3

Table 5: Backups That Need to be Prepared and Maintained

Backups
Server

Network
Laptop 1
Laptop 2
Laptop 3
Laptop 4
Mobile device 1
Mobile device 2
Mobile device 3

Table 6: Prioritized List of Components for Recovery

Devices
Router
Laptop 1
Laptop 2
Laptop 3
Laptop 4
Mobile device 1
Mobile device 1
Mobile device 3
Server
Home server
Passwords (Roles)
Admin on Laptop 1
Admin on Laptop 2
Admin on Laptop 3
Admin on Laptop 4
Owner on mobile device 1
Owner on mobile device 2
Owner on mobile device 3
Backups
Server
Network
Laptop 1
Laptop 2
Laptop 3
Laptop 4
Mobile device 1
Mobile device 2
Mobile device 3

When it comes to finding deficiencies in the deliverables, one thing that comes to mind is not being specific enough so that when it comes time to the recovery process, not everything is completed. To resolve this problem, it is best to get with the team (whoever that consists of

within the network) and run through each deliverable to see what can be re-written to where everyone understands clearly. When it comes to a larger organization, it is better to have outside opinions for this specific reason. I have found that sometimes the way our process maps are written within my department at work, I do not always understand what needs to be done. When time is available, it would be beneficial to hear these words and make updates where needed.

What did you learn?

By looking at what could be wrong in the specific deliverables in the results, I have learned that when I am not understanding this same process when it comes to the organization that I work with, something can be said to helps things run more smoothly in the future. I was not sure what all consisted of preparing for a ransomware attack, and it is great to be able to walk through each step and understand why we do things the way they are done.

In the future, this could be beneficial to an organization and the way that the team involved understands things. If no one speaks up about confusing components of the recovery process, this could lead to problems when it comes times to put that process in place. Ransomware attacks are common and vital points can be missed if all components are not maintained and updated regularly. It is better to be preventative vs trying to fix the issues when they come up.