Article

Hackers identify 6 poorly protected areas in your network commonly attacked

Thousands of hackers travel to Las Vegas annually for the Social Engineering Village at DEF CON to learn about the latest in security research and techniques. Each year the village hosts talks and interactive lessons on human hacking. The following list of data points have been identified by the conference as the ones commonly targeted by hackers. Although these points seem basic, it's important to note that each one is something that's rarely missed during attack attempts.

1. **WiFi Networks:** The connectivity between wireless and internal networks can be a way for malicious attackers to compromise corporate resources. In addition, finding poorly configured wireless networks isn't uncommon, and can turn into another vector for an attacker.
2. **3rd. Party Vendors:** Knowledge gained through interaction with 3rd party vendors create believable pretexts for impersonation through phishing, vishing, and onsite attempts.
3. **Product Information:** General knowledge gained of any internal systems, such as software and operating systems, are used by attackers to exploit any known vulnerabilities.
4. **VPN access:** General knowledge gained of VPN access such as type or name of vendor providing access can alert the attacker of known vulnerabilities.
5. **Organizational Access:** General knowledge gained relating to the use of badges for various levels of access, including doors or systems, can be used to clone counterfeit identification for use in onsite impersonation attempts.
6. **Website Navigation Requests:** Testing the target's willingness to navigate to an unknown website at the request of an unverified individual. This places the corporate network at risk of downloading malware or disclosing login credentials.

Social engineering has become the top attack technique for beating cyber security, replacing exploits of hardware and software vulnerabilities. Estimated global cost of Cyber-Attacks in 2016 is 400 billion and forecasted to increase to 2.1 Trillion in 2019.

Many of the solutions to defend against these attacks may only require a simple change in process rather than costly technology upgrades. 81% of data breach victims, however, reported they had neither a system nor a managed security service in place to ensure they could self-detect data breaches.

If you would like to learn more about what you can do to protect your business, and/or schedule a free assessment of your network, please contact us for a consultation today.