CYBER VT2022

Case 1 Policy Group #10

High Level Cyber Security Policy

Definition of Information Security

Information Security aims to protect sensitive information from unauthorized activities such as data disclosure, modification, disruption, and destruction. The overall goal is to prevent such security incidents or mitigate the adverse impacts of them to ensure that Eastschange business, customers, suppliers and other parties will be adequately protected.

Objectives

To guide all information security activities and provide management frame for information security in accordance with Eastschange business requirements and relevant laws and regulations to protect the integrity of the private and confidential members and business data that resides within the business's infrastructure.

Scope

This policy applies to the use, access, and acquisition of information, electronic and computing devices, software, and network resources and services to conduct Eastschange business or interact with other networks and business systems, whether owned or leased by Eastschange, the employee, or a third party.

Responsibilities Assignment for Information Security Management

All employees, directors, contractors, consultants, temporaries, and other workers at Eastschange, including all personnel affiliated with third parties, are responsible for exercising good judgment regarding appropriate compliance of Eastschange security policies and standards, local laws, and regulations.

Deviations and Exceptions Handling

A document that handles the situations of responding to nonconformities with policies and procedures that will occur by stakeholders is identified and defined in a separate document (not presented). Moreover, the situations in which the regular security rules are not applicable is identified and defined in a separate document (not presented) such as in case of a disruptive incident then the physical access controls will not be applied.

Information Protection Requirements:

All Eastchange physical environments must be protected against unauthorized physical access, and natural and electrical incidents. Monitored and secured by sufficient and efficient measurements and tools. Business and stakeholders data must be protected and accessed by authorized parties according to the Identity Management System, backed up and tested for restore, encrypted in transit and at rest. Network resources (Servers, firewalls, routers, printers, etc) inside the company perimeter must have a good level of protection. All endpoints (Desktops, laptops, mobile devices) must have effective protection against malware and spy software. The business software must be patched in realtime to prevent zero day attacks. Accepted usage policy must be obeyed by all stakeholders for optimal protection.

Necessary measures toward this end involve the creation of specific policies targeting areas such as:

- Patch Management: monitor system of potential bugs and threats, and promptly install patches following appropriate testing and release.
- Encryption: defines the importance of using encryption methods, and some recommendations towards this topic.
- Backup and Restore: defines information on how backup and restoration should be accomplished.
- Access Control: defines different kinds of access control that ought to be implemented within the company.
- Network Security: defining a perimeter between internal subnetworks and internal-external networks.

This document states the developed high-level cyber security policy which is reviewed by the relevant stakeholders and approved by the high management. All the stakeholders have to implement and comply with the security rules stated, CISO/CIOs and Mangers are responsible for checking compliance by the other parties and act according to the rules. The policy will be evaluated regularly every year or when needed. A technical policy document and other policy documents (not presented) are underlying this policy.

Technical Cyber Security Policy

The objective of this technical cyber security policy document is to provide some level of guidance on different technical aspects that must be taken into account in order to maximize the organization's cyber-resilience. Towards this end, we have outlined a series of technical policies that cover the most critical information/information-related assets and processes that belong to the organization.

1. Backup and restore policy

As the company has to deal with confidential data (e.g., maintaining private keys), it needs to make sure that these data are not going to disappear, whether it is media failure, natural disaster, or a cyber-attack. To maintain the integrity and availability of information, routine procedures should be established to implement the agreed backup policy and strategy for taking backup copies of data and rehearsing their timely restoration. Adequate back-up facilities should be provided to ensure that all essential information and software can be recovered following a disaster or media failure. The followings should be considered:

a) The necessary level of back-up information should be defined

b) Accurate and complete records of the back-up copies and documented restoration procedures should be produced

c) Back-up information should be given an appropriate level of physical and environmental protection

d) Back-up media and restoration procedures should be regularly checked and tested

Backup should be accomplished every night and the weekend when there is less traffic in order to not congest the network.

2. Encryption Policy:

The company is handling confidential data, such as private keys, and personal information from people in the exchange platform. Hence, access should be restricted, and protected in order to obtain confidentiality, integrity and authenticity of the information. The company should use the AES-256 encryption method as we only need to protect the data in the databases from any intruders. And using a symmetric key would help to improve speed at encrypting large amounts of data. Furthermore, the company should develop a way to protect the lifetime of the cryptographic key, that will be used to access the sensitive data, hence the company should use the combination with RSA to protect the secret key from AES-256, and give access to the private key to only specific people within the company. The source code of the in-house software should also be encrypted, or they should use specific ways to obfuscate the code in order to make it harder for someone to reverse engineer it. Every communication within the company, and outside the company should be encrypted, and accessing the company from outside the network, a VPN should be used for that.

3. Access Control Policy:

The company is using different tools in order to make the business work. They have for instance developed their own software, using an operating system, using network equipment and so on. However, it appears that the company does not have an appropriate access control. They should establish an operating system access control, where only authorized people should have access, should log any failed attempts, and should implement a limited time connection to the operating system. This can also work for the use of the software, as there should make sure that only authorized people, and especially during working hours should have access, and not intruders. Furthermore, the company should be able to monitor the networks, in order to prevent any unauthorized access to the network. Access from internal or external should be controlled. Regarding the user access management, a strong password is necessary to access the laptops. The current system asks for at least 8 characters, however, because the company is handling financial information, money exchange and such, they should increase the number of characters to at least 13, which would contain lower/upper case alphabets, special characters, and numbers. This would prevent any bruteforce from someone who managed to steal the laptops. Furthermore the password should be changed at regular intervals in order to maximize security. Regarding the mining of bitcoin, only specific people should have access to the information and handle any issues related to the mining.

4. Patch management policy:

Because the organization’s success heavily relies on the efficient functioning of the specialized hardware (and software) equipment for bitcoin mining, as well as on minimizing the latency of exchange operations, a proper patch management policy must be designed by taking such factors into consideration. Therefore, technical issues involving hardware/software/systems on which bitcoin generation and exchange are dependent upon must be patched as soon as upgrades become available to allow for business continuity.
All potential bugs or vulnerabilities must be documented when discovered and responsibilities for monitoring them must be assigned to the relevant actors. Furthermore, patches must be tested and evaluated thoroughly in a controlled environment (before being installed) to avoid fatal side effects.

5. Network Security policy:

Segregation of networks must be applied to separate the different organizational units belonging to Eastchange AB. The internal economy systems, human resources systems, DNS services, FTP services, internal web services' perimeters should be defined by clear boundaries connected via some specific type of gateway (filtering routers or firewalls) whose sophistication level may vary based on the security requirements and access control policies defined for each of the internal subnetworks.

Communication between the internal and external network (Eastchange's website, database and backend calculation engine servers, API server, FTP server) must be strictly controlled.
Border routers should be configured to only route traffic to and from the company's public IP addresses, firewalls should be deployed to restrict traffic only to and from the minimum set of necessary services, and intrusion prevention systems should be configured to monitor for suspicious activity crossing the border between internal and external networks.

Furthermore, critical assets including specialized hardware for bitcoin mining, storage and trading require additional protection from the rest of the network, especially due to the fact that the Bitflip web platform runs in the same data center in which those assets are physically located. Strong authentication in conjunction with a strict access control must be set up to maximize the isolation of those parts of the network from the rest.