Info Hacker

RESUMO QUINZENAL OFICIAL DA ACADEMIA HACKER

LEMBRETES

-

01 - Os Pilares da Segurança da Informação

02 - DMZ (Demilitarized Zone)

Os Pilares da Segurança da Informação

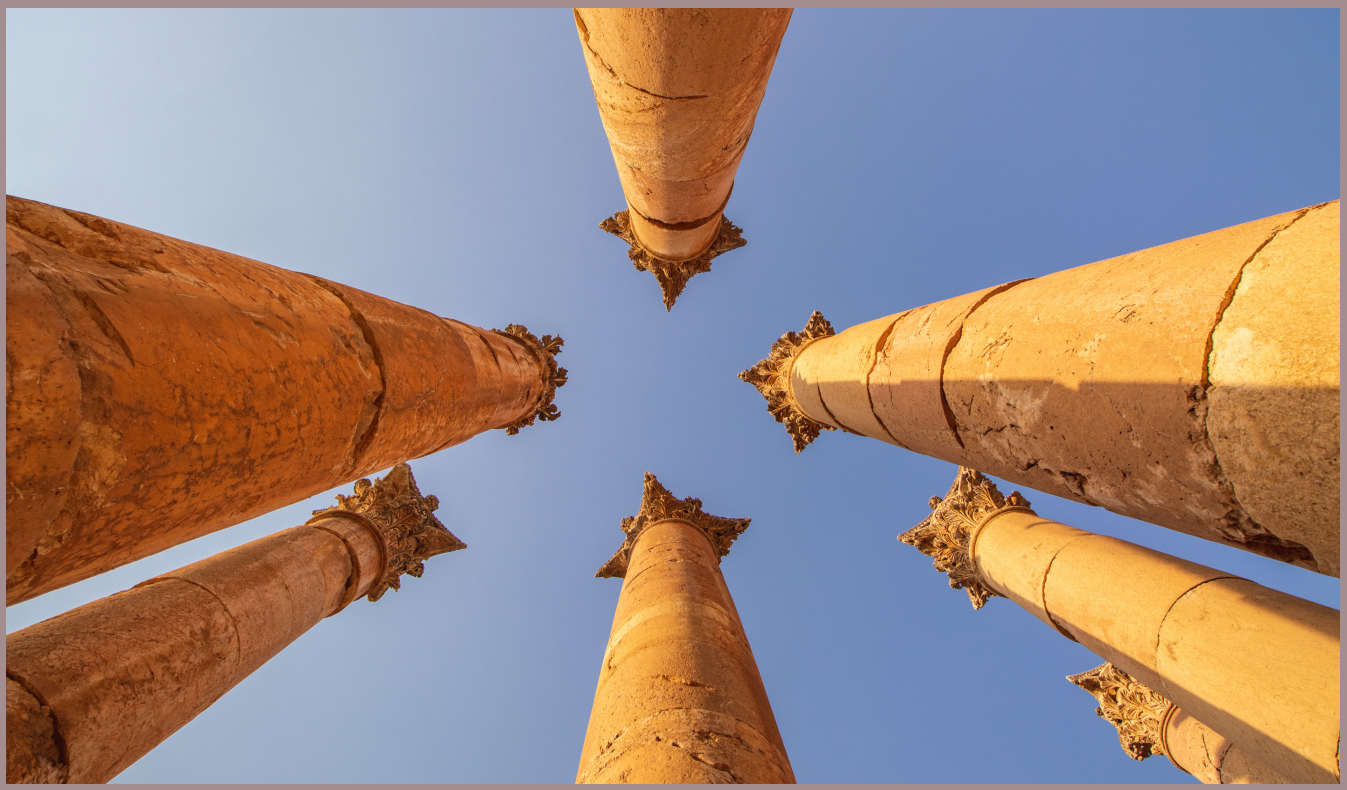
por Everton Borges

Na segurança da informação foram definidos três pilares: Confidencialidade, Integridade e Disponibilidade. Essas três propriedades são conhecidas como CIA (*Confidentiality, Integrity e Availability*).

A confidencialidade é quando a informação só está disponível para usuários autorizados a acessar. Quando um criminoso consegue escalar privilégio dentro da rede, de forma ilícita, temos uma quebra de confiança daquela informação.

A integridade garante que a informação chegue ao seu destino sem modificações e só será modificada por usuários com permissões de escrita. O ataque *Man in the Middle* pode comprometer esse pilar, onde o criminosos vai interceptar os dados no meio da comunicação e a informação deixará de ser integra.

A disponibilidade é a propriedade que torna a informação acessível a qualquer momento que o usuário necessite utilizar. Uma forma de ameaça a essa propriedade é o ataque de negação de serviço ou *Denial of Service (DoS)*.



DMZ (Demilitarized Zone)

por Guilherme Medeiros

Uma Zona Desmilitarizada (DMZ), em segurança da informação, é uma parte de uma rede que contém hosts expostos a outra rede. Essa outra rede é geralmente maior, *WAN*, não confiável, como a Internet. A função da DMZ é criar uma camada de segurança a uma rede local, expondo apenas os hosts que oferecem serviços para fora daquela rede. Desse modo, acessos externos podem ser feitos apenas a esses hosts dentro da DMZ, enquanto que o restante da rede da organização fica protegida por um firewall. Ela funciona como uma rede isolada da rede local que fica entre a Internet e a rede local privada.

Quais são os hosts que precisam estar conectados na DMZ? Aqueles que fornecem serviços como e-mail, servidores Web, servidores DNS, FTP, entre outros. Como eles são os mais propícios a um ataque externo, eles são propositalmente colocados numa região isolada dos demais hosts da rede, de forma preventiva, caso algum deles seja comprometido. Os hosts da DMZ podem se comunicar tanto com os hosts da rede interna quanto com os da rede externa. Podem inclusive contar com um firewall para dificultar conexões indevidas, caracterizando uma arquitetura de duplo firewall.

Caça Palavras

U	C	E	I	Z	I	L	I	M	L	C
X	Z	B	M	B	P	C	W	A	O	Y
F	Y	C	P	R	Y	S	C	Y	A	E
I	P	N	H	O	R	D	L	P	N	S
D	Z	V	C	K	S	A	A	S	O	Z
P	A	A	S	E	C	A	U	Z	W	C
T	N	L	I	R	G	M	I	Y	H	T
A	C	O	N	S	U	M	I	D	O	R
A	U	D	I	T	O	R	H	V	M	B
Q	J	P	B	J	G	H	S	H	F	G
C	A	R	R	I	E	R	O	M	I	C

SaaS PaaS IaaS Broker
Consumidor Auditor Carrier

Referências

https://www.canva.com/pt_br/

Livro: Fundamentos de Segurança da Informação: com base na ISO 27001 e na ISO 27002

Livro: Redes de Computadores. Pearson,2021.

Edições Anteriores

https://github.com/Academia-Hacker/Info-Hacker

Info Hacker - Edição 006
03/05/2022

Autores:
Everton Borges
Guilherme Medeiros

Revisão
Bruno Severo