Company of Choice: Jannou Credit Union

Research on company: Jannou Credit Union is a financial institution situated in Castries, St Lucia. Its main focus is to efficiently serve the clientele while incorporating automation and technology to achieve such a goal. Being a financial institution, it is equipped with both the physical means of security as well as technological mean. In terms of physical security, the credit union has implemented surveillance cameras as well as security guards as well as fencing in order to keep the infrastructure secure. The building is also equipped with a fire detection system to instantly alert personnel of any fires within the building. The credit union has also implemented a secure room for the servers which is inaccessible by any unauthorized party. Jannou has incorporated both hardware and software firewall in order to filter incoming and outgoing traffic. The core system is based on windows domain which is responsible for controlling and maintaining user access to files and network drives, while also maintaining user privileges. The Credit Union also uses IP based phones in order to contact one and other and has so vendor software as well as a few custom software integrated in their network. Jannou Credit Union deals with confidential member information and continues to instill confidence in their clientele when it comes to assurance of confidentiality and maintaining the integrity of their information.

1. Policy Compliance

5 Definitions and Terms

The following definition and terms can be found in the SANS Glossary located at: https://www.sans.org/security-resources/glossary-of-terms/

- Proprietary Encryption

Policy Compliance

External Resources

6 Revision History

2. Policy Compliance

Policy Compliance

5. Policy Compliance

Policy Compliance

Encryption key management, if not done properly, can lead to compromise and disclosure of private keys used to secure sensitive data. While users may understand it’s important to encrypt certain documents and electronic communications, they may not be familiar with minimum standards for protection encryption keys as well as the technological means of encrypting their data which is why this policy is geared to providing standards which should followed. Further more passwords are a critical component of information security. Passwords serve to protect user accounts; however, a poorly constructed password may also result in the compromise of individual systems, data, or network.

Another vulnerable tool used in networks are electronic emails. Misuse of email can pose many legal, privacy and security risks, thus it's crucial for users to understand the appropriate use of electronic communications. Apart from emails, remote access is also another widely used technology ay Jannou Credit Union, it is essential in maintaining their team's productivity especially in situations when work from home becomes a major request, but in many cases this remote access originates from networks that may already be compromised or are at a significantly lower security level than the corporate network. While these remote networks are beyond our control, we must mitigate these external risks the best of our ability. Due to this any individual who requires work from home can only access the network via the use of a laptop provided by Jannou Credit Union which must be installed with Fortinet firewall and Fortinet vpn client.

The mass explosion of Smart Phones and Tablets wireless connectivity is almost a given at every organization. Insecure wireless configuration can provide an easy open door for malicious threat actors, due to Jannou Credit Union being a financial institution it is crucial that the wireless technology is configured based on current security standards to maintain its data integrity. As we all know Database authentication credentials are a necessary part of authorizing application to connect to internal databases. However, incorrect use, storage and transmission of such credentials could lead to the compromise of very sensitive assets.Currently database is being accessed at Jannou Credit Union for report generation and data analytics.

Another pressing security issue is allowing employees to install software on company computing devices, which opens the organization up to unnecessary vulnerabilities. Such as exposing the network to malware from infected installation software, unlicensed software which could be discovered during audit, and programs which can be used to hack the organization's network. In addition to that unsecured and vulnerable servers continue to be a major entry point for malicious threat actors. Consistent Server installation policies, ownership and configuration management ensure that a network topology is hardened and secured from outside threats. Web application vulnerabilities are also another security risk which account for the largest portion of attack vectors outside of malware. It is crucial that all web application to be implemented at Jannou Credit Union are assessed for vulnerabilities and any vulnerabilities be remediated prior to production deployment.

Lastly proper disposal of equipment is both environmentally responsible and often required by law. In addition, hard drives, USB drives, CD-ROMs and other storage media contain various kinds of Jannou Credit Union data, some of which is considered sensitive. In order to protect our constituent's data, all storage mediums must be properly erased before being disposed of. However, simply deleting or even formatting data is not considered sufficient. When deleting files or formatting a device, data is marked for deletion, but is still accessible until being overwritten by a new file. Therefore, special tools must be used to securely erase data prior to equipment disposal. This is crucial to Jannou Credit Union since it deals with highly confidential information.