Jane Aldakkour

Ransomware Recovery

Network Management and Information Security

CDIM 6340

To do the right up use the 3-question format:

1. What did you do – in this section tell me what you did to generate the above outputs, be specific. This section is all about how you are doing things, do not put results or outcomes here, just how you did it.

To start this assignment, I went back to my previous assignments and reviewed the results. I also reviewed the reading “An Inside View of a Ransomware Attack Response and Recovery” by Dzimiela and Jennox, as well as the “Ransomware Recovery for Dummies”. I generated the necessary lists using the information from these assignments. These lists included: an inventory of network devices, servers that need to be backed up, devices that need updates, identify passwords that will also need to be backed up, and a prioritized list of components for recovery.

1. What are the results – in this section tell me what the specific deliverables are. Also identify any deficiencies in your deliverables and what should be done to resolve the deficiencies.

Inventory of Network: ￼ Priority List of Asset Recovery: (High to Low)

1. IPhone (Jane) 1. iPhone (Jane)
2. IPhone (Austin) 2. iPhone (Austin)
3. MacBook Pro (Jane) 3. Eeros Router
4. Gaming PC (Austin) 4. Eeros Router (extender)
5. Dell Laptop (Xcel) 5. MacBook Pro (Jane)
6. Smart TV – Roku (Living Room) 6. Dell Laptop (Xcel)
7. Smart TV – Apple (Bedroom) 7. Gaming PC (Austin)
8. Speaker (Living Room) 8. Ring Camera Connection Extendor
9. Xbox 9. Ring Camera (Front Door)
10. Nintentdo Switch 10. Ring Camera (Garage)
11. Playstation 11. Ring Camera (Street Side)
12. Alexa A (Living Room – Offline) 12. Ring Camera (Back)
13. Alexa B (Office) 13. Ring Camera (Front)
14. Alexa C (bedroom) 14. Ring Camera (House Side)
15. Eeros Router 15. Alarm System
16. Eeros Router Extendor 16. Smart TV – Roku (living room)
17. Ring Camera (Front Door) 17. Speaker (living room)
18. Ring Camera (Front) 18. Smart TV – Apple (bedroom)
19. Ring Camera (Back) 19. Xbox
20. Ring Camera (Garage) 20. Playstation
21. Ring Camera (Street Side) 21. Nintendo Switch
22. Ring Camera (House Side) 22. Alexa A (living room)
23. Ring Camera Connection Extendor 23. Alexa B (office)
24. Alarm System 24. Alexa C (bedroom)

The priority list was developed by assessing which devices are most critical in our daily lives. Our phones were determined to be the most critical for many reasons. They can operate without Wi-Fi (only needing a cellular connection), which puts them ahead of the router. They are also the main method we use to communicate with others, which makes them critical to the recovery, as it is vital that we can communicate between ourselves or to those outside our network. Also, many things that need to be accessed can be done through our phones, an example being school. Next, I have the router. It is important to recover the router next, as it is the device which connects all the other devices in the network. The router extender just extends the router’s reach so that that connection is spread across the whole house. Next, I have the computers. My MacBook is first because currently, I have a lot more schoolwork with pressing deadlines than Austin does (he finally started his classes!) which is easiest and best to access through my MacBook. After my MacBook I have the Dell laptop, which was provided to me by Xcel for work. This is also important to recover, however it is not as high on my network’s priority list because the data that is on it is located on Xcel servers and cloud networks. To recover this, I would have to go through Xcel’s IT department to ensure that there is no remaining malware on the device before it is allowed to connect to their servers and recover data. When I am working from home, I must manually connect to the Xcel servers through a program called BIG-IP. This means that most of the time I am not connected and the malware from the ransomware attack would, hopefully, not spread to their network. After the dell laptop, I have Austin’s gaming PC that he has been using to do his homework on, which moved it up the priority list to where it is now.

The next category of devices to be recovered in the ransomware attack are the ring camera system and our alarm system. This is our security system for our house, which provides me with peace of mind. They are not as high of a priority as the items that are necessary for our day-to-day functions for communication, work, and school; however, they are still a high priority for me in terms of recovery because I like to ensure that I know what is happening around the house. The last category of items that I have on the recovery list is what I consider the “entertainment items” which includes the TV’s, speakers, gaming devices, and the Alexas. These are low priority items, as they are not necessary for our daily functions, and are there for fun. The Alexas are the lowest priority items because if they were never recovered, I would not be upset. They are more trouble than they are worth and, in my opinion, a higher security threat in terms of privacy than they are worth. They are also rarely used.

Critical Servers: (High to Low)

1. After double checking with the network administrator (i.e. Austin), I determined that we do not have any servers that need to be maintained.

Components Currently Needing Updates:

1. MacBook Pro (Jane) requires a software update
   1. Microsoft Office has missed several software updates from January 2024 to currently (August 2024)

Maintaining Components Needing Updates:

1. IPhone (Jane)
2. IPhone (Austin)
3. Eeros Router
4. MacBook Pro (Jane)
5. Gaming PC (Austin)
6. Dell Laptop (Xcel)
7. Ring Cameras
8. Smart TV – Roku
9. Smart TV – Apple
10. Xbox
11. Playstation
12. Nintendo Switch
13. Alexas (A, B, and C)

List of backups that need to be maintained:

1. MacBook Pro (Jane)
2. IPhone (Jane)
3. IPhone (Austin)
4. Gaming PC (Austin)
5. Router configuration
6. Ring Cameras

Passwords that require to be backed up:

1. For the Eeros app (for the router)
2. Apple ID (for phones and MacBook)
3. ICloud
4. Microsoft Cloud
5. Gaming PC password
6. For the accounts for the entertainment devices
   1. Xbox
   2. Playstation
   3. Nintendo Switch
7. What did you learn – discuss your takeaways from the assignment, tell me what you learned about ransomware and preparing to recover from a ransomware attack and how you can use it in the future, also discuss how this has value to the organization in the future.

There is a lot to learn about ransomware, preparing for an attack, and recovering from an attack. I learned that ransomware is a type of software that is designed to block a user from accessing a computer system. To work, cybercriminals must gain access – either themselves or through an authorized user – to run the software. Often, cybercriminals that are using ransomware are demanding ransoms from those who they are performing the attacks on (hence the name). The cybercriminals that are using ransomware have become more advanced, and their methods more aggressive. One example of this is the emergence of Ransomware as a Service (RaaS), which is making it so that cybercriminals no longer must write their own malware; furthermore, there are cybercriminals that take copies of all the data that is on a system as well as block access to computer systems, which they can sell or release to cause further harm to the organization that they are performing the attack on. With all of this going on, it is important that organizations and individual users have as many protections as possible in place that they can so that, in the event of a ransomware attack, they can recover their data without paying the cybercriminal(s) behind the attack. The less these criminals can make from doing these attacks, the less these attacks will occur, as it no longer becomes profitable.

The best way to deal with ransomware attacks is to try to avoid them in the first place. This is not always possible, but there are measures that can be taken to do this. People are some of the biggest security threats that there are, as people can be manipulated easily. One way that cybercriminals get access to networks is by social engineering users of a network to download malware unknowingly. Training users of a network to be weary of all downloadable content, clicking links in emails from unknown senders, plugging in USBs that they are unsure where they came from, and so on are some ways that can help to prevent ransomware attacks. Another good way to prevent attacks is to regularly scan your network for vulnerabilities and suspicious activity. Open ports, un-updated devices, and many other vulnerabilities can be detected through doing this. There are many free programs that can be used to perform these scans such as NMAP, Wireshark, Shields Up, and Nessus - each of which brings a different value. To determine the devices on a network, one can use NMAP. To watch the packet traffic on a network (for suspicious activity), one can use Wireshark. To watch for vulnerabilities such as open ports one can use NMAP and Shields Up, and to scan for vulnerabilities such as un-updated one can use Nessus. Open ports allow anyone unfiltered access to establish a connection through this open port – which hackers can use to establish connections send malware to a system. Packet traffic tracking can help ensure there is no suspicious activity on the network by observing the source and destination of packets, as well as the information inside these packets. Nessus is probably the most useful program in terms of vulnerability scanning. It provides so much information about the vulnerabilities on a network, how they arose, and how they can be fixed as well.

On my network specifically, one thing I learned is that my MacBook is that it has many security issues and is probably the most vulnerable device on our network, as well as the device at most risk in terms of a ransomware attack. It is the most vulnerable because, as the Nessus scan showed, it is missing much needed updates on applications as well as its operating system; furthermore, it provides a lot of information to users scanning it (which also appeared in the Nessus scan). There are several applications that appeared in the Nessus scan that could be utilized to initiate a ransomware attack on the network. In terms of recoverability, this device is very high risk. I learned that it has not been backed up since July 2019. The reason behind this is that the “Time Capsule” that it was backing up and that was storing the data lost connection, which was never restored. This Time Capsule is located on another network now (my parents’ network) and is inaccessible currently. To resolve this issue, I will have to use cloud storage to back up my data rather than the time capsule and machine. Knowing this about my network makes me more aware of the vulnerabilities in the network and helps me to eliminate them or keep them controlled if they cannot be eliminated. Continuing these scans helps me stay aware and on top of these vulnerabilities in the future.

Resources:

[1] Solomon, Michael G. *Ransomware Recovery for Dummies*. 2nd ed., John Wiley & Sons, Inc., 2023.

[2] Dzimiela, Casey, and Murray Jennox. “An Inside View of a Ransomware Attack Response and Recovery.” *Blackboard*, learn-us-east-1-prod-fleet02-xythos.content.blackboardcdn.com/5beddfe10b70f/16240335?X-Blackboard-S3-Bucket=learn-us-east-1-prod-fleet01-xythos&X-Blackboard-Expiration=1715191200000&X-Blackboard-Signature=LbqWleBc3ypvIOX9855pRWt1%2BHx6FBZF5DN9YYqh%2B/E%3D&X-Blackboard-Client-Id=101257&X-Blackboard-S3-Region=us-east-1&response-cache-control=private,%20max-age%3D21600&response-content-disposition=inline%3B%20filename\*%3DUTF-8’’9.2%2520PS%2520UPGRADE%2520STUDENT%2520GUIDE.docx&response-content-type=application/vnd.openxmlformats-officedocument.wordprocessingml.document&X-Amz-Security-Token=IQoJb3JpZ2luX2VjEJX//////////wEaCXVzLWVhc3QtMSJIMEYCIQC01%2BnEbqerISuaPhbf/TEEVI8WQIRObNj7iZMfiyDD0QIhAPU2bexIjMJ2zb2Qo6v%2BCbudIUm06Bc2KqGkK7G7s2WVKr0FCO7//////////wEQBBoMNjM1NTY3OTI0MTgzIgx%2BaTEnUTOO8dZACMoqkQW5MqElmcPWE/kquJu7aIbG1lLFfy4Fa03EPczv4GIpWa/K4AM5KBg7vOMSCmCL6BTT5VVxJHtiAv9/T9n5Pad7JYPshFlX93r%2Bsc2fiMB3dWJrUrivEK2SuCknjaeSblXpmrh7JlaiP4wIiHi7wh9HTIkI34zlb0e2me4CtJ5qfwwm6wes15DvExW0vMNhbl1NXw4misiYzO0v4tZz2dcLtBrbVoyoN5tBZ1ZSiT6aE2yBJ2kSYPnB82zVtQrCHZv6CzIUz5TA%2BlSOpk91a9IOjt0A/IPDW96AXZBECbuc%2BTSBfXbGGh7wUJXDR8KflE0wYyhHdELTydU03OH8BZPClt0KGQZlZBvXv0uFMeOd3qFIpOpxZpEgMx6C3%2B5/EiI/5xOqy4mtlt7T7Psc%2BPhRPIhFlZg0WSV1LcN584FefNImEkcD2oZilhKZ5Z0NZ%2BfRX0njFeRTz89KH8q05UWHZW8w6OCUNTafv1EPceRChuTwF65GK2UzE/yvxp4x4LMf3JTJraFrNmkSusxuAaraYCA3ZYPHzVsKjn4PLZ1ZzrbKYKEEoRBNsnT0dJGsjnzWKvbwnVg8ejmQgiunySPL9SGblFo4xl06gtLahs2JBP%2Bu7slZquheqCGVcN2DGz/8WK0nqsK3l3lBTmZESoonLkAEyUW%2BBpmqqvwP5zQ//%2BgEuncHrST33BF36UQO2%2B/SVIJaqk3T6wizJ/LH8dHYWmd4g1vpq1Sdqf/Qp%2BA6N4lWpmae9GIVIOK0tR6zT4c7HkE4uQ7y4jwFGx/WntBjigJKvIbjsBIPjdvxaPdLc5wB2x/Hd5gxbO4uWucsyUkKqUfKEfVDtfr6H2Db%2BlnxJA3V6Tc5RID8HoxGAw3xfQkwlOPtsQY6sAHT78ZI69AicNY1R1TlSCPNprZxA1iWp/6cs4Y6mBqA6AH5Ls3MJ0JINNKFuHWHpxn90oMIJgbxZO8v7rzQLwa5Gew3Y5VKxTvBTvYGOmRVfMmH93bp/w2WPhgBmPtBEokG5oEsO0jxMfraL9uliy2Y/2TprUonesMhX3q1SeIeyybFEYngMbZhJdgs3jSCEUOxgb9/S83zNWlYytYtFgq4cZFLjYM7eTzrIPR/ZumOEQ%3D%3D&X-Amz-Algorithm=AWS4-HMAC-SHA256&X-Amz-Date=20240508T120000Z&X-Amz-SignedHeaders=host&X-Amz-Expires=21600&X-Amz-Credential=ASIAZH6WM4PLTDXAOF6T/20240508/us-east-1/s3/aws4\_request&X-Amz-Signature=5ed7027db50a7dfaba6a370bb0cca723af566a0277eae9eff9c2df7108ad72a0. Accessed 18 Aug. 2024.