Cybersecurity Assessment Report for the Telecommunication Company, SBB: Aligning with NIST CSF 1.1 Framework

Sara Tesic, 2087203

01.07.2023. UNIPD, Italy

Table of Contents

Scope

SBB is the leading operator of digital and analog cable television, satellite and Internet television in Serbia. They also provide their users services of both cable internet and fixed telephony. Their currently most used service is “EON” which offers users to play games, surf the internet, customize the profile and content regarding their preferences and etc. Since it operates through network and collects data for each of the users, that makes company more exploitable to different attacks. So, the aim of this report is to analyze all potential vulnerabilities and it will serve as guide for implementing comprehensive controls that cover wide range of anomalous events. It gives insights to what is important to establish for the SBB to prevent and face the attacks. In this matter, we will use Cybersecurity Assessment framework NIST CSF, version 1.1. Framework is organized by 5 key functions which we will cover:

1. Identify,
2. Protect,
3. Detect,
4. Respond,
5. Recover

Identify

ASSET MANAGEMENT (ID.AM)

The SBB needs to understand the importance of confidential data and other assets such as IT equipment that is crucial for all operations of the company (computer servers, network equipment, data center and many more). They need to realize that they should adequately protect sensitive information from being disclosed to attackers otherwise it increases the likelihood of data breaches and compromises.

These assets help the organization to achieve business purposes and are identified and managed consistent with their relative importance to business objectives and the organization’s risk strategy

By identifying and managing these elements in line with their relative importance and the organization's risk strategy, the SBB can effectively align its resources and security measures to support its business goals while mitigating potential risks.

ID.AM-1: Identifying the physical systems and devices of the organization, like computer servers, telecommunication networks, data center (with users data in it), the SBB can better maintine them and implement security measures. This minimizes the risk of compromising data security, and harming the system of the organization. Moreover, we are decreasing the possibility of malicious actors to gain unauthorized access to resources.

ID.AM-3: Ensuring monitoring netwrok between the internet and the cloud environment but also within applications in the cloud environment. So we need to make sure that data flows are mapped because it can provide insight and transparency into the security of the system's processes as a whole. Another important segment is categorization the assets based on their importance to business objectives and their relevance to the organization's risk strategy.

ID.AM-6: SBB should define clear workforce roles and responsibilities for all relevant departments within the organization as well as setting clear role for the stakeholders. Also it

should establish secure communication channels for the communication to be implemented with all relevant parties when it is needed.

Protect

IDENTITY MANAGEMENT AUTHENTICATION AND ACESS CONTROL (PR.AC)

It has been identified that some users, with EON packages, are sharing their accounts with other, not authorized, users. SBB needs to focus on limiting unauthorized accesses and securing that the provided accounts (credentials) are verified. It should implement safeguards to limit potential attacks. Ensuring that only authorized users have access to system, network and data.

PR.AC-1: SBB should assign unique identifiers to authorized users and devices. Passwords should also contains certan requrements so it will ensure its strenght. Also, SBB should implement verification system, not just in metter of checking the credentials and identificators of users, but its IP adresses so they can secure that only „real“ users have access to their content.

PR.AC-5: - It is important for SBB to implement strict monitoring procedures for network and to continuously control the traffic flow inside of it. This way SBB will detect unauthorized accesses on time and restricting them so they will not be repeated.

AWARENESS AND TRAINING (PR.AT)

Since SBB has recently faced some type of phishing attack and even though they were warned about it, they did not respond properly to this case. It Is also reported that the attack is still ongoing and the proper defense mechanisms were not applied. This shows that in SBB there is no awareness about significance of the attacks and users data.

PR.AT-1: SBB needs to properly train people in its organization about potential threats and how to adequately react to them, defining their clear responsibility in those situations. They should be able to react fast and effectively and implement measurements that will prevent such threats of happening again. They should also be educated about the importance of users data and role of users as customers.
Also, employers should be informed to be cautious in interaction with suspicious requests for personal information. Especially, if the employers are not in security domain, they should verify the authencity of any request by contacting the experts in this area.

Detect

SECURITY CONTINUOUS MONITORNIG (DE.CM)

We already mentioned how process of monitoring is important, especially taking into consideration that SBB is one of the most used telecommunication provider in Serbia and has large amount of loyal clients. Organization may face lot of different attacks, not just phishing, and its should be able to detect them or even prevent from happening. It shoud ensure that all required data is collected, analyzed and processed. The mandatory procedures and processes should be defined and implemented in this matter.

DE.CM-1: In order to detect potential or already present cybersecurity attacks, SBB needs to carry out monitoring precedure on ongoing basis. It has been relaized that SBB possess large amoung of data that needs to collect and store. Therefore, company needs a monitoring methodology that will reduce the size of the accumulated data without reducing

the accuracy of the measurement collected. This can be done in multiple ways, one of the solutons is usage of software tools such as „Flamingo“.

DETECTION PROCESS (DE.DP)

As network is very important segment of the organization, it is not the only one. To be aware of any kind of unexpected events that may occure, SBB needs to implement adequate procedures and processes in hole system structure. Mainly, company should focus on defining clear roles and parties who have responsibility in this matter and their functions.

DE.DP-1: SBB employers seems to not have clear picture in what is their responsibility when it comes to protecting the company from anomalous events and that they are accountable for preventing it. So, it should well-define the roles for relevant people and groups (in some cases people are working in teams). And also clearly present what are their responsibilites and mandatory steps for each of them (monitoring, processing, analyzing and etc) that will help the organization prevent or prepare to react to as many as possible unexpected events. This will positively influence the data protection in the organization.

Respond

COMMUNICATIONS (RS.CO)

Response activities should be established in the process of incident and it should be communicated properly. As we have noticed that the SBB company has been strugguling with adequatelly dealing with situation when the incident happens, it is important that they establish good reports of those incidents as form of a response activity.

RS.CO-2: To create such a report, firstly the organization should establish the criteria (regarding some guidlines). Based on that predefined criteria, incidents should be reported. It is also important, for the company, to pay atention to the timing of writing a report, since it is acquired to be done as soon as the incident has been recognized, with no delay.

ANALYSIS (RS.AN)

It can be challenging for the organization to understand the impact of the incident that has occured. It makes it even more difficult, if the damage of it is not visible or it seems like it does not have an huge impact on the organization, meanwhile it does. We noticed in the example of phishing attack, that the company did not understand the impact of the attack since it let it freely happen again. In order to change this, company need to perform impact analysis of the incident.

RS.AN-2: This analysis that should be performed is focusing on evaluating the consequences of the incident and in that sense helping in understanding the effect of it. SBB should have the Incident Respons team that will perform this anlysis, and they will use the historical snapshots (historical record of the states of features of the IT instrastructure) for that purpose. Since SBB did not have practice to use historical snapshots, but they are used to using less robust approach, they will be required to implement this strategy beforehand.

Recover

RECOVERY PLANING (RC.RP)

At this part we have identified the importance of the establishing proper plan to recover the system from the incident that has happened. We realized that, SBB did not perform adequate operations to redeem after the phishing attack that has happened. So the

company has to define clear post-actions when such incidents happen, and it can be done through defining so-called recovery plan.

RC.RP-1: SBB should precise the clear steps, processes and procedures that should be performed in after the unexpected event/attack phase. It is important to understand the significance of reacting quickly (in relative time manner) and being effictive. When doing so, the organization can faster go back to normal working procedures as well as the possibilites of such a thing happening again decreases and the security of data in longer term increases.

COMMUNICATIONS (RC.CO)

The „physical things“in terms of attack/incident, are not the only assets that have been damaged. In those cases, when incidents occurs, especially when they involve users data (as we had a example of such a case) it is important to perform adequate communication strategy to relevant parties. It is imporatnt for the SBB to realize that with every attacks, the image of the SBB as brand loses one tiny pixel. So, not working on the fixing that pixels in image at the given moment, can result in completely distruction of the organization.

RC.CO-2: In this matter, SBB needs to perform certan steps to repair the reputation that it has violated. Action should be clearly defined, and they should have intention to repair the trust with relevant stakeholders. This can be followed by evaluating the perception of relevant people, so the company gathers more accurate results and better defines actions that need to be performed. In some cases reparing the reputation might require establishing trust with the users from scratch. At this point we do not see need of Public Relations involvement for the situations that SBB has been facing or might face in the near future

Conclusion

This report emphasis the benefits the company can gain by following the recommendations that are stated. SBB can improve the security in terms of decreasing possibilities of unauthorized access and data breaches as well as competently react in case of these or any other attacks. Also, it will build up risk management by identifying vulnerabilities. Moreover, SBB can improve the trust among the users and other relevant stakeholders.

All in all, by identifying and managing these elements in line with their relative importance and the organization's risk strategy, the SBB can effectively align its resources and security measures to support its business goals while mitigating potential risks. It is a proactive approach to safeguard organizations assets, reputation and business in general.