

REDES DE COMPUTADORES

Aula 15 — Segurança Física e Lógica

Proteger equipamentos, sistemas e dados — as duas faces da segurança de redes

Unidade 4 — Servidores, Segurança e Segmentação | 2 horas



Objetivos da aula



Física x Lógica

Diferenciar segurança física e lógica, com exemplos de cada uma.



Firewall x Antivírus

Explicar por que essas ferramentas são complementares, não substitutas.



Menor Privilégio

Aplicar o princípio do menor privilégio a casos concretos de acesso.

Segurança física e segurança lógica



Segurança física

Protege os equipamentos em si: sala trancada, rack fechado, controle de acesso, câmeras, incêndio, poeira, temperatura, umidade, energia (nobreak).



Segurança lógica

Protege sistemas, contas, dados e serviços: senhas, autenticação, permissões, firewall, antivírus, atualizações e backup.

As duas se complementam: de nada adianta uma sala trancada se a senha é "admin/123456", e de nada adianta um bom firewall se qualquer um entra na sala do servidor.

Cuidados com o ambiente físico

- Sala técnica ou rack com acesso controlado, protegido contra poeira.
- Temperatura e umidade adequadas — equipamentos geram calor e precisam de ventilação/climatização.
- Sistemas de detecção de incêndio e proteção contra água, sempre que possível.
- Nobreak (UPS) evita que quedas de energia derrubem serviços de forma abrupta.
- Circuitos elétricos dedicados evitam sobrecarga.



Firewall x Antivírus: complementares

Critério	Firewall	Antivírus / EDR
Onde atua	No perímetro da rede	Diretamente no dispositivo
Função	Controla e filtra o tráfego, com base em regras	Identifica e responde a softwares maliciosos
Não impede sozinho...	...um funcionário abrir um anexo malicioso de e-mail	...uma tentativa de conexão indevida vinda de fora

São camadas complementares — nenhuma das duas cobre tudo o que a outra cobre.

FRASE-CHAVE DA AULA

De nada adianta um firewall bem configurado se a senha é "admin/123456".

Segurança física, segurança lógica e boas práticas de senha precisam funcionar juntas — uma falha em qualquer uma delas compromete as outras.

Senhas fracas e autenticação multifator

Erro básico e comum

Credenciais administrativas nunca devem usar valores óbvios como "admin", "123456" ou "senha" — é uma das primeiras coisas que um atacante tenta.

Sempre que disponível, use MFA

MFA (autenticação multifator) adiciona uma camada extra: mesmo que a senha vaze, o acesso ainda depende de um segundo fator.



Princípio do menor privilégio

Cada usuário deve receber apenas os privilégios estritamente necessários para sua função.

Exemplo: um funcionário do financeiro não precisa de acesso administrativo aos servidores.



Por que reduz o risco? Limita o estrago possível caso uma conta específica seja comprometida.

Encontrando vulnerabilidades

Cenário: uma pequena empresa apresenta os seguintes problemas.

- Servidor fica em uma sala sem porta, conectado diretamente à rede.
- O usuário administrador utiliza a senha "123456".
- Não existe backup dos dados.
- O Wi-Fi usa uma única rede para funcionários e visitantes.
- O firewall está desativado.



O que os grupos devem fazer

- Em grupos, identifiquem quantos problemas de segurança conseguem encontrar no cenário.
- Classifiquem cada problema: segurança física, segurança lógica, ou falha de senha/privilegio.
- Proponham uma solução concreta para cada problema identificado.
- Cada grupo apresenta suas respostas para a correção coletiva.

Resumo para levar da aula

- Segurança física protege equipamentos; segurança lógica protege sistemas, contas e dados — as duas se complementam.
- Ambiente físico do servidor: acesso controlado, temperatura/umidade, incêndio/água, energia (nobreak).
- Firewall filtra tráfego no perímetro; antivírus/EDR atua no dispositivo — um não substitui o outro.
- Senhas nunca devem ser óbvias; use MFA sempre que possível.
- Princípio do menor privilégio: cada um só com o acesso que sua função exige.





Obrigado!

Próxima aula: Segurança da Infraestrutura — Defesa em Profundidade