**Security Baseline Report**

Emani K. Atkins

April 28, 2022

**Security Baseline Overview**

Obtaining a good understanding of the infrastructure of the network will provide foundational tools and strategies when preparing a security baseline. From this baseline, methodology is established, and an attribute report, network security checklist, and risk and vulnerability report will be outlined. These documents will ascertain the security posture of Australia.

**Attribution Report**

IP addresses have been provided to Australia’s cyber team via the host of the summit. There are fourteen IP addresses supplied and the team will analyze the set of addresses to acquire the source of atypical activity taking place on the network of the Global Economic Summit. Within this report, bad actors are to be identified and the effect of the activity on surrounding countries will be discussed.

Upon receiving the IP addresses, AlienVault is the technology used by the team to gain initial information about the suspicious activity. AlienVault is a source created by cyber professionals that provide sharing of resources and information about cyber threats. Ip2nation is another source used to determine information about the IP addresses. Ip2nation is a MySQL database that provides reference to a given IP address. Using ip2nation, the sources of the addresses are displayed in the table below.

|  |  |
| --- | --- |
| **IP Address** | **Country** |
| 7.26.42.136 | United States |
| 190.142.94.44 | Venezuela |
| 113.245.133.236 | China |
| 17.158.163.43 | United States |
| 82.196.6.46 | Netherlands |
| 207.88.46.144 | United States |
| 46.3.152.107 | United States |
| 222.215.134.15 | China |
| 85.209.52.248 | Germany |
| 174.43.217.102 | United States |
| 161.234.248.208 | Venezuela |
| 16.106.9.38 | United States |
| 209.183.236.40 | United States |
| 203.96.22.39 | New Zealand |

In total, it appears that attempted access to the network is from the United States, Venezuela, New Zealand, China, Germany, and the Netherlands. Ip2nation appears to be more unreliable than AlienVault as it is somewhat limited in information it can provide. It also seems to be less accurate as well. Perhaps the use of other varying tools can help to identify more useful information to assist in obtaining information about the anomalous activity.

A cyber intelligence alliance consisting of five countries including Australia make up the Five Eyes Alliance (FVEY). Australia’s engagement with the alliance over time has shifted from a sharing and discussion of wartime intelligence to its general intelligence practices mimicking the United States and the United Kingdom (O’Neil, 2017) . Among the countries of origin discovered to be associated with the provided IP addresses, China and possibly Venezuela and Germany stand out as potentially bad actors. China has been noted as problematic for many of the countries in the FVEY. The aforementioned countries are also the only listed in the table as countries not part of the FVEY. New Zealand has expressed concerns over the past few decades about China’s activity in the South pacific “with regard to apparent cyber security threats and political influence operations” (Gee & Patman, 2021, pp. 41). Concerns over telecommunication security has heightened awareness in the South Pacific. Similar relationships appear to be common amongst other nations participating in the summit as well.

Once a source and more information about potential threats are identified, it is important to outline remediation. This usually includes steps such as strengthening security, documenting, and reporting any findings after an incident. Eliminating the root cause of the threat is an integral part of remediation.

As it has been difficult to reach a solution about the odd activity, it would be unwise to associate it with another nation at the summit. It is imperative that countries participating in the summit disclose their findings and resources among one another to verify that systems are functioning as intended and to protect nations from cyber threats and risk.

**Network Security Checklist**

Ensuring network security is vital to protecting the integrity of data relayed and stored within it. This checklist will draft requirements for operating a secure network within the summit and highlight key components needed to establish a baseline infrastructure. It will also detail important features of the system components configuration and offer methods of protection within the network.

Devices and components on the network to be secured will include

* public-key infrastructure (PKI)
* firewalls
* SSL, IPSEC,
* Virtual Private Networks (VPNs)

The firewalls on the network will filter incoming and outgoing traffic to prevent attacks. This will require rule sets in the form of whitelists to restrict traffic on the firewall. PKIs help systems exchange data over non-secure networks. Major components of a PKI are the certificate authorities (CAs), registration authorities, repositories, and archives. The role of the CA is to identify the senders and receivers. The registration authorities register and issue certificates. Protecting these components will require practicing concepts such as privileged access of inbound and outbound traffic (CISA, n.d.).

The following methods should be applied with the goal of protecting data integrity:

* Multifactor authentication and changing passwords often,
* Cyber training to increase the chance of staff recognizing threats
* Installation of antivirus software
* Organize a catalog of all software, hardware and their locations on the network

Overall, necessary steps to take in securing the network include (Best, 2021):

* Encourage the use VPNs for secure connections
* Patching software in a timely manner to prevent vulnerability
* Create strict policies regarding remote access of the network (BYOD, etc)
* Encourage the use of strong user passwords

Secure cryptographic protocols will also prevent listening and interception from taking place on the network. To keep up with the standard, the TLS protocol is typically used to ensure traffic is encrypted across the network. In terms of account management, network administrators must be sure to catalog all account information of users and provide an agreed upon expiration date.

Overall, ensuring that all communication on Australia’s network is secure is of the utmost importance when deploying in the global summit. This checklist outlines the necessary pieces to solidify Australia’s security. Assimilating the above-mentioned strategies will manage risk threat and risk to the security of the network.

**System Security Risk and Vulnerability Report**

Classifying vulnerabilities and threats to a network will comprise this report to strengthen Australia’s network.The purpose of this report is to issue guidance to show potential weaknesses in the network infrastructure and protect the future defense. This includes an outline to respond to the threats and risks already occurring. Threats to authentication and credentials can include social engineering, PKIs, and leapfrogging.

Social engineering is often a threat due to the ease in which it can be executed. For example, an attacker could send a seemingly harmless email though it contains a link with malicious content that could exploit the system if clicked on. Informing staff about the dangers of this attack can save an organization from financial downfall.

PKIs are important as they verify authentication of senders of sensitive information. The user receiving the message gains a certificate from the CA, who creates the certificate. The registration authority then registers and issues the key to the user. Finally, the repository stores and handles all keys to be used by the nation. PKIs are essential to preventing threats such as a man-in-the-middle attack.

Leapfrogging happens when “a nation bypasses traditional stages of development to either jump directly to the latest technologies (stage-skipping) or explore an alternative path of technological development involving emerging technologies with new benefits and new opportunities (path-creating)” (Yayboke, 2020). Specifically, this can occur with the use of mobile devices compared to a PC and allowing for another form of internet access for users.

Mitigation and remediation are important topics to discuss when outlining risk. Controlling and mitigation of risk can occur by implementing various technologies to reduce the risk of a successful threat. Executing a risk assessment should include the following steps (NIST, 2017, pp.38):

* Identify threat sources that are relevant to organizations;
* Identify threat events that could be produced by those sources;
* Identify vulnerabilities within organizations that could be exploited by threat sources through specific threat events and the predisposing conditions that could affect successful  
  exploitation;
* Determine the likelihood that the identified threat sources would initiate specific threat events and the likelihood that the threat events would be successful;
* Determine the adverse impacts to organizational operations and assets, individuals, other  
  organizations, and the Nation resulting from the exploitation of vulnerabilities by threat  
  sources (through specific threat events); and
* Determine information security risks as a combination of likelihood of threat exploitation of vulnerabilities and the impact of such exploitation, including any uncertainties associated with the risk determinations.

Overall, a major impact to the Australian network is the cost to recover loss sue to a breach of confidentiality, integrity, or availability of sensitive information (NIST, 2017). Threats to a system can include natural disasters or damage caused by insidious bad actors. Controlling risk can include ensuring that certain hardware is stored in a specific environment to prevent damage to materials. This can also look like knowing which parts of a system can be vulnerable to attacks like viruses. Countermeasures often consist of controls used to mitigate damage or eliminate the threat altogether. Staying current with software updates, restricting input in SQL queries, strengthening passwords, and disabling auto discovery are just a few methods used as controls to avoid threats.

**References**

Best, Alexis. (2021). *The quick and essential network security checklist for 2022*. Inspired eLearning. <https://inspiredelearning.com/blog/network-security-checklist/>

CISA. (n.d.). *Security tip (ST18-001)*. https://www.cisa.gov/uscert/ncas/tips/ST18-001

Gee, A., & Patman, R. G. (2021). Small state or minor power? New Zealand’s Five Eyes membership, intelligence reforms, and Wellington’s response to China’s growing Pacific role. *Intelligence & National Security*, *36*(1), 34–50. <https://doi-org.ezproxy.umgc.edu/10.1080/02684527.2020.1812876>

NIST. (2012). *NIST*. Guide for Conducting Risk Assessments. https://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-30r1.pdf

O’Neil, A. (2017). Australia and the ‘Five Eyes’ intelligence network: the perils of an asymmetric alliance. *Australian Journal of International Affairs*, *71*(5), 529–543. <https://doi-org.ezproxy.umgc.edu/10.1080/10357718.2017.1342763>

Yayboke, E. (2020). *The need for a leapfrog strategy*. The Need for a Leapfrog Strategy | Center for Strategic and International Studies. https://www.csis.org/analysis/need-leapfrog-strategy