Austin Cupp

CS462

11/14/2022

In December 2020, the multinational home appliance giant Whirlpool was affected by a ransomware attack that was carried out by the notorious Nefilim ransomware gang, who stole corporate data before encrypting it, and then published the stolen files from Whirlpool that they acquired from the ransomware attack. The data that was leaked included documents related to employee benefits, background checks, medical information requests, accommodation requests, inventory spreadsheets, work charts, plant audit details, and more. The cyber operation has 6 distinct phases incorporated into it. These phases begin with phase 0, which involves having an effective incident response plan that provides the proper guidelines an organisation should take well before a disruptive incident occurs, meaning that the organization should be prepared in case of a ransomware attack. Phase 1 is the deter phase where the crisis is defined questions such as who discovered the breach, what is the damage caused by the breach, is the ransomware attack affecting our operations, and where is the source of the compromise are asked. Phase 2 is the seize phase, where an organization takes steps to mitigate the damage once they have been breached. Depending on the nature of the incident, this could mean taking actions to remove the criminal hacker from your systems or to isolate the already compromised data. Phase 3 is the dominate phase, where the organization establish dominant force capabilities and achieve full spectrum superiority by rectifying the weakness that enabled the data breach to occur. Phase 4 is the stabilize phase, where an organization establishes proper security and restores the services that were affected, in this case, by a ransomware attack. It is important to test the networks, computers, or any functions that were affected by a ransomware attack or other cybersecurity event. Phase 5 is the enable civil authority phase, where the transfer to civil authority and the redeployment occurs. This is the final phase of the cyber incident response plan. This phase also can include the reviewing of the incident and scoping out opportunities for improvement. This is where the incident response team can meet to evaluate parts of the plan that worked and problems within the plan that may have been encountered. The ways to combat ransomware attacks are to perform regular system backups within two different systems, and with different backup methods to have multiple avenues where the information is stored. Network segmentation should also be enacted, which involves dividing the computer network into smaller portions into various subnetworks, which each having own firewall and vlan protection. Regular network security assessments should be performed, which can include vulnerability and penetration testing. Employee security training should take place every so often in order to make sure the employees have the knowledge to either prevent a phishing attack, which can lead to a ransomeware attack as it is deemed a vessel for delivery, or know how to migitate the attack, as well as having the knowledge to migitate a ransomware attack. Another way to combat a ransomware attack is to block several executables and scripts, as they also can be entry point for a cybercriminal to “sneak” in and begin the process of a ransomware attack. The difference however between what was mentioned and the non-applicability of cyber operations on the retail market sector in general, is that the core focus of cyber operations can involve cyber warfare, nation states, and other adversaries. Cyber operations in the module are meant to be aimed towards entities such as those involved or associated with the U.S. Intelligence community.

Sources:

Abrams, L. (2020, December 28). *Home appliance giant whirlpool hit in Nefilim Ransomware attack*. BleepingComputer. Retrieved November 15, 2022, from https://www.bleepingcomputer.com/news/security/home-appliance-giant-whirlpool-hit-in-nefilim-ransomware-attack/

Irwin, L. (2022, October 5). *The 6 phases of a Cyber Incident Response Plan*. GRCI Law Blog. Retrieved November 15, 2022, from https://www.grcilaw.com/blog/the-6-phases-of-a-cyber-incident-response-plan#:~:text=Many%20organisations%20use%20NIST%27s%20Computer,eradication%2C%20recovery%20and%20lessons%20learned.