PUMA: Scope, goals, and risk assessment report

Scope and goals of the audit

Scope: The scope is defined as the entire security program at PUMA. This means all assets need to be assessed alongside internal processes and procedures related to the implementation of controls and compliance best practices.

Goals: Assess existing assets and complete the controls and compliance checklist to determine which controls and compliance best practices need to be implemented to improve PUMA's security posture.

Current assets

Assets managed by the IT Team include:

- Management of systems, software, and services: image storage provider (minio), email provider (mailjet), database, security and server memory allocation (gigacandanga)
- Internal network
- Data retention and storage
- PM2 Logs

Risk assessment

Risk description

Currently, there is inadequate management of assets. Additionally, PUMA does not have all of the proper controls in place and may not be fully compliant with Brazil's LGPD (LEI Nº 13.709, DE 14 DE AGOSTO DE 2018) and international regulations and standards.

Control best practices

The first of the five functions of the NIST CSF is Identify. PUMA will need to dedicate resources to identify assets so they can appropriately manage them. Additionally, they will need to classify existing assets and determine the impact of the loss of existing assets, including systems, on business continuity.

Risk score

On a scale of 1 to 10, the risk score is 8, which is fairly high. This is due to a lack of controls and adherence to compliance best practices.

Additional comments

The potential impact from the loss of an asset is rated as medium, because the IT team does not know which assets would be at risk. The risk to assets or fines from governing bodies is high because PUMA does not have all of the necessary controls in place and is not fully adhering to best practices related to compliance regulations that keep critical data private/secure. Review the following bullet points for specific details:

- Currently, not all employees and developers (only DevOps and Tech Lead members) have access to internally stored data and may be able to access customers' PII/SPII. That is great to make sure internal leaks are avoided.
- Access controls pertaining to least privilege and separation of duties have not been implemented.
- The server has a firewall that blocks traffic based on an appropriately defined set of security rules.
- No antivirus software is installed and being monitored regularly by an IT team member.
- The IT department has not installed an intrusion detection system (IDS).
- The team does implement Swagger so it can track existing API routes and its uses.
- The team does not implement a logging library or a log management system on any of its services and web products. The only logging implemented is the PM2 terminal on the deployment machine that could easily be wiped by an attacker if it got inside the server.
- There are no disaster recovery plans currently in place, and the company does not have backups of critical data.
- Although a password policy has been debated upon, no pattern has been adopted, the only rule implemented being a minimum of 8 characters. This does not take account the needs of requiring special characters, upper and lowercase characters in making a strong password.

Controls Assessment

Administrative Controls			
Control name	**Control type and explanation**	**Needs to be implemented (X)**	**Priority**
Password policies	Preventative; establish password strength rules to improve security/reduce likelihood of account compromise through brute force or dictionary attack techniques	X	High
Separation of duties	Preventative; reduce risk and overall impact of malicious insider or compromised accounts	X	Medium

Technical Controls			
Control Name	**Control type and explanation**	**Needs to be implemented (X)**	**Priority**
Intrusion Detection System (IDS)	Detective; allows IT team to identify possible intrusions (i.e., anomalous traffic) quickly	X	High
Logging	Preventative/detective; can reduce risk of certain events; can be used after event for investigation	X	Very High
Backup	Corrective; can restore/recover from an event;	X	High
Antivirus (AV) software	Corrective; will detect and quarantine known threats;	X	High

Manual monitoring, maintenance, and intervention	Preventative; Necessary to identify and manage threats, risks, or vulnerabilities to out-of-date systems	X	Medium

Compliance Checklist

Lei Geral de Proteção de Dados (LGPD)

Brazil's Lei Geral de Proteção de Dados (LGPD) is a comprehensive data protection law designed to regulate the processing of personal data. Officially known as Law No. 13,709, it was signed into law on August 14, 2018, and came into full effect on September 18, 2020. The LGPD is influenced by the European Union's General Data Protection Regulation (GDPR) and aims to provide individuals with greater control over their personal data, ensure transparency in data processing, and establish clear guidelines for businesses and organizations handling personal data.

Key Components of the LGPD

Scope and Application: The LGPD applies to any processing of personal data carried out by individuals or legal entities, whether public or private, that operate within Brazil or process data collected in Brazil. It covers both online and offline data processing activities.

Personal Data: Personal data under the LGPD includes any information related to an identified or identifiable natural person. This encompasses a wide range of data, from names and identification numbers to location data and online identifiers.

Data Processing Principles: The LGPD outlines several principles that must be adhered to when processing personal data, including:

Purpose Limitation: Data must be processed for specific, legitimate, and clearly stated purposes.

Adequacy: Data processing must be compatible with the purposes for which the data was collected.

Necessity: Only the minimum necessary data should be processed for achieving the intended purpose.

Transparency: Data subjects must be provided with clear, accurate, and easily accessible information about how their data is being used.

Security: Appropriate technical and organizational measures must be taken to protect data against unauthorized access, accidental loss, destruction, or damage.

Data Subject Rights: The LGPD grants individuals several rights regarding their personal data, including:

- Access: The right to access their personal data.
- Correction: The right to request correction of inaccurate or incomplete data.
- Deletion: The right to request deletion of data that is unnecessary or processed in violation of the law.
- Portability: The right to transfer their data to another service provider.
- Information: The right to be informed about data processing activities.

Legal Basis for Data Processing: The LGPD specifies ten legal bases for processing personal data, including consent from the data subject, compliance with legal obligations, and the legitimate interests of the data controller.

Consent: When consent is the basis for data processing, it must be freely given, informed, and explicit. Data subjects have the right to withdraw their consent at any time.

Data Protection Officer (DPO): Organizations are required to appoint a Data Protection Officer to oversee data protection strategies and ensure compliance with the LGPD.

Data Breach Notification: The LGPD mandates that data breaches must be reported to the National Data Protection Authority (ANPD) and, in some cases, to the affected data subjects, in a timely manner.

Penalties and Enforcement: Non-compliance with the LGPD can result in significant fines, which can be up to 2% of a company's revenue in Brazil, capped at R$50 million per violation. The ANPD is responsible for enforcing the law and has the authority to issue fines and other sanctions.