Ransomware Recovery Assignment

Jim Kinter

CIDM6340

1. What did you do – To be frank, I struggled with this assignment. The examples provided below are for my home network which really fails to meet the objectives this assignment looks to address. I have managed recovery for a global ransomware attack that involved recovering over two thousand servers and four thousand endpoints. I’m intimately with this exercise and am keenly aware of the implications, cost, impact, and risks associated with both the event, its post-event mitigation, and the lessons learned about effective cyber-security practices and controls to prevent such events. I regret that I don’t have access to a meaningful network to use. I still carry some of the battle scars from our “cyber event” from October 2023 and truly wish that this assignment was for me to recount everything that we had to do to recover from that catastrophic event. With all that being said, I will, to the best of my ability, layout the recovery actions required for my network.

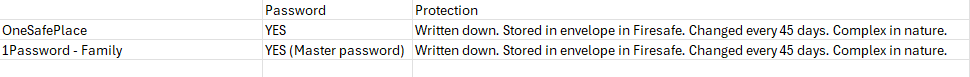
I started this assignment by taking the output of the NMAP exercise, loading all the identified hosts into a table, then scored each item by impact to operations and time to remediate. I chose these metrics because it’s a personal network used by my family. In a scenario where an ongoing commercial operation were impacted, these metrics would differ significantly. Next, I assessed the likelihood and susceptibility of compromise for each host and scored them accordingly. Next, I documented what mitigation practices are in place for each device. Finally, I identified which passwords needed to be backed up, what the protocol is for managing and maintaining those passwords, and how a disaster recovery scenario for any critical systems and passwords would be optimized. As part of the scoring methodology I used the Nessus and ShieldsUp results; however, since there were no significant threats identified by either tool, I was left to assess based on my experience.

The methodology I used to score and, subsequently prioritize recovery follows a 1-5 ranking with 1 being the smallest (least impactful/critical/likely/susceptible) and 5 being the greatest (most impactful/critical/likely/susceptible).

2. What are the results – The current security posture seems adequate. Recovery of all key devices on the network would likely be completed within 3 days and everything recovered within 6 days. This recovery plan is predicated on the availability of power and Internet access. Without both of those most recovery mechanisms are both moot and pointless. I have a weekly cloud backup of both of the personal Windows PCs on the network configure to execute on Sunday nights, and all of the iPhones on the family account are configured to use iCloud backup daily. I store the password to the OneSafePlace online backup in an envelope inside of the firesafe we keep in our master bedroom closet. When I change the password every 45 days, I also replace the password in the firesafe. I also have a family account with 1Password and we use it to store and share key passwords. I similarly store the 1Password master password on paper, in our family firesafe.

A screenshot of a computer

Description automatically generated



3. What did you learn – My key takeaways from this assignment are that my current Defense In Depth approach and routine analysis of the hosts on my home network are sufficient; however, as the threat landscape is always changing I need to remain vigilant and recognize that complacency and acceptance that what I currently have in place is sufficient could lead to future risks.