Internship report. Information Security Analyst

Anastasiya Kornitska 177360IVCM

MSc Cyber Security, First Year

Tallinn University of Technology

This report was written as a part ITX8512 course taught in 2017 spring semester (MSc Cyber Security, First year, Tallinn University of Technology).

            Contact: anakornitska@gmail.com

In this short paper, I would like to present my responsibilities and tasks as well as to report what I have achieved during the period of 12.01 – 29.06 working at MYJAR as an Information Security Analyst.

*General:*

* Getting to know the environment of information security, network security, studying penetration testing reports and scans, information security policies, data security, previously done operations and changes in order to identify needed steps, tasks and challenges.
* Identifying a need for creation of Data Classification Document (DCD), preparing it based on the information provided by IT Operations Department, consulting employees on this matter. It would allow MYJAR to implement the DCD in all available policies, evaluating the scale of data used in the company and the risks, which might occur. It is a fundamental document for several policies, which tackle the issue of data classification regarding Confidentiality, Integrity, Availability. Developing the strategy how to create the Data Classification Document for each department.

*Project #1. Internal IT Security Audit*

* An on-going project cooperation with Compliance and DevOps department.
* Determining the scope and preparing quarterly IT Policy Monitoring Report and Schedule of the Audit in cooperation with Group Compliance Officer from the compliance department. Checking the technical aspects of policy compliance (configurations, scanners running, anti-viruses, firewalls, network architecture reports, etc.).
* Monitoring, updating, examining aspects of information security at MYJAR to provide compliance to PCI DSS. Assisting colleagues on the path to the PCI DS Compliance: checking vulnerabilities, the progress of their patching, reviewing and editing the policies.
* Conducting consultations with DevOps, Dev and Marketing and CS departments on assessing company’s IT security compliance and improving the current state.

*Project #2. Business Impact Analysis/Risk Assessment, Business Continuity Action Plan, Disaster Recovery Plan*

* Creating a framework for conducting BIA/RA, BCAP, DRP based on best practices and books;
* Conducting sets of meetings and consultations with heads of such departments as Customer Service, Collections & Recoveries, Fraud, Secure Recoveries LTD, Quality and Customer Care. Assisting managers on this task.
* Assist on developing a business continuity strategy for the aforementioned departments.

Project #3. Policy-related:

* Reviewing and editing such policies and documents as: Information Security Policy (Policy Management, Acceptable Use Policy a Right of Media Equipment, Access Control Policy, Anti-Virus Policy, Data Protection Policy, Data Retention Policy, Information Security Incident Management Policy, IT Vulnerability Policy, Network Security Policy, Password Policy, Personal Data Breach Management and Reporting Policy, Physical Security Policy, Remote Access Policy), IT Disaster Recovery Plan.

Ongoing security tasks:

* Assisting DevOps in basic Linux security-related tasks;
* Reviewing, updating, monitoring and creating tickets based on the recent scans and updates on security.

Security Awareness Program:

* Managing and maintaining internal security awareness program for all employees in the company.