Franklin Parrini
Educação e Tecnologia

REDES DE COMPUTADORES

Aula 16 — Defesa em Profundidade

Segurança da infraestrutura: backup, phishing e camadas de proteção

Unidade 4 | 2 horas

Objetivos da aula

Backup e engenharia social

Explicar por que backup é medida de segurança e reconhecer phishing/engenharia social.

Defesa em profundidade

Explicar o conceito de camadas de proteção, com exemplo prático.

Disponibilidade e responsabilidade

Explicar redundância, plano de contingência e por que segurança é tecnologia + processos + pessoas.

Backup: medida de segurança, não só de continuidade

Ransomware criptografa arquivos e exige pagamento para restaurar o acesso.

Um backup confiável — e, idealmente, desconectado da rede principal — é frequentemente a única forma de recuperar os dados sem ceder à extorsão.

Atualizações fecham vulnerabilidades conhecidas

Manter equipamentos, sistemas operacionais, aplicações e firmware atualizados fecha vulnerabilidades conhecidas antes que sejam exploradas por um atacante.

Engenharia social e phishing

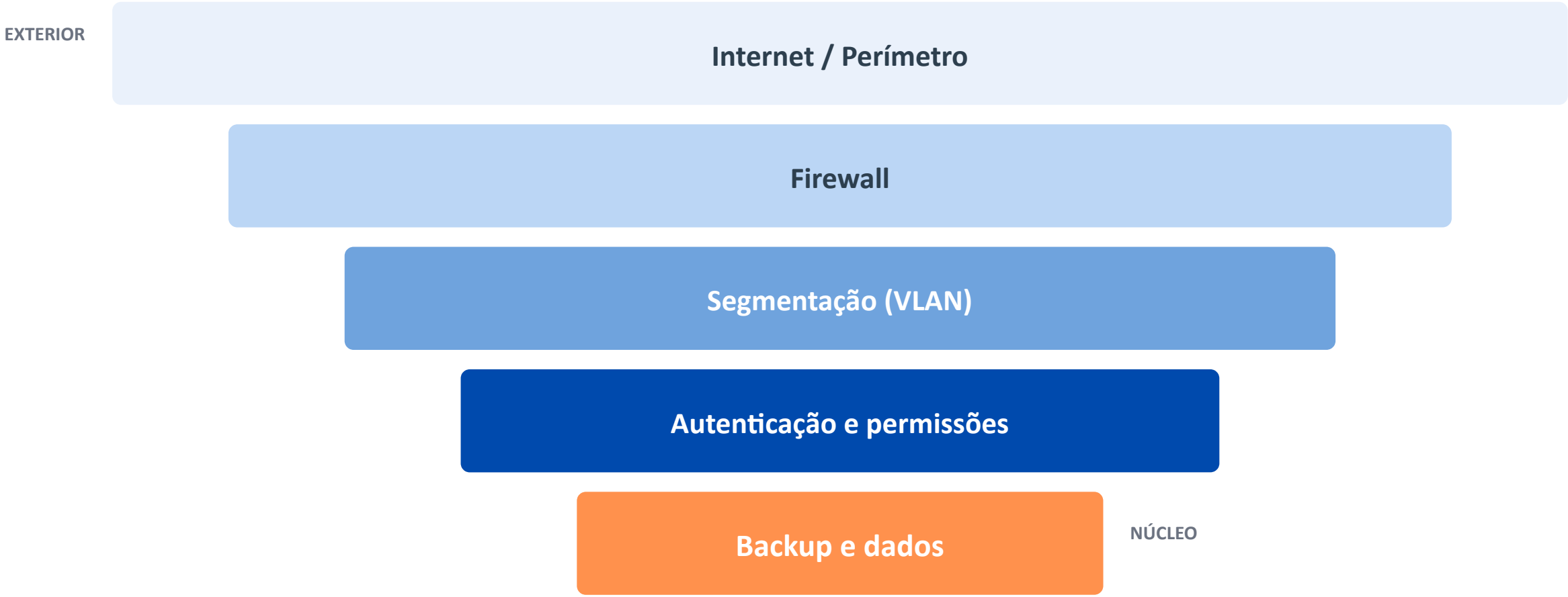
Nem todo ataque é técnico: a engenharia social explora diretamente o fator humano, contornando qualquer proteção puramente tecnológica.

- Phishing: e-mail (ou mensagem) engana o usuário para que ele mesmo forneça credenciais ou clique em um link malicioso.
- Sinais de alerta: urgência artificial, remetente estranho, link suspeito, pedido de senha por e-mail ou telefone.
- Um firewall bem configurado não impede que um funcionário forneça a senha voluntariamente.

- Por isso, treinamento de pessoas é parte da segurança — tanto quanto tecnologia.

Defesa em profundidade: camadas do perímetro ao núcleo

Segurança não deve depender de uma única proteção — se uma camada falhar, as demais ainda protegem o dado mais crítico.



IDEIA CENTRAL

“Segurança não deve depender de uma única proteção.”

Um firewall sozinho não resolve; um antivírus sozinho não resolve; uma senha forte sozinha não resolve. Segurança é construída em camadas.

Redundância: eliminando pontos únicos de falha

Ponto único de falha: componente cuja falha isolada derruba todo o sistema.

Redundância reduz esse risco:

- Dois servidores oferecendo o mesmo serviço
- Duas fontes de alimentação
- Dois links de Internet

Plano de contingência: respostas prontas antes do incidente

Toda organização deveria responder, com antecedência, a perguntas como:

- O que fazer se o servidor principal falhar?
- O que fazer se houver um ataque de ransomware?
- O que fazer se faltar energia?
- O que fazer se o firewall falhar?

Ter essas respostas definidas antes do incidente é a diferença entre recuperação rápida e horas (ou dias) parados.

Segurança é tecnologia, processos e pessoas

Tecnologia

Firewall, antivírus/EDR, IDS/IPS, criptografia, MFA, segmentação, monitoramento.

Processos

Quem acessa o quê, como fazer backup, como responder a incidentes, como recuperar serviços.

Pessoas

Treinamento para reconhecer phishing, proteger senhas e comunicar comportamentos suspeitos.

FECHAMENTO

Resumo para levar da aula

- Backup confiável e desconectado é a defesa mais eficaz contra ransomware — é medida de segurança, não só de continuidade.
- Engenharia social e phishing exploram o fator humano e contornam proteções puramente tecnológicas.
- Defesa em profundidade: perímetro → firewall → segmentação → autenticação/permissões → backup e dados — camadas que se complementam.
- Redundância elimina pontos únicos de falha; plano de contingência prepara respostas antes do incidente acontecer.
- Segurança é uma combinação permanente de tecnologia, processos e pessoas.

Franklin Parrini
Educação e Tecnologia

Obrigado!

Próxima aula: Redes Corporativas e Segmentação (VLAN)