CLIENT CYBERSECURITY

SYSTEMS SECURITY ASSESSMENT

JASON M. STARR

Contents

1. IT Security Program Policy Review

1.1 Document Structure

This policy review will comment on specific sections of CLIENT's Information Technology Services' Information Technology Security Program Policy. The comments will address any gaps or recommended modifications, including recommendations for compliance with the General Data Protection Regulation (GDPR). Lastly, the document will include specific information regarding the GDPR and how it may apply to CLIENT.

1.2 Scope and Purpose

It is recommended that the scope and purpose address the information collected from CLIENT employees, candidates, and any data gathered from marketing. Because CLIENT markets to an international audience, CLIENT must meet the security requirements and regulations of the GDPR. The current policy defines "constituent" as "[redacted]". This definition should be expanded to include data subjects with an indirect relationship with CLIENT. As explained previously, marketing data may include information about candidates and interested parties that may be protected under GDPR.

Furthermore, it is recommended that the current definition of confidential and/or sensitive information specify what may be considered as PII or PHI. Personal data, under Article 4 of the GDPR, includes information related to "an identified or *identifiable* natural person". I emphasize "identifiable" because data may contain identifiers that can indirectly identify a person. Therefore, a single data set may not be classified as PII or PHI, but when combined with other collected data, lead to identification of a data subject.

1.3 Information Technology Security Program Coordinator

The current policy defines the duties of this role well and meets the requirements of a Data Protection Officer as defined by the GDPR. However, it should be considered whether the role is fulfilled by the CIO. This role may be better suited for an employee who is less dependent and affiliated with CLIENT's Information Technology Services. The GDPR recommends that the data protection officers be able to perform their duties and tasks in an independent manner.

Relevant GDPR articles:

- Article 37 – Designation of the data protection officer
- Article 38 – Position of the data protection officer
- Article 39 - Task of the data protection officer

1.4 Cybersecurity Program Measures

It is recommended that this section of the policy include a description of ITS configuration and change management. Change events can be both planned and unplanned as a reaction to compliance

requirements, infrastructure problems, or for internal improvements. Nevertheless, change events are a regular function of the IT infrastructure. Therefore, the policy should mention the methods and procedures used to handle the changes that aim to minimize the impact of any related incidents.

An organization's ability to adapt to IT operational risks—often referred to as *operational resilience*—is an important part of any IT security program. That is why having an established configuration and change management process is necessary when working towards maturing the security posture of the organization. Because an organization will inevitably add, modify, and eliminate information or technology assets and supporting infrastructure, a process for controlling and approving such changes is needed.

In response to the GDPR, it is also recommended that Training and Awareness include a program with the goal of improving GDPR readiness. Training could be in the form of an online course that teaches participants to better identify personal data and to know how to control data processing. The online lessons should cover how to perform the following tasks in compliance with GDPR:

- Obtaining consent from data subjects
- Manage consent withdrawal
- Recognize and respond to possible data breaches
- Understand and realize data protection impact assessments

1.5 Incident Response

It is recommended that the section on the notification of security incidents, especially incidents involving breach of data, detail acceptable time spans for which notification should occur. The policy should emphasize the need for notification to occur without undue delay.

The policy sets the minimum for what notification to constituents should include. It is recommended that in addition to the current minimum information, constituents also be notified of the likely consequences of the personal data breach.

1.6 Section for Remote Work

To address the increase in the number of employees working remotely, the need for a separate policy that targets the management of remote employees also increases. The way in which protected information and technology assets are managed will likely be different for these programs as compared to traditional programs. It is important to identify the unique risks associated with remote employees and how their data is managed. For work requiring live communication and team collaboration, the risks associated with the new tools and software needed to support these functions will need to be addressed.

1.7 GDPR and CLIENT

As defined by the GDPR, CLIENT is the data controller, as it dictates what is done with data. CLIENT can also be a processor. For example, CLIENT may have a partnership with other [redacted]

For CLIENT to comply with GDPR regulations, the information management and transparency obligations imposed by the GDPR must be met. These obligations include implementing data protection safeguards, processes for allowing data subjects control over their personal data and their "right to be forgotten", and meeting GDPR's data breach notification requirements.

To comply with GDPR regulations, the policy should state that data subjects have the right to:

- Access their data
- Right to erasure
- Rights to restrictions on data processing

CLIENT data effected by the GDPR

- Personal data of employees who are foreign nationals
- Human resources data for E.U. employees
- Data collected from potential hires (marketing data)

How CLIENT falls under GDPR jurisdiction

- Recruitment and acceptance of applications from hires located in the EU
- Employees that participate in branches located in the EU.
- Conducting research with personal data sets from the EU.

Compliance Tasks

- Develop a GDPR data registry, and document relevant data flows.
- Have clear purposes for data processing and the legal grounds for doing so.
- Create and implement privacy statements for impacted processes.
- Begin developing a sustainable ongoing GDPR compliance program.

2. Internal Vulnerability Assessment

2.1 Executive Summary

The following assessment was conducted for the purposes of providing CLIENT with information to aid in improving the security of its internal systems. Under the guidance and with the support of CLIENT information technology instructors and staff, the assessment occurred during the last week of July 2019. A machine on the CLIENT internal network running Windows 10 was remotely controlled and used to scan internal systems.

With limited access, systems controlled and patched by third party vendors were targeted as highest priority. The system scans revealed high occurrences of network related risks. The remote devices scanned ran EXAMPLE OS. Many of the high-risk vulnerabilities were detected by plugins in the EXAMPLE family. Although it was common for these vulnerabilities to be medium to critical risk level, it was rare for the plugins to confirm the presence of the vulnerabilities on the devices.

The most common vulnerabilities detected and confirmed were related to SNMP communication. SNMP scans identified remote hosts with an open UDP port 161. Further investigation into these SNMP servers revealed certain poor security practices. SNMPv2c is the protocol version being used and is known to be less secure than SNMPv3. SNMPv2c and early versions do not authenticate and encrypt payloads. SNMPv3 replaces the clear text password sharing used in SNMPv2c. Furthermore, the SNMP servers were using the default community name. This allows attackers to gather information about the host and possibly modify its configuration. Lastly, the scan revealed that the SNMP daemons were affected by a vulnerability that can allow a reflected distributed denial of service attack. Leaving the default 'public' community string increases the risk of the SNMP servers being used in a reflected DDOS attack. Once identified, attackers can use GetBulk requests against these devices to create a large amount of malicious traffic.

The Nessus scans also revealed that the same set of hosts were running a Telnet server over an unencrypted channel. Therefore, sensitive information such as logins, passwords, and commands are transferred in cleartext. Transmitting traffic in cleartext allows a remote, mam-in-the-middle attacker to eavesdrop on a Telnet session to obtain credentials or modify the traffic exchanged between a client and a server.

2.2 Methodology and Approach

Remote access was configured to allow for a scan of a range of hosts on CLIENT's internal network. A machine connected to the internal network was provided by CLIENT IT. The network was scanned using a licensed Nessus scanner installed on the machine. Using TeamViewer, a remote connection was established with the machine in order to conduct the assessment.

Due to time and access constraints, the scope of the assessment included only a subset of the hosts provided by the customer. These devices were given priority because the systems are controlled and patched by third parties and were more likely to contain vulnerabilities. The following table lists the range of devices included in the assessment:

10.x NAT /16

10.10.x	Edge connections
10.70.x	Digital Signage
10.110.x	[redacted]
10.120.x	HVAC controls
10.192.x	[redacted] system

Table 1 - Scope

2.3 Findings

Device Group	Critical	High	Medium	Low
[redacted] system	1	25	52	24
[redacted]	1	40	25	0
Digital Signage	1	22	8	2
Edge Connections	1	22	20	6
HVAC Controls	1	23	15	0

Table 2 - Total Issues Detected

2.3.1 SNMP Vulnerabilities

SNMP vulnerabilities were found within each group of network devices. Scanning the devices using SNMP information revealed that UDP port 161 was open on several of the hosts:

Edge Connections	Digital Signage	*******	HVAC Controls	*** POS
10.10.0.1	10.70.01	10.110.0.1 10.110.60.1 10.110.60.10 10.110.60.11 10.110.60.12 10.110.60.21 10.110.60.3 10.110.60.30 10.110.60.31 10.110.60.32 10.110.60.33 10.110.60.4 10.110.60.40 10.110.60.41 10.110.60.5 10.110.60.6 10.110.60.7 10.110.60.8 10.110.60.9	10.120.0.1 10.120.1.20	10.192.0.1 10.192.10.1

Table 3 - SNMP Servers

Public Strings and Protocol Version

The community string acts as the password for SNMP communication. This remote SNMP server replies to the default community string (public). Leaving the default community string makes it easy for attackers to obtain information about devices on the network and even reconfigure them.

Nessus scanner sent an SNMP 'get-next-request' and determined that protocol version SNMPv2c was being used by the remote SNMP agent. CISA has released and alert regarding SNMP abuse. The alert emphasizes that SNMPv3 should be the only version of SNMP deployed. Earlier versions do not authenticate and encrypt payloads. SNMPv3 replaces the clear text password sharing used in SNMPv2.

SNMP 'GETBULK' Reflection DDoS

Scans indicated that these devices can be abused in an SNMP Reflection DDOS attack. These devices are abused when the remote SNMP daemons responds to 'GETBULK' requests. The responses to these requests include a large amount of data. It has been found that these particular SNMP daemons are responding with a larger than normal value for 'max-repetitions'. This makes these devices useful to remote attackers when conducting a reflected distributed denial of service attack on an arbitrary remote host.

2.3.2 Telnet Vulnerabilities

Unencrypted Telnet Server

The scan revealed that these remote hosts were running a Telnet server over an unencrypted channel. This can be cause for concern because logins, passwords, and commands are transmitted in cleartext. It makes it possible for a remote, man-in-the-middle attacker to eavesdrop on a Telnet session. While eavesdropping, the attacker may obtain credentials or other sensitive information and manipulate the traffic exchanged between a client and server.

3. Web Application Assessment

3.1 Executive Summary

A licensed version of BurpSuite Professional was used to scan www.CLIENT.com for security issues. The majority of the issues were found in the A-DEPARTMENT and B-DEPARTMENT sections of the application. The A-DEPARTMENT and B-DEPARTMENT sections allow user input and interaction. Scans revealed that these pages might cause the application to be vulnerable to cross-site scripting. However, these advisories had only tentative confidence. I personally did not see how client-side scripts could read data from a part of the DOM in an unsafe way.

A second issue detected is of low severity but can be a potential vulnerability. The application does not enforce strict transport security. As a result, the application can be used as a platform for attacks against its users. In the event that a targeted user follows a link to the site from an HTTP page, their browser will not attempt to use an encrypted connection. This issue can be remediated by enabling HTTP Strict Transport Security (HSTS). This will prevent applications from allowing web browsers access to the site without using HTTPS.

3.2 Targets

The application was an ASP.NET web application running on a Microsoft-IIS server.

Target ID	Domain	Path 1	Path 2	Path 3
1	https://www.CLIENT.com/	**********	*****/	
2	https://www.CLIENT.com/	**********	*****/	[redacted]
3	https://www.CLIENT.com/	**********	*****/	[redacted]
4	https://www.CLIENT.com/	**********	*****/	[redacted]
5	https://www.CLIENT.com/	**********/	*****/	[redacted]
6	https://www.CLIENT.com/	**********/	********/	
7	https://www.CLIENT.com/	**********/	********/	[redacted]
8	https://www.CLIENT.com/	**********/	********/	[redacted]
9	https://www.CLIENT.com/	**********/	********/	[redacted]
10	https://www.CLIENT.com/	**********/	********/	[redacted]
11	https://www.CLIENT.com/	**********/	********/	[redacted]
12	https://www.CLIENT.com/	**********/	*****/	
13	https://www.CLIENT.com/	B-DEPARTMENT/	********/	

Table 4 - Primary Target URLs

3.3 Findings

3.3.1 Cross-site scripting (reflected)

In many of the paths from https://CLIENTcom/[redacted], reflected cross-site scripting issues were detected. It was demonstrated that arbitrary JavaScript could be injected into the application's

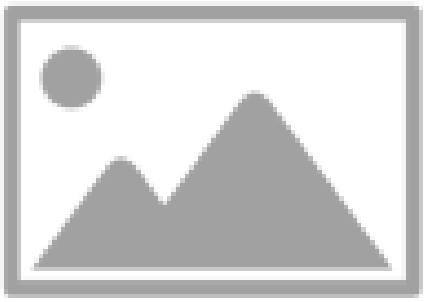
response. Event handlers can be used for this purpose to introduce arbitrary JavaScript into the document.

This issue was detected in the following application paths:

3.3.2 Cross-site scripting (DOM-based)

Potential vulnerabilities arise when controllable parts of the DOM, such as the URL, are read by client-side scripts and processed in an unsafe way. An attacker can take advantage of this by writing controllable data into the HTML document. Because this data is read by a client-side script, the attacker's JavaScript code could be executed within another application user's browser in the context of that user's application session. Depending on the attacker's code, the attacker can access sensitive data from that user such as credentials and session tokens.

Instances of this issue were detected in the following locations:



3.3.3 HTTP Transport Security

The web application accepts connections through HTTP and then redirects to HTTPS. A user can access the site by entering http:// CLIENT.com or simply CLIENT.com and establish unencrypted communication with the site before being redirected. An opportunity for a man-in-the-middle attack is created as a result.

When a user requests a URL with HTTP, the server responds with a 301 redirect to switch from HTTP to HTTPS. If an attacker is able to capture this network traffic, tools such as SSLStrip can be used to strip the HTTPS URL and force the victim's browser to communicate with the attacker in plain-text over HTTP. The attacker then proxies the modified content from an HTTPS server to steal valuable data or present a fake login portal page.

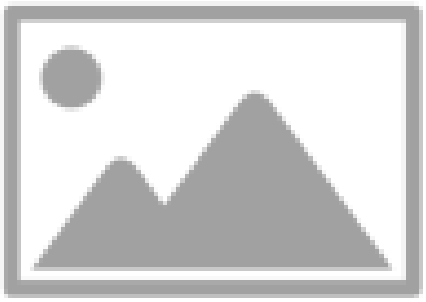


Figure 1 - 301 Redirect from http://CLIENT.com

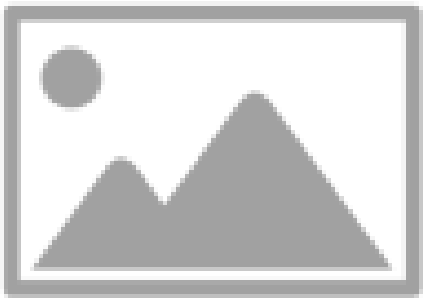


Figure 1 - CLIENT.com Response Headers

HTTP Strict Transport Security (HSTS) is a widely supported standard to protect site visitors. HSTS ensures visitors' browsers always connect to a website over HTTPS by removing the need for the common, insecure practice of redirecting users from http:// to https:// URLs (HTTP Strict Transport Security, n.d.). A domain instructs a browser that it has enabled HSTS by returning a specific HTTP response header over an HTTPS connection. Once the browser is instructed by the domain that is has enabled HSTS, the browser does two things:

- Always uses an https:// connection. This is true even when a visitor clicks on an http:// link or types the domain into the location bar without specifying a protocol.
- Prevents visistors from clicking through warnings about invalid certificates.

Forcing HTTPS is not the same as enforcing HSTS. HTTPS is enforced by redirection on the server side. HSTS is client-side, where the server sends a specific response header to force the browser to prevent requests sent through HTTP.

HSTS Preloading

A user's browser will not utilize HSTS protection until it is exposed to the HSTS header at least once. As a result, users are not protected until their first successful secure connection to CLIENT.com. When users visit http://CLIENT.com, they are redirected to https://www.CLIENT.com. Therefore, https://CLIENT.com is never visited and connecting clients will never be exposed to an HSTS policy with an *includeSubDomains* directive (see Figure 3) that applies to the whole zone.

To remedy this issue, browsers incorporate Chrome's *HSTS preload list.* Domains in this list get Strict Transport Security enabled automatically, including the first visit. Although the list was created by the Chrome security team, Firefox, Safari, Opera, and Edge incorporate the HSTS preload list.

3.4 Recommendations

3.4.1 Cross-site scripting (reflected)

If possible, user-controllable data should not be echoed by the application response. Otherwise, there are two primary recommended defenses for this issue. First, input should be validated on arrival. The input can be validated by ensuring the input matches a well-defined regular expression that checks if the input contains expected content. Secondly, at the points where user input is copied into the application responses, the user input should be HTML-encoded. HTML metacharacters should be replaced with their corresponding HTML entities. For cases where certain HTML tags are allowed in user-authored content, the supplied HTML should be parsed to check for dangerous syntax.

3.4.2 Cross-site scripting (DOM-based)

This issue can be remediated by not allowing untrusted sources to dynamically write data to the HTML document. But, if the application requires data to be written dynamically into the HTML document, the data must either be validated on a whitelist basis or sanitized and encoded.

3.4.3 HTTP Strict Transport Security

The CLIENT.com domain should instruct browsers that it has enabled HSTS by returning an HTTP header over an HTTPS connection. The HSTS policy should include all subdomains.

The response should include the following header:

```
Strict-Transport-Security: max-age=31536000; includeSubDomains; preload
```

Figure 2 - HSTS Response Header

It is important that the HSTS policy be deployed at https://CLIENT.com and not https://www.CLIENT.com. Secondly, all subdomains associated with CLIENT.com must support HTTPS. However, the subdomains do not have to each have their own HSTS policy.

The CLIENT.com domain should be added to the HSTS preload list. In order for the domain to be submitted to the list, certain requirements must be met.

- The root domain and all subdomains must have HTTPS enabled. Most importantly, HTTPS must be enabled on the *www* subdomain, if a DNS record exists for it. This includes any subdomains in use solely on intranets.
- The HSTS policy must include:
    - All subdomains

  - A long *max-age*
  - A *preload* flag, indicating the domain owner consents to preloading
- The website redirects from HTTP to HTTPS

To configure Microsoft systems running IIS to use HSTS, the web.config file configuration will need to include the following:

```
<?xml version="1.0" encoding="UTF-8"?>
<configuration>
    <system.webServer>
        <rewrite>
            <rules>
                <rule name="HTTP to HTTPS redirect" stopProcessing="true">
                    <match url="(.*)" />
                    <conditions>
                        <add input="{HTTPS}" pattern="off" ignoreCase="true" />
                    </conditions>
                    <action type="Redirect" url="https://{HTTP_HOST}/{R:1}"
                        redirectType="Permanent" />
                </rule>
            </rules>
            <outboundRules>
                <rule name="Add Strict-Transport-Security when HTTPS" enabled="true">
                    <match serverVariable="RESPONSE_Strict_Transport_Security"
                        pattern=".*" />
                    <conditions>
                        <add input="{HTTPS}" pattern="on" ignoreCase="true" />
                    </conditions>
                    <action type="Rewrite" value="max-age=31536000; includeSubDomains; preload" />
                </rule>
            </outboundRules>
        </rewrite>
    </system.webServer>
</configuration>
```

Figure 3 - HSTS Supported web.config (HTTP Strict Transport Security, n.d.)

For nginx servers, an add_header command must be applied the pertinent virtual host configuration. The following batch of HTTPS rules should be used to set the header:

```
add_header Strict-Transport-Security 'max-age=3153600;
includeSubDomains; preload;' always;
```

Figure 4 - Configuration for nginx servers

References

HTTP Strict Transport Security. (n.d.). Retrieved from https.cio.gov: https://https.cio.gov/hsts/

Intersoft Consulting. (n.d.). *General Data Protection Regulation*. Retrieved from GDPR-Info.eu: https://gdpr-info.eu/