Recent DNS Attack Scare and How we Should Secure Systems

Alexei Hooks, anh5653@psu.edu

I am writing to you today to announce that there has been an influx of DNS hijacking attacks within our sector of business. Securing the DNS servers of our company needs to be the of the upmost importance in the near future. The Department of Homeland Security have been alerted "is aware of multiple executive branch agency domains that were impacted by the tampering campaign and has notified the agencies that maintain them" (Kirk). Along with this, both FireEye and Cisco's Talos Intelligence units identified an increase in DNS attacks, especially coming from the Middle East. It is incredibly important to assign team members to increase their security, totally analyzing our domain name systems and auditing the server that host this information. The current DNS attacks allow the aggressors to enter and view multiple information areas about the traffic that flows through the site, who accesses the page, and possibly victimize users with future spoofing attacks. Having access to the DNS of a high priority target such as our company could be advantageous for attackers, so we need to move swiftly in securing any access points that may be vulnerable to potential hijackers.

DNS hijacking attacks are currently being researched and believed to transmit information about email and potential credential information through VPN traffic. With security for our company in mind, we need to take action against the risk of a DNS hijack, as we cannot afford to lose confidentiality with our clients over leaked or stolen credentials. The Department of Homeland Security's Cybersecurity division released statement with possible fixes to decrease risks of being a victim to a DNS hijacking. The cyber division said that it is recommending a secondary DNS server being used to backup and audit that of the initial server. This tactic could allow our company to monitor and locate if our DNS server has been breached in any way, malicious or not. Other tactics being recommended are to require all employees and users to change their passwords, limiting the amount of data that attackers can use against the company. Among the recommendations that the Homeland Security's Cybersecurity division has come up with, their main concern within the government sector is to install and use Two Factor Authentication when accessing the server. The group recommends that these Two Factor Authentication user codes not be sent over any SMS signals, as these can be picked up by aggressors and maliciously used against the company.

The amount of information on this topic is immense as many companies have fallen to DNS hijacking attacks in the past. With this, we are at an advantage, knowing what to do and how to secure our systems from any intrusions through our DNS server. With this information now at our disposal, action needs to be taken by leadership in order to mitigate the potential risk that lay within our systems. Using the recommendations given by government entities, along with in house knowledge and user cooperation, we will be able to secure our DNS server to the best of our ability.

Word Count – 508

References

Kirk, Jeremy, and Ron Ross. “DHS Issues More Urgent Warning on DNS Hijacking.” *Bank Information Security*, https://www.bankinfosecurity.com/dhs-issues-more-urgent-warning-on-dns-hijacking-a-11962.