Security Incidents Report

Greenham House Asset Management

Colin Cooper
R00240295
Security Architecture (COMP 9080) 2022/23 - Assignment 2

1) Executive Summary

Greenham House Asset Management was recently the victim of two separate IT security breaches that resulted in significant business, reputational and financial impact. In the first attack, an external malicious actor was able to compromise a web server and use it as an entry point to the company's network to breach a critical database server containing business-critical data. This data was exfiltrated and encrypted in an attempt to extort payment from Greenham House. In the second attack, it appears that an internal malicious actor accessed sensitive files that were stored on a file-sharing server and sent them without permission to a journalist.

The company's IT and network infrastructure has evolved from a simple single-office to a multi-office configuration in line with the rapid expansion of the business. With limited IT staff capacity, priority was given to supporting business growth over initiatives to re-assess and re-configure this infrastructure. This resulted in critical weaknesses that were exploited on multiple occasions by both external and internal malicious actors.

To significantly improve the company's security posture, this report focuses on the state of Identity and Access Control, the role of Threat Prevention technologies to block future attacks and Threat Detection technologies to detect attacks that have breached Threat Prevention system controls.

It is recommended that the company:

- Improve identity and password policy by introducing multi-factor authentication for internal stakeholder, replacing all shared-password systems such as the highly vulnerable office WiFi system, and introducing group policy settings to ensure only strong fresh passwords are in place for both internal and external stakeholders.

- Harden our cybersecurity Threat Prevention suite to include threat blocking at the email gateway. The company needs to adopt anti-malware software that includes Host Intrusion Protection (HIPS) features and is up to date with the latest threat definitions on all Windows, Linux, Mac and mobile operating systems that connect to the company infrastructure. Network Intrusion Protection (NIPS) software to detect and block malicious network traffic; and additional firewalls to support the network architecture and design recommendations from the previous report.

- Improve our ability to detect and react to suspicious events within the IT infrastructure by partnering with a managed service provider for SIEM and XDR capabilities. To detect anomalous, unexpected behaviour within the IT infrastructure, internal honeypots should be deployed to quickly detect anomalous behaviour. Honeypots are seemingly attractive targets for attackers, but actually have no operational value other than to serve as a warning signal to the SIEM / XDR system when accessed by a malicious actor.

The overall incremental cost of this implementation would be in the region of €76,000 per year which compares favourably to both the company's annual profits and revenue, as well as the alternative costs of a security breach (as Greenham House has now experienced).

Table of Contents

2) Introduction

2.1. Background

Greenham House is a specialist asset management company that focuses on investment funds related to renewable energy, energy storage and commercial forestry. It has evolved from a small company with less than a dozen employees located in Cork to over 150 employees who work in offices in Cork, Dublin, and the UK – as well as remote working.

The company currently has €730m of Assets Under Management (AUM) on behalf of institutional and private investors. In 2022 it had a core net income of €7.44m that translated to an operating profit of €2.64m.

	2021 (€m)	2022 (€m)	Change
AUM	658.00	730.00	+11%
Net Income	4.62	7.44	+61%
Adjusted Operating Profit	1.38	2.64	+91%

Greenham House's IT infrastructure is primarily based in a self-managed data centre within its Cork office that contains the company web, email and database servers as well as being the hub for its network infrastructure.

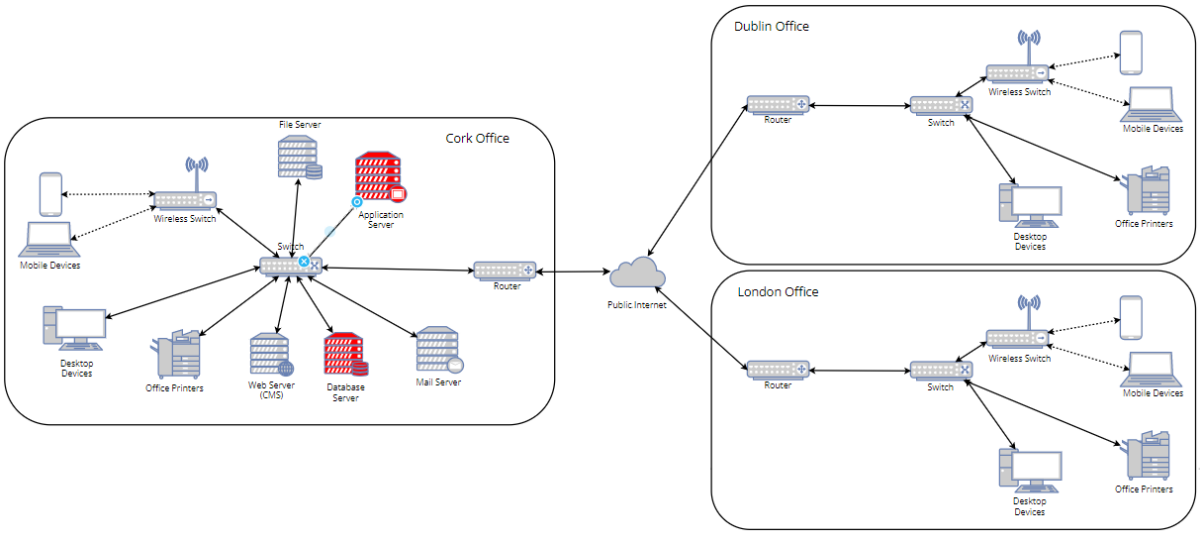

Figure 1 - Greenham House's current network design

Figure 1 shows the high-level network architecture at the time of the security breaches in 2022.

2.2. Purpose

The purpose of this report is to:

1. Appraise the effectiveness of Greenham House's Identity and Access Control (IAC) mechanisms, looking at how different groups identify themselves and gain access only to those internal company systems to which they are entitled
2. Make recommendations regarding the application of cybersecurity controls and technologies that could be used to
    - Prevent a cyberattack
    - Detect and respond to a cyberattack
3. Perform a high-level cost analysis of the products being recommended to address the Threat Prevention and Threat Detection challenges faced by the company

3) Report Body

3.1. Effectiveness of Identity and Access Control Mechanisms

3.1.1. Stakeholders and Noted IACM weaknesses

It is critical that the company can confidently and correctly identify who (subject) is accessing its technology assets. It is also critical to ensure that once identified, the requesting subject should only be able to access those physical assets, services, and data (objects) to which they are entitled in the appropriate conditions (environment).

> *"Identity proofing establishes that a subject is actually who they claim to be. Digital authentication is the process of determining the validity of one or more authenticators used to claim a digital identity. Authentication establishes that a subject attempting to access a digital service is in control of the technologies used to authenticate." - NIST Special Publication 800-63B* [5]

Greenham House has two main categories of subjects who need to be confidently identified:

- **Internal stakeholders**: These include employees and contractors within different departments such as HR, Customer Relations, and Investment Management. These groups have different needs from the IT environment. Even within those groups, different individuals need different privileges – for example, the Director of Investment Management needs access to different investment portfolios, while individual Investment Managers need access only to their own assigned accounts.

Today, internal stakeholders are identified and authenticated through a domain username and password. When accessing the company internal network from non-company locations such as employee homes, hotels or customer sites, internal users must use a Virtual Private Network (VPN) client to create a secure communication "tunnel". The VPN client authenticates with the VPN server using the employees Active Directory username and password (single factor authentication). Greenham House does not currently enforce minimum password complexity or length requirements and does not check for password age or historic re-use.

- **External stakeholders:** These include private and institutional investors who need information about their investment performance and the ability to make changes to their portfolios. Other external stakeholders include third parties who are contracted to manage physical assets such as commercial forests, wind farms and solar farms. All IT services available to external stakeholders are on publicly facing web servers and do not require access through a VPN system. These web servers render information that is stored on back-end database servers. Users are authenticated using email addresses and passwords that are stored in the databases. Passwords are not stored in cleartext but are obfuscating using a one-way hashing algorithm known as "MD5". To authenticate the user, the website checks that the hash value of the password presented by the user matches the hashed value stored in the password field of the database table. This means that Greenham House does not directly store any customer passwords, but only a representation of that password that is difficult to reverse engineer.

As noted in the previous network architecture report, the company also uses an internal Wi-Fi access point to allow employees to connect wireless devices when at the office. This network utilized a common shared password to control access.

3.1.2. Recommendations: Improving Identity and Access Control Mechanisms

- **Replacement of Wi-Fi access point with Active Directory based authentication.** The use of a simple common, shared password for access to the internal network represents a significant hole in the security posture of Greenham House. The presentation of a correct password for Wi-Fi access does not identify who is presenting that password to add a device to the internal network. Replacing this access point with one integrated with the company's Active Directory authentication will at least allow accurate identification of the account being used.

- **Improved Password Policy.** For all stakeholders, a minimum password complexity should be introduced. Forcing minimum password lengths, non-alphabetic characters, and a mixture of upper-case and lower-case characters would significantly reduce the risk of password guessing and dictionary attacks by malicious

actors. For internal users, group policies can be applied to achieve this as well as applying maximum password age requirements[1] and disallowing re-use of old passwords. To prevent brute force authentication attacks, accounts should be automatically locked when a login fails to be correctly authenticated more than 5 times in a row.

- **Improved Password Hashing for Web Applications.** The MD5 hashing algorithm is used to convert clear text passwords into a fixed-length representation (hash) of the password without needing to store the password itself. It is difficult to reverse engineer passwords from the hash. However, MD5 has been found to have extensive vulnerabilities and is no longer considered to be a secure hashing algorithm [1]. Replacing the MD5 system with SHA256 and implementing a "salting" function when hashing passwords would significantly improve the security of password storage and reduce the possibility of password exposure through dictionary attacks where an attacker uses a known dictionary of hashes to lookup the cleartext password.

- **Introduction of Multi-Factor Authentication.** Username and password authentication is a form of single-factor authentication that is based on something only the authorised entity should know. The largest weakness with username and password authentication is that once the information is shared (deliberately, or accidentally through social engineering for example), it is no longer reliable as an identifier. By adding an additional factor such as "something we have" to "something we know", it means that even where one authentication factor (the password) is compromised, a malicious actor would still need to get access to the "something we have". It's possible for "something I know" to be disclosed to an attacker. It's possible for "something I have" to be lost or stolen. However the likelihood of both things happening at the same time is much smaller than then risk of either one happening individually. This increases the difficulty of a successful authentication attack exponentially. In this case, using a hardware or software token to generate one-time passwords would be appropriate. To further improve the security of a software-based one-time-password authentication layer, the company should avoid push notifications, as "MFA fatigue" can lead to users blindly accepting these even when they are not expecting them [2].

  While Greenham House could consider factors such as biometric information ("something I am"), storing such information does come with significant additional responsibility and cannot be reset if compromised.

[1] There is some debate in the industry around the value of forcing users to change their passwords regularly. Microsoft remove the password-expiration policy from their v1903 security configuration baseline settings. When an interval is too long, if a password is disclosed an administrator will want to reset in anyway and not wait for password expiration. When the interval is too short, users tend to make "small and predictable alterations to their existing password" – making them guessable [4].

3.2. Application of Cybersecurity Controls and Technologies (Prevention)

Prevention technologies are designed to block actions that are indicative of threats. Current preventative security controls mainly consist of externally facing firewalls at each office location and anti-malware clients on all Windows Operating System devices. Compliance with malware signature updates is not monitored and the company does not have a documented policy for anti-malware solutions for Mac, Linux or mobile OS devices.

The following recommendations should be implemented to improve that security posture:

- **Introduce a Managed Cross-Platform Anti-malware Policy and Solution**: The company currently has a policy of enabling Windows Defender on all managed Windows devices. It is recommended that the company introduce a solution to monitor compliance to policy to ensure that users are not disabling their endpoint anti-malware and that they have the latest malware detection updates installed. It is also recommended that the security policy require anti-malware software for both managed and unmanaged non-Windows devices that connect to the company LAN – either through VPN or directly at office location. Devices that do not meet the minimum anti-malware security posture should not be permitted to connect to VPN or directly to the LAN. It is recommended to use Trellix Endpoint Security as this is a cross-platform anti-malware solution with advanced capabilities that also include Host Intrusion Protection System features. Trellix ePolicy Orchestrator should be used to manage endpoint security policy compliance.

- **Introduce Email Gateway Anti-malware:** Email is a common means of introducing threats to an internal network. An email gateway anti-malware solution can inspect incoming and outgoing email for signs of malicious activity such as phishing, ransomware, business email compromise (BEC) and malicious attachments by using threat intelligence feeds of URL and IP reputation, malware signatures, heuristic detection methods and advanced sandboxing techniques to analyse potentially malicious files. Emails that are deemed to be potentially malicious can be dropped before reaching an employee. It is recommended to deploy Trellix Email Security software to meet this security need. This solution leverages threat intelligence to provide prioritised alerts to help threat analysts respond to attacks.

- **Introduce both Host and Network Intrusion Prevention Systems:** An intrusion prevention system can either be host-based (HIPS) on network-based (NIPS). Some enterprise anti-malware vendors now bundle HIPS features into their anti-malware solutions [3]. To simplify endpoint management and reduce potential contention on the endpoints between different product vendors, Greenham house should choose such a unified solution. The company should also introduce a NIPS solution close to external network entry points. This will allow the company to detect and block patterns of malicious network activity over-and-above what can be blocked by the traditional firewalls. The NIPS solution must be able to scale to analyse network

traffic in real-time without meaningful impacting on network performance. It is recommended to use Trellix Endpoint Security for HIPs functionality and Snort for NIPs functionality.

- **Add a Web Application Firewall (WAF):** A WAF is an additional layer of security of web applications. A WAF can protect web servers from attack by filtering http/s traffic and reacting to malicious patterns of behaviour. Our web server is a critical piece of infrastructure for our customers and partners to do business with us. For Greenham House it is recommended that we purchase a protection plan with Cloudflare that includes customizable WAF rules and DDOS attack protection. One additional benefit of using Cloudflare is that it allows the company to hide the web server's true IP address, making reconnaissance for attackers more difficult.

- **Additional Firewall Controls:** As noted in my first report, the network design did not segment externally facing assets such as web servers from the internal local area networks. Externally facing systems by their nature are more exposed to threats coming from outside the company's network and so should be separated from the rest of the internal network by a firewall with restrictions that allow only expected traffic using allowed protocols and ports. All endpoints should have Windows Firewall enabled and configured.

- **Ongoing User Training:** While technical solutions can help to protect Greenham House's IT infrastructure, employees need to be vigilant and aware of their roles in preventing cyber-attacks. These "soft" solutions include training on how to recognise signs of social engineering attacks and ensuring they are aware of the company's security policies and how to report suspicious emails, phone calls or other communications.

3.3. Application of Cybersecurity Controls and Technologies (Detect & Respond)

While prevention technologies are designed to block threats from entering or being triggered on the IT infrastructure in the first place, it can never be assumed that these controls cannot be breached. Detection technologies assume that prevention controls can be breached and are designed to detect anomalous behaviour that should be investigated as being signs of active threats in the infrastructure.

While Threat Prevention technologies can be quite binary in their reaction ("block or don't block"), detection technologies usually take a risk-based measurement of actions that are seen and help to prioritise what should be investigated. A baseline of "normal" behaviour is often useful for detection technologies. For example, a correct password and MFA authentication from an Irish IP address between 8am and 9pm on her company laptop might be normal for the company's CEO. However, the same action at 2am from an unknown device from an Australian IP address should be cause for investigation.

The following recommendations should be implemented to improve that security posture:

- **Use a Managed SIEM Solution:** SIEM (Security Information and Event Management) solutions are designed to collect and collate logs and other forms of data from across the IT infrastructure, providing unified visibility across email gateways, firewalls, anti-malware solutions and Intrusion Detection / Prevention tools. These solutions provide holistic views of activities across the infrasturcture, but often require massive amounts of data storage, computing capacity to make sense of the data and create insights for action, and an internal organisation that can configure, use and react to the SIEM alerts. These solutions have therefore been often considered too expensive for medium-sized organizations like Greenham House. An alternative to natively-managed SIEM is to use a Managed Detection and Response (MDR) Service where an external vendor uses economy of scale to provide SIEM services to multiple customers at a reduced price. It is recommended that Greenham House implement a solution based on Rapid 7's Managed SIEM offering.

- **Use Intrusion Detection System**: As mentioned in Section 3.2, it is recommended that Greenham House introduce both host- and network-based intrusion prevention system. Intrusion Prevention solutions also provide Intrusion Detection features, so not additional solution is required for the these.

- **Deploy Honeypots and Honeynets:** A relatively cheap but effective Threat Detection solution is to use honeypot and honeynet systems. These kinds of systems are designed to do no actual operational work or to be accessed by employees or other IT infrastructure assets. They therefore have a very simple "normal" behaviour baseline. Deviation from that baseline is easy to detect, less likely to be operational "noise", and likely to be as the result of malicious behaviour that should be investigated.

3.4. Cost Analysis

Solution	Indicative Cost
Trellix Endpoint Security (including Host Intrusion Prevention / Exploit Prevention features)	€100 per host per year Total €30,000 for 300 endpoint licences (assume 2 per employee on average)
Trellix ePolicy Orchestrator	Total €9,000 for one instance per year
Trellix Email Security	Total €4,000 for one instance per year
Network Intrusion Prevention: Snort	Free for sensor installation €400 per sensor per year Total €4,000 for 10 licences
Windows Firewall (Host)	Free
Rapid 7 Insight IDR (SIEM / XDR)	€72 per device per year Total €21,600
Honeypot / Honeynets	Running costs for 5 honeypots, c. €1,000 per year Total €5,000

Web Application Firewall – Cloudflare	€2,400 per year
TOTAL	€76,000 per year

4) Overall Conclusions

Greenham House's IT infrastructure security is currently vulnerable due to weak Identity and Access Control mechanisms that include shared passwords, weak passwords and single-factor authentication that is vulnerable to dictionary attacks, brute force attacks and social engineering. Improving policy and forcing the use of strong, regularly-changes passwords and adding an additional layer of authentication for internal stakeholders would significantly mitigate against the risk of these kinds of attacks.

Greenham House does have some rudimentary Threat Protection technology, but there are significant gaps on Linux, MacOS and mobile platforms and no policy enforcement to ensure protection features are enabled and up to date on Windows platforms.

The company's security posture would be strengthened by the hardening of the existing anti-malware system, and expanding protection features to the email gateway through scanning and blocking of incoming email for attached threats and phishing attempts. A Web Application Firewall would help to protect the company's public web server from web application attacks such as SQL injection, cross-site scripting, brute force password guessing and path traversal attacks.

Greenham House does not have a scalable Threat Detection capability today. The point at which a threat is detected is after damage has been done. Improving that Threat Detection capability requires investment in a SIEM which can be made affordable to this medium sized business by partnering with a Managed Detection and Response provider. Additionally, simple but effective use of honeypot systems within the architecture will help provide "tripwires" for early detection of threats.

5) Bibliography

[1] A. Sotirov, M. Stevens, J. Appelbaum, A. Lenstra, D. Molnar, D. A. Osvik and B. d. Weger, “MD5 considered harmful today,” 30 Dec 2008. [Online]. Available: https://www.win.tue.nl/hashclash/rogue-ca/.

[2] L. Jenkins, S. Hawley, P. Najafi and D. Bienstock, “Suspected Russian Activity Targeting Government and Business Entities Around the Globe,” Mandiant, 6 Dec 2021. [Online]. Available: https://www.mandiant.com/resources/blog/russian-targeting-gov-business.

[3] “McAfee Endpoint Security 10.6.0 - Threat Prevention Client Interface Reference Guide - Windows,” Trellix, 28 1 2019. [Online]. Available: https://docs.trellix.com/bundle/endpoint-security-10.6.0-threat-prevention-client-interface-reference-guide-windows/page/GUID-3D9AB771-0415-45C5-B62A-1EC74738BAB8.html.

[4] F. Y. Rashid, “Decipher - Security news that informs and inspires,” Duo Security, 2022. [Online]. Available: https://duo.com/decipher/microsoft-will-no-longer-recommend-forcing-periodic-password-changes.

[5] Y.-Y. Choong and K. K. T. M. F. Greene, “NIST Special Publication 800-63B,” US Dept of Commerce, 2017.