Security Governance
AA 2023-2024
2nd assignment

Due Date: January 21st, 2024

Maximum score: 3

Evaluation Criteria: *the assignment will be evaluated according with the following evaluation criteria:*

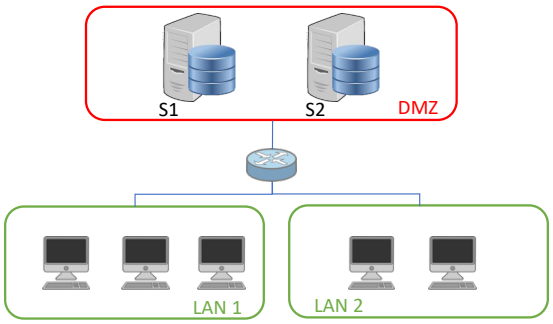
1. *Correct interpretation of the question*
2. *Clarity of the answer*
3. *Fitness of the answer with the question*
4. *Correctness of the answer*
5. *Completeness of the answer*
6. *Maturity demonstrated by the student.*

The assignment will be checked against anti-plagiarism.

Assignment Question

Identify, assessing and managing risks are fundamental activities that every organization must carry on for implementing a proper security protection strategy. During the years, many different risk assessment and evaluation methodologies have been proposed to support organization in this complex and important task and currently there exists many different methods to practically identify, assess and manage cyber risks.

Let us consider the network fragment depicted in the following schema:



Let us assume the following reachability conditions:

- Inside each LAN, every machine can reach any other machine,
- Machines in LAN1 can reach all machines in DMZ,
- Machines in LAN2 can reach only S1 in DMZ,
- S2 in DMZ is also exposed on Internet.

Let us assume that the organization has an important asset represented by the business process BP_i and let us assume that it is performed by orchestrating some applications (App_1, App_2, … App_n). Considering the CIA (Confidentiality, Integrity and Availability) properties of BP_i we have the following dependencies:

- Confidentiality of BP_i is guaranteed by preserving the confidentiality of App_1,
- Integrity of BP_i is guaranteed by preserving the integrity of App_1 and the integrity on App_3,
- Availability of BP_i degrades depending on the number of available applications i.e., it is progressively compromised as soon as the applications App_i lose their availability.

Applications are deployed on S1 and S2 as follows:

- On S1 we have running all the applications, and we have the vulnerability CVE-2013-3678 and the vulnerability CVE-2016-3169,
- On S2 we have running App_1 and App_3 and we have the vulnerability CVE-2013-3678 and the vulnerability CVE-2018-11218.

The machines in LAN1 can be accessed by an employee (Bob) who has the bad habit of leaving his password written on a Post-it easily accessible, while machines in LAN2 can be accessed by an employee (Alice) who has a high trust in her colleagues and thus tends to share her access credentials. Machines in the DMZ can be accessed only by the network administrator who is very careful in managing the passwords. However, sometimes he leaves the door of the data centre hosting the machines open with machines still logged in.

Given the described scenario, the student must:

1. evaluate the following risks:
    a. Loss of availability of BP_i
    b. Loss of integrity of BP_i
    c. Loss of confidentiality of BP_i.
2. Identify the possible mitigation strategies considering that:
    a. The organization must ensure a minimum level of availability and the service cannot be out-of-service for more than 1 minute (i.e., installing patches is possible only if the reboot time is less than 1 minute)
    b. The cost of data leaks for the organization is very high,
    c. The organization performs regular backups, so the cost of integrity violation is moderate,
    d. The organization has a limited budget for mitigating risks related to BP_i.

NOTE: For all that is not clearly specified in the text, the student can take proper assumptions (clearly specified in the answer) and solve the assignment accordingly.