Auric Enterprises Threat and Vulnerability Analysis

Michael Bossner

***Abstract*— Realised threats to enterprise level information systems can be devastating to the companies that implement them. It is vital in modern information systems that these threats are identified and appropriate risk analysis is performed. Should the identified threats be cause for concern then controls should be put into place to either mitigate or remove the threats from these systems. Threat and Vulnerability analysis should not be a one off thing and should be constantly updated and performed so that new threats to a system are identified early before major loss occurs.**

I. Introduction

Information and network security are a major consideration when it comes to modern enterprise level systems. When only a single security incident can cost a business tens of millions of dollars in less than a day, the advantages of identifying threats early and implementing controls to reduce the risks of such events becomes evident.

In a survey done by [1] they found that 48% of Australian organisations who participated had experienced a security attack in the past 12 months which is significantly higher than the 33% reported in the previous year. The mining industry is not any less susceptible to such incidents with some examples such as a gold mining company, Goldcorp having 14.8Gb of data published on the internet in 2016 [2]. Or Precision Drilling Corp admitting they detect intrusion attempts almost daily [2].

In this paper I will attempt to identify some major threats and vulnerabilities to the company Auric Enterprises, based on the information that I have been provided by them. I will then recommend some controls to help minimize the risk posed by these threats. The structure of this paper will be as follows. Section II will identify some of the major threats faced by the company and discuss what makes them a threat. Section III will talk about the vulnerabilities and exploits that can be used to realise the threats from section II. It will also discuss the recommended controls to help minimize the risk of such threats being realised. Finally I will finish the paper in section IV with a brief conclusion.

II. Threats in Information Systems

According to [3] a threat is defined as “Any circumstance or event with the potential to adversely impact organizational operations, organizational assets, individuals, other organizations, or the Nation through a system via unauthorized access, destruction, disclosure, modification of information, and/or denial of service.”

In this section I will be discussing the 3 most relevant threats that Auric Enterprises currently faces to its information systems.

1. Loss of Productivity/Denial of Service

As stated by the COO of Auric Enterprises, a loss of production in any of a number of systems can cost the company $5,500,000 a day from expenses and lost revenue. This would constitute as a major risk for the company as there are many attack vectors and the impact of a successful attack would cost the company millions every day.

A loss of production can occur for many reasons from malicious employees sabotaging equipment to distributed denial of service attacks against a company [4]. In a survey done by [1] 46% of participants in Australia found loss of productivity to be a major concern from a security breach making it the largest concern in the list.

2. Data Loss/Tampering

Data loss or corrupted business data is the second major concern on the survey done by

[1] with 42% of Australian stating they find it concerning in the event of a major security breach. One of the most common causes of loss of data is because of malware. Some of the most notable malware attacks causing data loss have been the WannaCry ransomware which encrypts data stopping legitimate users from accessing it [4].

According to the CFO of Auric Enterprises a loss of financial data in the company could cost upwards of $10,000,000 making it a high impact threat that should have sufficient controls to reduce the likely hood of the threat being realised.

3. Loss of Data Confidentiality/Privacy

A loss of data confidentiality can occur from many of the same attack vectors as data loss but the goal is vastly different. Cyber espionage from other companies to employees who have leaked the information for various reasons are some of the motivations behind this threat being realised [4].

According to the CFO a loss of confidentiality on mining product and volume databases can result in losses of $10,000,000 per annum. Another high impact threat that should have controls put in place to reduce the risk to acceptable levels.

III. Vulnerabilities, Exploits and Recommended Controls

In this section I will list some of the most vulnerable attack vectors that can be exploited to realise the threats discussed in the previous section. I will also recommend some controls that will help reduce the threats being realised.

1. Use of a Flat Network Hierarchy

The use of a flat network hierarchy is a major vulnerability in a large information system as once a single part of the network is compromised it leaves the entire network open to attacks with little to help detect the breach [5]. Once the vulnerability has been exploited through any number of means such as social engineering [6], malicious employees or by various malware. All three of the threats listed in section II can become easily realised costing the company tens of millions of dollars [7], [5].

The way to reduce the risk when such a breach occurs is to implement segregation and segmentation across the entire network. By limiting what devices can communicate and how they do so you can hinder lateral movement by intruders through your network and increase the chance of detection in a timely manner [5], [7].

To provide this security each section of the network should be split all the way down to the lowest practical level. The principals used for the networks should be such that if a device does not need to talk to another device then it cannot. Devices that do need to talk to each other should be limited to only the protocols or ports that they need and nothing else [7], [5].

2. Use of Telnet

Telnet is an unencrypted protocol for remotely logging into a networked device over TCP connections [8]. Using unencrypted communication protocols are very vulnerable to eavesdropping by anyone who has the ability to see the flow of information between the two endpoints using readily available tools and little knowledge. An attacker either outside the network or a malicious insider can exploit this vulnerability using packet sniffing to find useful information such as login names and passwords which are being sent in plain text [9], [10].

If a system administrator was to log into the network using a super user account from open Wi-Fi it would become a major vulnerability. Anyone else within range of that signal or who has the ability to see network traffic between his laptop to device he is logging into has the ability to easily see the super user login name and password [9]. This allows for every threat listed in section II to be realised as now a large number of devices can easily obtain full access to the network.

A simple solution to correct this issue would be to use an encrypted remote terminal protocol such as SSH rather than using Telnet. Using an encrypted protocol removes the ability of eavesdroppers to be able to see the usernames and passwords as well as what it is you are doing [10], [9].

3. Use of Insecure Wireless Encryption Standards and Open Wi-Fi

Use of insecure encryptions and open Wi-Fi are major vulnerabilities in a network as they can be easily exploited by packet sniffers [9] and freely available tools designed to break the protocols being used. WEP is a very insecure wireless encryption protocol that can be cracked in minutes using a basic laptop, opening the network to all further attacks that can see all three of the threats in section II realised [11], [12].

Relying on the fact that the open Wi-Fi signals do not reach outside the property is also not a very secure security measure as it still leaves the network vulnerable to insider threats [4].

The solution to this problem is it make sure all wireless communications are only using secure wireless encryption protocols such as WPA2 [11], [12].

4. Insufficient Password Strength

Password strength is determined by the amount of entropy that is contained in its creation [13]. A password such as “auricblackcoalmining” was not created using random words as each word used in the password is very clearly linked to the company and thus vulnerable to attackers who could use current password cracking techniques to guess the password and gain access to the network [13], [14].

To prevent the likelihood of intruders exploiting weak passwords to gain access the staff should be trained in proper password creation techniques and the passwords used should be audited and changed regularly [13], [14].

5. Inappropriate User Access Control

According to [4] in 2018, 77% of business data breaches were caused by insiders. This shows that a large vulnerability in a system is the trusted individuals accessing that system. The users may intentionally or unintentionally exploit the fact that they have access to a system by misusing or mishandling the privileges they are provided [4], [15].

To limit the impact if such an event occurred, users should only be given the bare minimum level of access to the system they need to perform their job. User accounts should also be segregated much in the same way that the network should be. An individual from finance should not be able to access SCADA systems for example. Likewise personal assistants should not have access to the entire system [4], [15].

IV. Conclusions

After an analysis of the information system used by Auric Enterprises it is clear that there are many controls that can be implemented to minimize the risk of some very high impact threats being realized within the company. Information security is always evolving and as such, company’s need to stay ahead of the many threats that can potentially cause major harm to them. It is important that these threat and vulnerability analysis reports are continually updated and change to meet the requirements of the company using them.

References

[1] Telstra, “Telstra Security Report 2019,” 2019. [Online]. Available: https://www.telstra.com.au/content/dam/shared-component-assets/tecom/campaigns/security-report/Telstra%20Security%20Report%

202019%20(1).pdf. [Accessed 23 Aug 2019].

[2] EY, “Does cyber risk only become a priority once you’ve been attacked?,” 2018. [Online]. Available: https://www.ey.com/Publication/vwLUAssets/ey-cyber-in-mining-report/$FILE/EY-cyber-in-mining-report.pdf. [Accessed 07 10 2019].

[3] R. Ross, P. Viscuso, G. Guissanie, K. Dempsey and M. Riddle, “Protecting Controlled Unclassified Information in Nonfederal Systems and Organizations,” NIST, 2016.

[4] H. Kettani and P. Wainwright, “On the Top Threats to Cyber Systems,” *2019 IEEE 2nd International Conference on Information and Computer Technologies (ICICT),* 2019.

[5] ACSC Australian Cyber Security Centre, “Implementing Network Segmentation and Segregation,” 04 2019. [Online]. Available: https://www.cyber.gov.au/sites/default/files/2019-05/PROTECT%20-%20Implementing%20Network%20Segmentation%20and%20Segregation%20%28April%202019%29.pdf. [Accessed 07 10 2019].

[6] K. D. MITNICK, THE ART OF DECEPTION, John Wiley & Sons, 2002.

[7] J. Arnaud and J. W. Wright, “Network segregation in the digital substation,” *13th International Conference on Development in Power System Protection 2016 (DPSP),* 2016.

[8] J. Postel and J. Reynolds, “TELNET PROTOCOL SPECIFICATION,” 3 1983. [Online]. Available: https://tools.ietf.org/rfc/rfc854.txt. [Accessed 07 10 2019].

[9] S. Ansari, S. Rajeev and H. Chandrashekar, “Packet sniffing: a brief introduction,” *IEEE Potentials,* vol. 21, no. 5, pp. 17 - 19, 2003.

[10] SSH, “Telnet - and SSH as a Secure Alternative,” SSH, [Online]. Available: https://www.ssh.com/ssh/telnet. [Accessed 07 10 2019].

[11] Y. Zou, J. Zhu, X. Wang and L. Hanzo, “A Survey on Wireless Security: Technical Challenges, Recent Advances, and Future Trends,” *Proceedings of the IEEE,* vol. 104, no. 9, pp. 1727 - 1765, 2016.

[12] A. H. Lashkari, M. M. S. Danesh and B. Samadi, “A survey on wireless security protocols (WEP, WPA and WPA2/802.11i),” *2009 2nd IEEE International Conference on Computer Science and Information Technology,* 2009.

[13] M. M. Taha, T. A. Alhaj, A. E. Moktar, A. H. Salim and S. M. Abdullah, “On Password Strength Measurements: Password Entropy and Password Quality,” *2013 INTERNATIONAL CONFERENCE ON COMPUTING, ELECTRICAL AND ELECTRONIC ENGINEERING (ICCEEE),* 2013.

[14] L. Bošnjak, J. Sreš and B. Brumen, “Brute-force and dictionary attack on hashed real-world passwords,” *2018 41st International Convention on Information and Communication Technology, Electronics and Microelectronics (MIPRO),* 2018.

[15] F. L. Greitzer, J. Purl, Y. M. Leong and P. J. Sticha, “Positioning Your Organization to Respond to Insider Threats,” *IEEE Engineering Management Review,* vol. 47, no. 2, pp. 75 - 83, 2019.