LBMC Information Security Cybersecurity Sense Podcast Show Notes
Author: Bill Dean
Episode: 6
Date: August 29, 2017

The Risks of Remote Access

Background

- Remote access to networks is commonplace in today's IT environments.
    - Remote access is mainly used for IT support, power users, and developers.
- This capability can be provided in a safe and secure manner. It can also be deployed in a manner that leaves the organization at great risk.
- Remote Desktop (aka Terminal Services), when not deployed properly, is a severe risk.
- You have deployed firewalls to internet communication that you deem to be of risk. You also deploy IDS/IPS technologies to detect and block internet traffic into your network that is of risk. Enabling remote desktop bypasses these controls and places you at risk of a system compromise, network compromise, and even a data breach.
- When remote desktop is enabled, attackers can brute force administrator credentials because you can't lock out the administrator account due to excessive failed logins.
    - It is just a matter of time.
- With this access, your entire network could be at risk of compromise and data theft.

Security Affairs Article: 4.1 Million Endpoints Have Remote Desktop Exposed to Internet

- Rapid 7, a computer security software and consulting company, reported that there are 4.1 million endpoints that have remote desktop, also known as terminal services, exposed to the internet.
- 28.8% or 1.1 million are in the United States.
- This number is shockingly high when you remember that this protocol is effectively a way to expose keyboard, mouse, and ultimately a Windows desktop over the network.
- The researchers pointed out that even if RDP is disabled by default on Windows, it is commonly exposed in internal networks for administration and maintenance purposes.
- The protocol poses serious risks, Microsoft addressed dozens of vulnerabilities in the Remote Desktop Protocol over the past fifteen years. Even the NSA has been documented to use zero day exploits on Remote Desktop.
- Remote Desktop Protocol attacks are a privileged attack vector for malware distribution, especially ransomware.

Additional Information

- These statistics are not just for discussion; this is a common, real-world threat.
- LBMC Information Security's incident response practice has worked many successful attacks against remote desktop using brute force password attacks.

- Ironically, we are currently finishing one in which up to nine different attackers had been logging into the server for more than four months.
- When compromised, the best-case scenario is that your systems are turned into Bitcoin mining bots, or maybe the attackers pivot from the compromised system to conduct financial fraud or file-fraudulent tax returns (making it look like it was someone from your organization).
- However, it goes downhill from there. Many manual ransomware infections, after manual deletions of backups occurs, happen in this fashion.
- Unfortunately, we have also had to convey the bad news of data breach situations involving personally identifiable information (PII) and electronic patient health information (ePHI), in which public disclosures were needed.

Protecting Yourself

- Do not permit remote desktop capabilities from the Internet.
- Where possible and remote desktop is necessary, force multi-factor authentication. RSA no longer has a monopoly on this technology.
- Enable Network-Level Authentication to prevent, or at least slow down, brute force password attacks.
- Perform external penetration tests to determine if there are instances of remote desktop enabled in your environment. In every compromise we worked in the past year that leveraged remote desktop, a penetration test would have noted this as a risk with suggested remediation. Odds are, this would have prevented the compromise from occurring.
- If you find that remote desktop has been accessible via the Internet and are concerned, there's a simple way to gauge whether additional analysis is needed.
    - Windows server maintains logging relevant to successful log-ons via remote desktop. It is the Microsoft-Windows-TerminalServices-LocalSessionManager-Operational log.
    - This log provides date, time, account, and IP address used to log on.
    - Using many of the IP geolocation sources, you can look up IP addresses to determine if some of the log-ons are unknown and of concern.

Bill Dean is a Senior Manager at LBMC Information Security. While involved in various aspects of LBMC's security services, he is also the practice lead for the organization's incident response, forensics, and litigation support practice.

References:

https://itunes.apple.com/us/podcast/cybersecurity-sense/id1269195484?mt=2

http://securityaffairs.co/wordpress/62004/hacking/rdp-exposure-report.html

https://security.berkeley.edu/resources/best-practices-how-articles/securing-remote-desktop-rdp-system-administrators

https://fadedlab.wordpress.com/2015/05/23/hardening-microsoft-remote-desktop-services-rds/

http://securityaffairs.co/wordpress/59450/hacking/nsa-esteemaudit-exploit-patch.html

https://www.kaspersky.com/blog/multi-factor-authentication/9669/

https://isc.sans.edu/forums/diary/Implementing+two+Factor+Authentication+on+the+Cheap/9580/

https://www.sans.org/reading-room/whitepapers/authentication/two-factor-authentication-2fa-openotp-36087