Ftp server in a datadiode

Rusu George, Boulif Ilias, Orinx Cédric

November 14, 2017

1 Risk Analysis

1.1 Assets and Vulnerabilities

1.1.1 Physical Assets

1.1.2 Logical Assets

1.1.3 Persons

1.1.4 Intangible Goods

1.2 Threat Sources

Nature: Natural disasters such as an earthquake or a storm could be a source of threat that would affect the building of the company.

Employees: All employees that don't have the necessary knowledge to interact with the data diode must be taken into account of the analysis.

Administrators: Since that they have all access and priviledge to the data diode, the adminstrators are possible threat source.

Script Kiddies: They can a be a potentiel source due to the fact that the system is connected to the internet.

Skilled Hacker: The information protected by the system can be a target for different reasons like selling the the data or getting information for rival company. Since the system is supposed to be well protected, attacks will require some skills.

Unauthorized user

Malware:

1.3 Vulnerabilities

The following table will give a set of possible vulnerability that we have to take in account to secure the most possible the data diaode. This table will give the **ID** of vulnerability, his **source**, in reference to the point 1.2, which part of the inforamtion security it will **affect** (*confidentiality*, *avaibility*, *integrety*), and a short **description** of the vulnerability.

ID	Vulnerability	Source(s)	Affecting	Description
1	Power outage	Nature	Avaibility	
2	Fire	Nature	Avaibility	
3	DDOS attack	Skilled Hacker	Avaibility	
4	Data diode hardware failure	Nature	Avaibility	
5	Zero Day Attack	Skilled Hacker	Avaibility, Confidentiality, Integrety	
6	Data diode hardware degradation	Unauthorized user	Avaibility, Confidentiality, Integrety	
7				
8				
9				
10				
11				

Table 1: Vulnerabilities

1.3.1 Vulnerabilities Affecting Physical Assets

1.3.2 Vulnerabilities Affecting Logical Assets

1.3.3 Vulnerabilities Affecting Persons

1.3.4 Vulnerabilities Affecting Intangible Goods

1.4 Risks and Countermeasures

ID	Vulnerability	Impact	Description
1	Power outage	Medium	The data diode will not work anymore untill the power will be reasablish.
2	Fire	High	The data diode can suffer significant damage wich could lead to the replacment of the hardware.
3	DDOS attack	High	
4	Data diode hardware failure	Low	
5	Zero Day attack	High	
6	Data diode harware degradation	High	

Table 2: Impact

ID	Vulnerability	Likelihood	Description
1	Power outage	Low	
2	Fire	Low	
3	DDOS attack	Low	
4	Data diode hardware failure	Medium	
5	Zero Day attack	Medium	
6	data diode hardware degradetion	Medium	

Table 3: Likelihood

After having analyzed the impact and the likelihood of each vulnerabilities, we can define for each of them a risk level using the Table 4 to adapt our countermesure accordingly.

Risk Level			
Likelihood	**Impact**		
	Low	**Medium**	**High**
Low	Low	Low	Low
Medium	Low	Medium	Medium
High	Low	Medium	High

Table 4: Risk Level

ID	Vulnerability	Source(s)	Countermeasure(s)	I	L	Risk Level
1	Power outage	Nature		M	L	Low
2	Fire	Nature		H	L	Low
3	DDOS attack	Skilled hacker		H	L	Low
4	Data diode hardware failure	Nature		L	L	Low
5	Zero Day attack	Skilled hacker		H	M	Medium
6	Data diode hardware degradation	Unothorized user		H	M	Medium
7						
8						
9						

Table 5: Countermeasure