Case Study: Network Security at ADVRTS

Date: April 18, 2024
Module: Network Security (CSC3064)
Professor: Dr Kieran McLaughlin
Author of the Report: Laura García Perrín (40438881)
Total Number of Words: 1842

Case Study: Network Security at ADVRTS

Laura García Perrín
Queen's University of Belfast Northern Ireland, UK

Abstract
In the following report I try to evaluate the network infrastructure of ADVRTS, an online marketing firm, highlighting its vulnerabilities in the face of cyber threats like Cactus ransomware. Then, I recommend some security improvements, such as VLAN implementation for better network segmentation, enhanced authentication and remote access policies, among others. These measures aim to mitigate risks and boost the company's resilience against future cyber-attacks.

Contents

1 Analysis of Network Security Threats – General Issues and Cactus Related Issues

In today's changing and growing digital world, the security of network systems has become really important. Whatever happens, the Internet carries many dangers. Cyber threats, like data breaches or sophisticated ransomware attacks, can lead to significant challenges when it comes to secure intellectual assets. ADVRTS, an enterprise specialized in the creation of online advertisements, lacks a clear policy for updating and patching their network devices, which raises some concerns about the security and currency of their network infrastructure, concretely about Cactus ransomware.

1.1 Background Information

The ADVRTS IT infrastructure operates from a single office location with multiple PCs and servers. The network uses two static IPv4 public IP addresses provided by their ISP. A device called a Fortinet 40F (firewall) is used to manage network security, creating a DMZ (a separate, more secure network area) and a private office LAN for internal use. This Fortinet device also allows remote access to the server *Docuware* via SSL VPN. Inside the DMZ, there's a server running *Qlik Sense*, a tool for analyzing advertisement performance and user interactions. This server can be accessed from both the internal LAN and remotely. A UniFi switch manages internal network connections within a private IP range, and the LAN includes a server for managing financial data. Finally, the network is configured to use Google's public DNS service, and most devices are connected via ethernet, though there is also WiFi available for mobile devices and laptops.

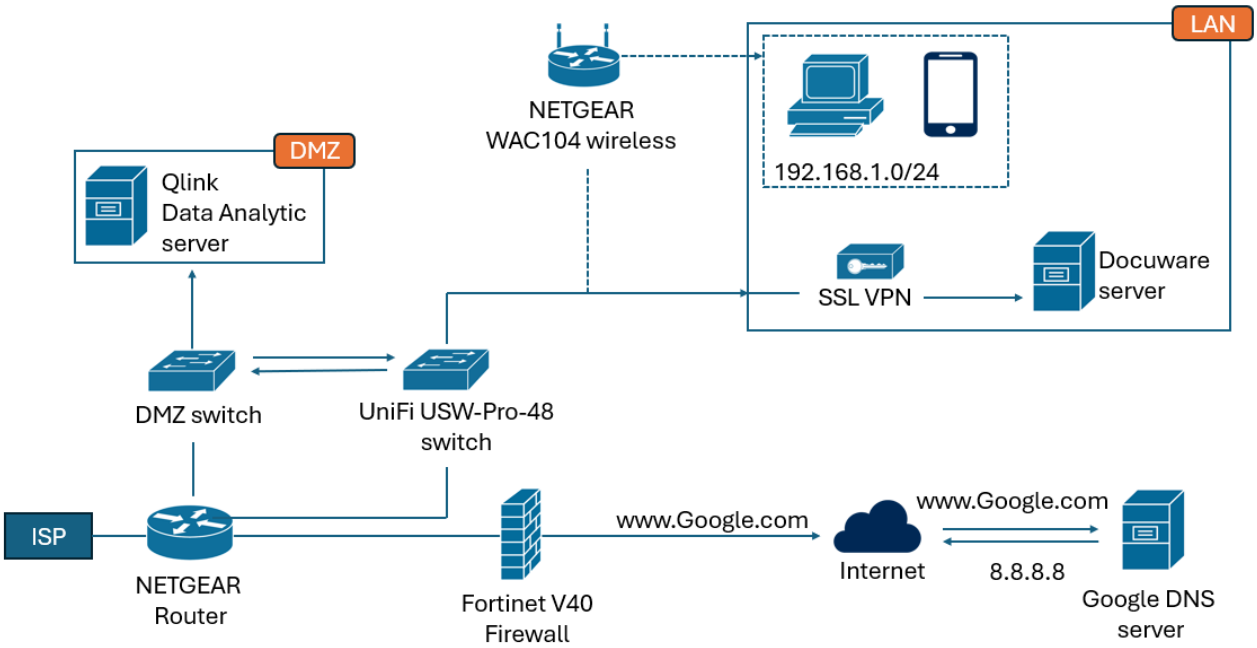

Figure 1: Network diagram showing the possible ADVRT's IT infrastructure

1.2 General Network Issues

Based on the background information, we can appreciate the following general network issues at ADVRTS:

1.2.1 Lack of Update and Patch Management

Without a clear policy for updating and patching, software and systems may be vulnerable to known exploits. The consequences are that attackers could exploit unpatched vulnerabilities to gain unauthorized access, potentially leading to data breaches or the introduction of malware, including ransomware.

1.2.2 Inadequate Remote Access Security

SSL VPN access to the Docuware server without strong authentication and encryption could be a weak point for attackers to exploit. For example, SSL VPN access without robust security measures, such as two-factor authentication, exposes the network to unauthorized access. With unauthorised access, cybercriminals could exploit weak remote access controls to infiltrate the network, posing a risk of data theft or malware infection.

1.2.3 Use of Public DNS Services

Using (or relying on) Google's 8.8.8.8 DNS service could lead to DNS hijacking or interception by attackers, like man-in-the-middle attacks. This vulnerability could redirect users to malicious websites, leading to phishing attacks or malware downloads.

1.2.4 Wireless Security Weakness

The NETGEAR WAC104 may not be configured with the latest security protocols, making Wi-Fi access a potential entry point for attackers. An insecure Wi-Fi network could be an entry point for attackers to launch attacks on the internal network, compromising sensitive data.

1.3 Cactus Ransomware Specific Issues

Cactus Ransomware is a type of malicious software designed to encrypt files on a victim's system, rendering them inaccessible without a decryption key. Like other ransomware, it demands payment from the victim in exchange for the decryption key. However, paying the ransom does not guarantee file recovery, and it encourages further criminal activity.

A notable characteristic of Cactus Ransomware is its method of marking encrypted files with specific extensions or dropping unique ransom notes, which aids in its identification. Moreover, its communication with command and control (C&C) servers is a critical behavior, revealing network-based indicators of compromise that can be pivotal for detection and mitigation efforts.

Based on the information provided, we can appreciate the following Cactus ransomware specific issues:

1.3.1 Phising as a Primary Infection Vector

Cactus Ransomware, like many ransomware strains, often infiltrates networks through phishing emails. ADVRTS's current security posture may not adequately protect against such attacks. In that sense, a successful phishing attack could lead to the encryption of valuable intellectual property, disrupting operations and causing significant financial loss.

1.3.2 Network Segmentation and Lateral Movement

Limited network segmentation could allow Cactus Ransomware to spread quickly across the network if a single device is compromised. The ransomware's ability to move laterally across the network could lead to widespread encryption of files, exacerbating the impact of the attack.

1.3.3 Monitoring and Detection Deficiencies

Without effective monitoring of network traffic, detecting the presence of Cactus Ransomware or its communication with C&C servers becomes difficult. Late detection of ransomware activity could delay response efforts, increasing the damage caused by the attack.

1.4 Severity Risk and Prioriza-tion

The prioritization outlined below is designed to guide ADVRTS in addressing the most critical vulnerabilities first, based on the potential impact and likelihood of exploitation.

- **1.3.1 Phishing as a Primary Infection Vector for Cactus Ransomware**: High severity due to the sophisticated techniques used in phishing and significant financial and reputational impacts. Recommended mitigation includes training and advanced email security tools.
- **1.2.1 Lack of Update and Patch Management**: High severity due to the exposure of multiple vulnerabilities and potential for significant data breaches. A structured patch management process is essential.
- **1.2.2 Inadequate Remote Access Security**: High severity due to increased remote work and the risks of data loss or system compromise. Implementation of robust measures like two-factor authentication is advised.
- **1.3.3 Monitoring and Detection Deficiencies**: High severity because delayed threat detection increases risk of damage. Enhancing monitoring and detection capabilities is crucial for early threat identification.
- **1.3.2 Network Segmentation and Lateral Movement**: Medium-High severity. Poor network segmentation could lead to extensive damage if a threat penetrates; enhancing segmentation is therefore prioritized.
- **1.2.3 Use of Public DNS Services**: Medium severity with a lower likelihood of DNS hijacking compared to direct network attacks. Transitioning to secure DNS services is a straightforward strategy.
- **1.2.4 Wireless Security Weakness**: Medium severity due to localized Wi-Fi vulnerabilities. Upgrading wireless security protocols is recommended, though it has a lower priority compared to direct external threats.

Issue	Severity
1.3.1 Phishing as a Primary Infection Vector for Cactus Ransomware	High
1.2.1 Lack of Update and Patch Management	High
1.2.2 Inadequate Remote Access Security	High
1.3.3 Monitoring and Detection Deficiencies	High
1.3.2 Network Segmentation and Lateral Movement	Medium-High
1.2.3 Use of Public DNS Services	Medium
1.2.4 Wireless Security Weakness	Medium

Table 1: Risk Prioritization for Network Security Protocol

2 Network Security Recommendations

To enhance the security posture of ADVRTS and protect against threats including Cactus Ransomware, the following recommendations are made. These recommendations are rooted in best practices and tailored to address the specific vulnerabilities identified in Part 1.

Figure 2: Key recommendations given in this report in order to improve the network security of the case study.

2.1 Implement Network Segmentation

We can use VLANs techniques to separate critical systems and data from the general network[3]. This strategy aims to mitigate the risk of attacks within the network by dividing it into smaller, controlled segments. For example, we can divide the LAN into different VLANs or segments (one dedicated to the management for network devices, another for the use of guests, etc.), each one of them governed by specific security policies to enhance access control and minimize the impact of potential breaches.

- **Detection and Protection**: Monitor inter-segment traffic for unauthorized access attempts or suspicious patterns.
- **Short-term Mitigation**: Identify and isolate the most critical network assets as an interim measure.
- **Effectiveness**: Significantly limits lateral movement in case of a breach but requires careful planning and configuration.

2.2 Implement Regular Software Updates and Patching to Threats

Establish a formal patch management policy that includes regular scanning for vulnerabilities, prioritization of patches based on severity, and timely application of patches.

- **Detection and Protection**: Use vulnerability scanners to identify and prioritize unpatched systems. Automate patch deployment where possible to ensure timely updates.
- **Short-term Mitigation**: Prioritize patching known vulnerabilities that ransomware like Cactus commonly exploits.
- **Effectiveness**: Ongoing diligence to keep up with new vulnerabilities could mitigate the risk of infection through known vulnerabilities by maintaining up-to-date systems and applications.

2.3 Strengthen Remote Access Security

Implement two-factor authentication (2FA) for all remote access systems, including VPNs,

and ensure that all communication is encrypted[4]. We can achieve this by implementing 2FA in every LAN or DMZ zone.

- **Detection and Protection**: Monitor access logs for unusual login attempts or locations, which could indicate attempted breaches.
- **Short-term Mitigation**: Immediately enforce 2FA for accessing critical systems.
- **Effectiveness**: Highly effective in preventing unauthorized access, though it may introduce slight inconveniences for users.

2.4 Enhance DNS Security Configuration

We can employ another DNS security solutions[2] that use threat intelligence to block requests to known malicious domains, including those related to Cactus Ransomware. For example, we can transition to a DNS service that supports DNSSEC to prevent DNS hijacking and spoofing.

- **Detection and Protection**: Regularly monitor DNS queries for signs of tampering or redirection to malicious sites.
- **Short-term Mitigation**: Use DNS filtering services to block known malicious domains.
- **Effectiveness**: This reduces the risk of DNS-based attacks but may require additional infrastructure changes and user training.

2.5 Deployment of Intrusion Detection Systems (IDS) and Intrusion Prevention Systems (IPS)

We can consider IDS/IPS solutions to detect a wide range of malicious activities by adding an IPS server, an IDS sensor and a management system into the network.

- **Detection and Protection**: This capability is essential in identifying potential threats before they cause harm.
- **Short-term Mitigation**: If a threat is detected, an IPS/IDS can immediately quarantine the affected systems or block malicious traffic, preventing the spread of an attack within the network.
- **Effectiveness**: The number of successful security breaches is generally reduced, as the IPS can stop many attacks automatically.

2.6 Proposed Network Infrastructure

A possible scenario in which the network security recommendations mentioned above apply is described and detailed below, which can be seen in Figure 3:

1. **DMZ Zone**: This is where the Qlink Data Analytic server resides, separate from the internal network to provide an additional layer of security. The server is marked with a 2FA (Two-Factor Authentication) icon, indicating that enhanced authentication is required for access.
2. **Internet Connection**: The network is connected to the Internet through an ISP, and traffic goes through a NETGEAR router and then through a Fortinet V40 Firewall. The Fortinet firewall is likely where security policies are enforced.
3. **Email Security Gateway**: Positioned after the NETGEAR router and that can presumably be positioned before or integrated with the firewall to filter emails for threats and spam.
4. **Intrusion Prevention System (IPS)**: Placed in the network flow to

monitor and protect against network-based threats in real-time.

5. **IDS (Intrusion Detection System) Sensor**: There's a device or software dedicated to detecting malicious activity within the network.
6. **VLANs (Virtual Local Area Networks)**: The internal network is segmented into VLANs, enhancing security and network management. Each VLAN is associated with different departments or types of data handling within the organization, also protected by 2FA.
7. **Switches**: Two switches are labeled for VLAN 20 and VLAN 30, respectively, indicating the ports configured for each VLAN on a single physical switch.
8. **Management System**: This refers to the network management solution, used for overseeing and administering the network infrastructure. It's commonly used when we want to have an IDS/IPS system strategy in our network.
9. **Wireless Access**: There is a NETGEAR WAC104 wireless access point, which provides Wi-Fi connectivity to devices, marked with a 2FA icon that might indicate secured wireless access or management.
10. **DNSSec Server**: The network uses DNSSEC server, a security extension for DNS, which adds a layer of protection against DNS spoofing and other DNS-related attacks.

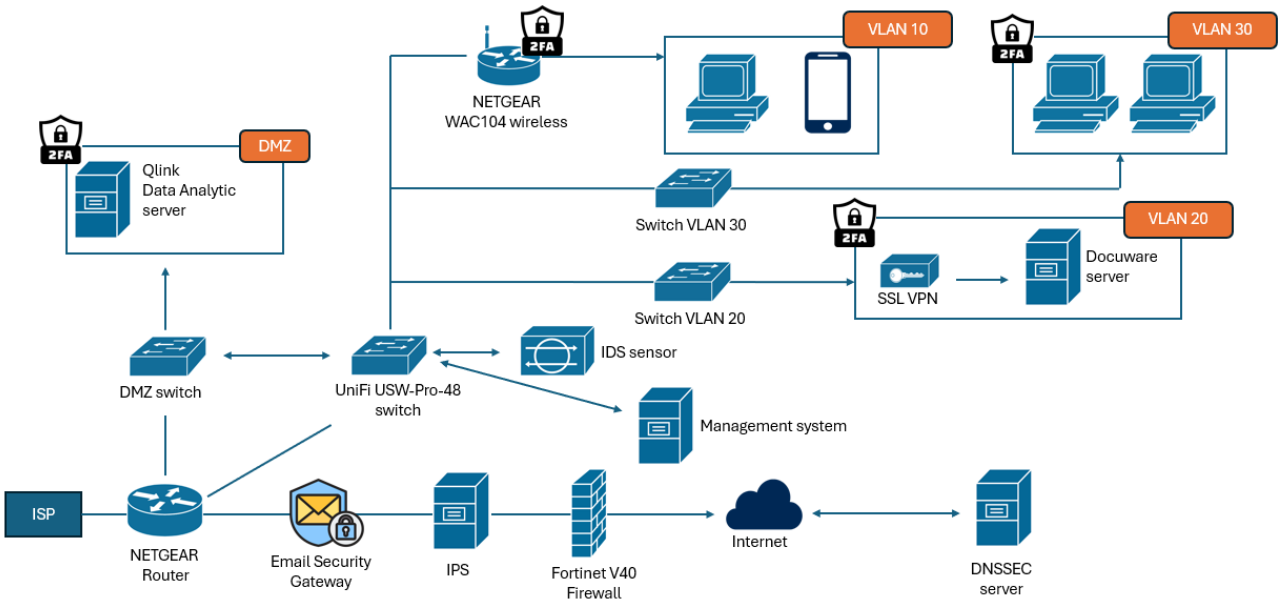

Figure 3: Diagram illustrating a possible network security configuration for the case study, following the recommendations given in *Part 2: Network Security Recommendations*.

I think that the network diagram already incorporates several strong security measures, but there's always a room for improvement. For example, it would be interesting to integrate advanced threat protection systems that utilize machine learning or AI[1] to detect sophisticated attacks.

References

[1] Joe Aucott. How ai will impact cyber attacks and security, 2024.

[2] Chad Kime. How to prevent dns attacks: Dns security best practices, 2023.

[3] Tom Olzak. Vlan network segmentation and security- chapter five, 2021.

[4] Linda Rosencrance. What is two-factor authentication and why is it used?, 2024.