IPB-Guide
By Damsith Marasinghe

Introduction and overview

I would like to emphasize the fact that weak wireless network can become an entry point for cyber attacks such as malware infections, phishing attempts, or ransomware attacks. Securing your network reduces the risk of becoming a victim of such attacks. The hacking incident involving Yanluowang gang had been an example of a ransomware attack at Wal-Mart. This particular group was snooping around, accessing Wal-Mart web page, exploring the vulnerabilities in the network to see if they can hack and penetrate the web page and the web server. The attackers used an infected file attached to an email to exploit the vulnerability in the network. Phishing is one of the most common methods of delivering ransomware. One of the employees at Wal-Mart downloaded an attachment in a phishing email. When a user downloads a malicious attachment within a phishing email, which contains ransomware, all of the user's files are encrypted and made inaccessible until ransom is paid.

Define the Environment

Wal-Mart servers are IBM servers, which are protected by firewalls, and lack of multi-factor authentication was a major weakness in Wal-Mart servers. There was no antivirus software, which can protect against ransomware and other kinds of viruses within the network and outside of the network. The Wal-Mart view their information security as being monitored 24 hours a day. Servers do have encrypted logins for usernames and passwords. Network switches control Wal-Mart servers, which monitors in and out, traffic within the network. None of the devices can be compromised due the protection layers within the network. These servers do have disaster recovery processes in place in cases of fire or any other natural disasters which may compromise or destroy data and will be recoverable to restore operation.

Describe the Effects

The following has been conducted after the attack about a month ago. Attackers were able to encrypt devices but could not steal any data as part of third attack. They asked 55 million on ransomware but never gotten from Wal-Mart. Attackers said that they stole data from Wal-Mart windows domain server which has been compromised due to the attack. 40 to 50 devices were compromised by this attack but Wal-Mart did not confirm that.

Evaluate the Threat/Adversary

Yanluowang gang wanted to gain access to the Wal-Mart servers and retrieve all the logins and passwords. They were trying access to the network to steal all the data from the Wal-Mart servers and also financial information from the system. The attempts were not possible because of protection layer. Kerberoasting is a method used by hackers to get hold of Windows services accounts and their hashed NTLM passwords. The hash passwords converted into text by using brute-force method and the get the logins elevated access on the Windows Domain. BleepingComputer Security Company had not been able to verify the information that attackers mentioned about the data breach on Windows domain data is really true or not, an had further questions for Wal-Mart.

Determine Threat Course of Action

Employees need to be mindful before click item on suspicious emails or files. I would also recommend having a strong anti malware software in case malware get into network it would block them to protect the network. To protect Windows Domain Controllers there are number of steps that can be taken: Secure domain controllers physically, implement a mechanism to administer domain controllers, limit network access to domain controllers, block internet access, use the most updated version of windows server, implement effective security measures, limit what is run on domain servers and also backup domain controllers.

Summary and Conclusion

Intelligence Preparation in the Environment (IPB) process would help us to mitigate the Risks by the adversary attacks. It would prevent the adversary attacking the Network with Ransomware and taking control of the system. By following security policies and IT Procedures to upgrade / update Operating system & firmware in hardware in time and Avoiding the vulnerabilities from surfacing, risk of an attacker hacking into the servers is also mitigated. Adversary is prevented from breaching into the systems when we have Multi-Factor authentication in place. Employees following the security protocols and Policies would mitigate the risk of having security breaches due to Viruses, Spam, Phishing scam emails and Ransomware, which in turn would prevent taking over the Systems.