|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| **Reconfiguration of Network Infrastructure** | | | | | |
| Project Title: | **AWS CyberShift Initiative** |  | Date Prepared: | | **20th of June, 2023** |
|  |  |  |  | |  |
| Project Manager: | **Giuseppe Raciti** |  | Project Sponsor: | **OzCazual** | |
|  |  |  |  |  | |
| Project Started: | **12th of June, 2023** |  | Projected Finish date: | **14th of July, 2023** | |

|  |
| --- |
| **Original Network Infrastructure** |
| The original OzCazual network infrastructure used a simple topology, that consisted of:   * a main router with a pre configured firewall, that was the DHCP server to the entire network. Although the network was subnetted, with LAN and Wi-Fi devices on a separate subnet, the one router was used as the main internet gateway to the ISP * The OzCazual building had open ethernet ports located around the facility, that were all connected to a local ethernet switch. The switch was not configured to allow only the ports being used to be OPEN. * A secondary router was used as a Wi-Fi AP, which although had the ability to be used as another router with additional settings, was set up in AP mode. * The Windows 2019 AD Server and Linux Web Server, were both connected to a switch going to the main router, with the web server allowing possible access to the AD server in the event of an attack. * The main router was not set up using a VPN to the ISP, therefore, was open to multiple vulnerabilities * The Windows 2019 Server had not been setup with any other security features, other than Windows Defender / Antivirus |
| **Reconfigured Infrastructure Details** |
| The OzCazual restructuring.  As shown above, the internal network of **OzCazual** had the following changes:   * The original Windows AD Server and Linux Web Servers were repurposed as on-site backup servers, to serve as a secondary backup to the primary off-site OneDrive backup. * All LAN switches were reconfigured, so that any ports not being actively used were closed for security. * The main router was reconfigured with a secure encrypted IPsec Tunnel to the cloud. The firewall was also configured with higher security rules. * The wireless router was removed, and replaced with dedicated APs around the building. This allowed for more devices such as monitors, phones, laptops, printers and other devices, to access the network with higher bandwidth and speed. * New routers were installed to create DMZ’s that separate LAN, Wi-Fi and the newly assigned backup servers.   All of the new cloud-based environment will be setup, configured and tested **PRIOR** to changes made at the OzCazual facility, which will minimise the impact the migration will have as the system transitions to the cloud.  Once a secure cloud environment is confirmed, the main router of the OzCazual HQ will require a period of downtime. To reconfigure the connection to the cloud system, and ensure secure encryption, VPN IPsec tunnel, and authentication systems can be implemented, SecureNET will organise a proposed downtime during a period the business is closed, or at its least active.  Customers of OzCazual will also be notified of a possible service outage, as the migration could cause disruptions during the transition to the cloud. With the Web Server active during the time of migration, it is expected that there should be no noticeable disruption to the e-commerce website. |
| **New Infrastructure Details** |
| |  | | --- | | Virtual Cloud Environment: | | * Virtual Windows 2022 AD Server * Virtual Linux 2 Web Server | | **OzCazual** HQ Equipment: | | * New routers were installed to segment the network into DMZs and increase security * New wireless APs were installed around the building, provided better Qos | | New Software and Security: | | * pfSense firewall installed as a virtual switch * Snort IDS/IPS intrusion detection software * Sophos Linux firewall and Windows and Linux Antivirus software * Splunk Log monitoring and analysis software * Wireshark real-time log analysis software |   This new infrastructure provides a secure connection from the OzCazual HQ, to the cloud infrastructure.  The Linux Web Server has been configured in a DMZ, in order to separate the e-commerce website from the internal server infrastructure, that attackers could access in the event of a breach.  Each system is protected by their own firewall, IPS/IDS, Antivirus/malware, and log monitoring systems, providing the highest possible security. |

|  |
| --- |
| **Approvals:** |
| |  |  |  | | --- | --- | --- | |  |  |  | | Project Manager Signature |  | Sponsor Or Originator Signature | |  |  |  | | Project Manager Name |  | Sponsor Or Originator Name | |  |  |  | | Date |  | Date | |