
UNAERP
Universidade de Ribeirão Preto
Campus Ribeirão Preto · Campus Guarujá

Segurança da Informação

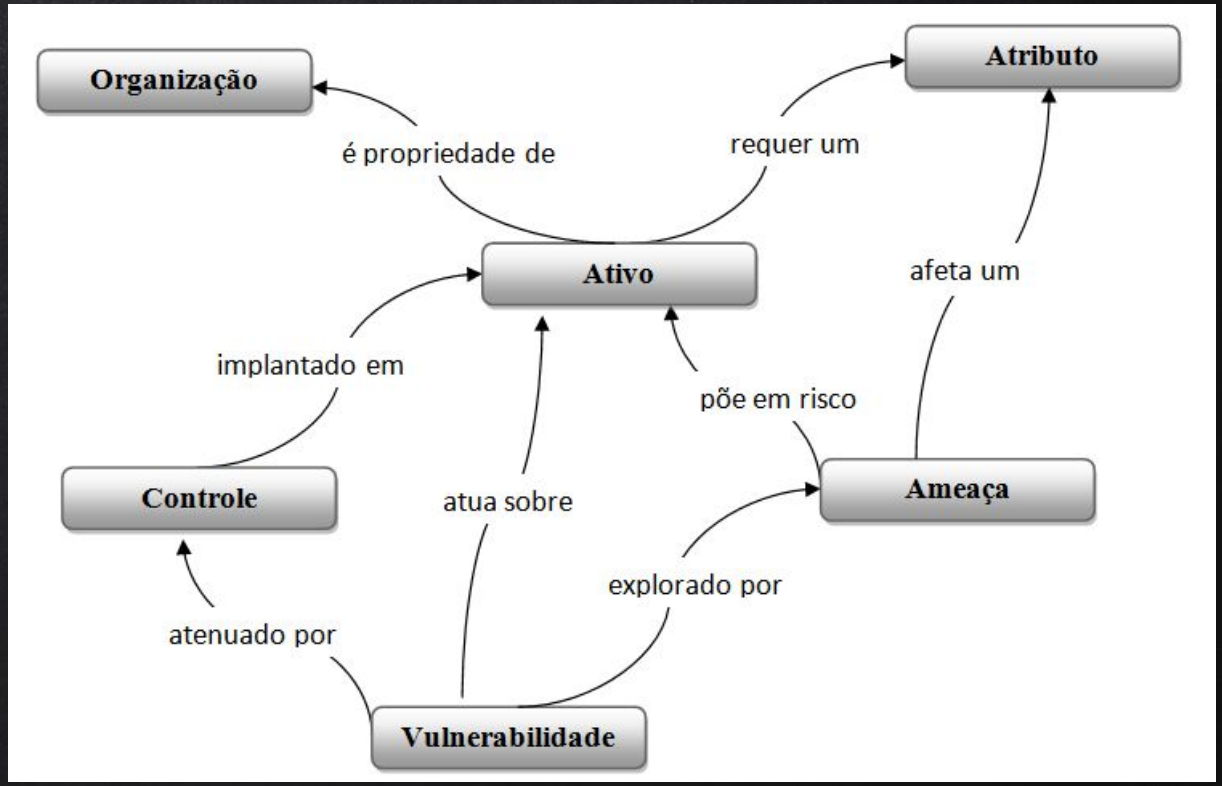
Tópicos Especiais em Engenharia

Novo Cronograma

17/04	Medidas de Segurança Físicas / Medidas de Segurança Técnicas
24/04	Medidas de Segurança Técnicas
01/05	**FERIADO**
08/05	Medidas de Segurança Organizacionais + Simulado
15/05	**AV1**
22/05	Ataques
29/05	Desenvolvimento Seguro
05/06	Desenvolvimento Seguro
12/06	**FERIADO**
19/06	Ferramentas
26/06	Ferramentas
03/07	**AV2**

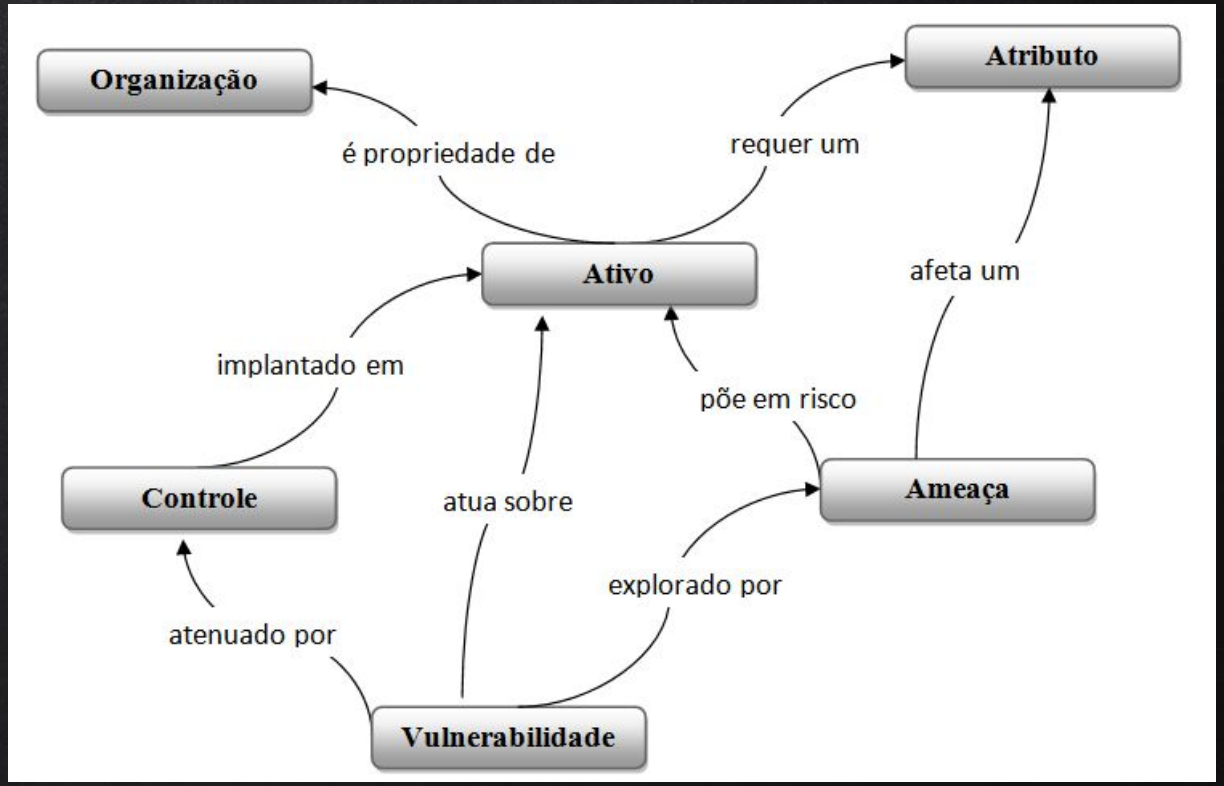
Revisão

Uma **organização** é uma entidade social composta por recursos materiais e humanos, a qual possui objetivos comuns, procedimentos sistemáticos para controle de seu desempenho e limites definidos que a separam do ambiente. Pode ser uma instituição pública ou privada.



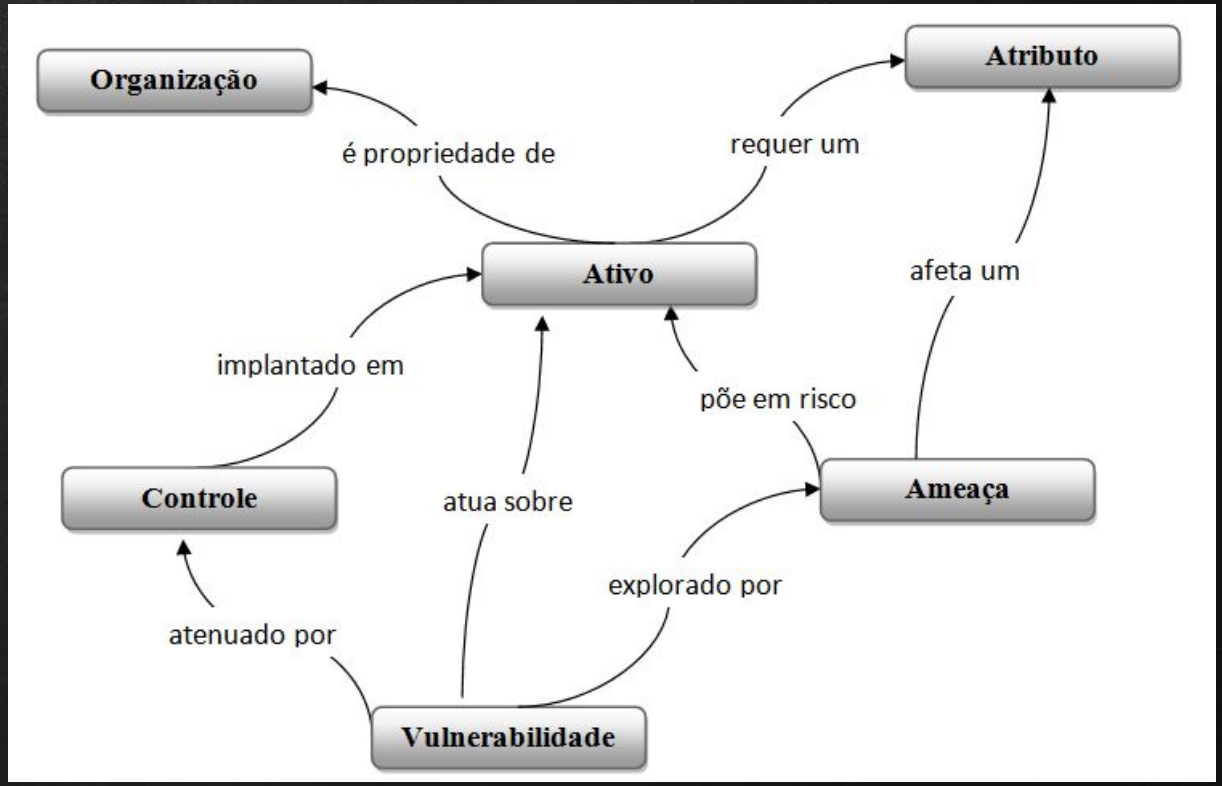
ALMEIDA, M. B.; SOUZA, R. R.; CARDOSO, K. Uma proposta de ontologia de domínio para segurança da informação em organizações. Informação e Sociedade: Estudos, v. 20, n. 1, p. 155-168, 2010.

Um **atributo de segurança** é uma propriedade atribuída a um ativo, a qual diz respeito a requisitos de segurança. Pode ser um atributo de confidencialidade, de integridade e de disponibilidade.



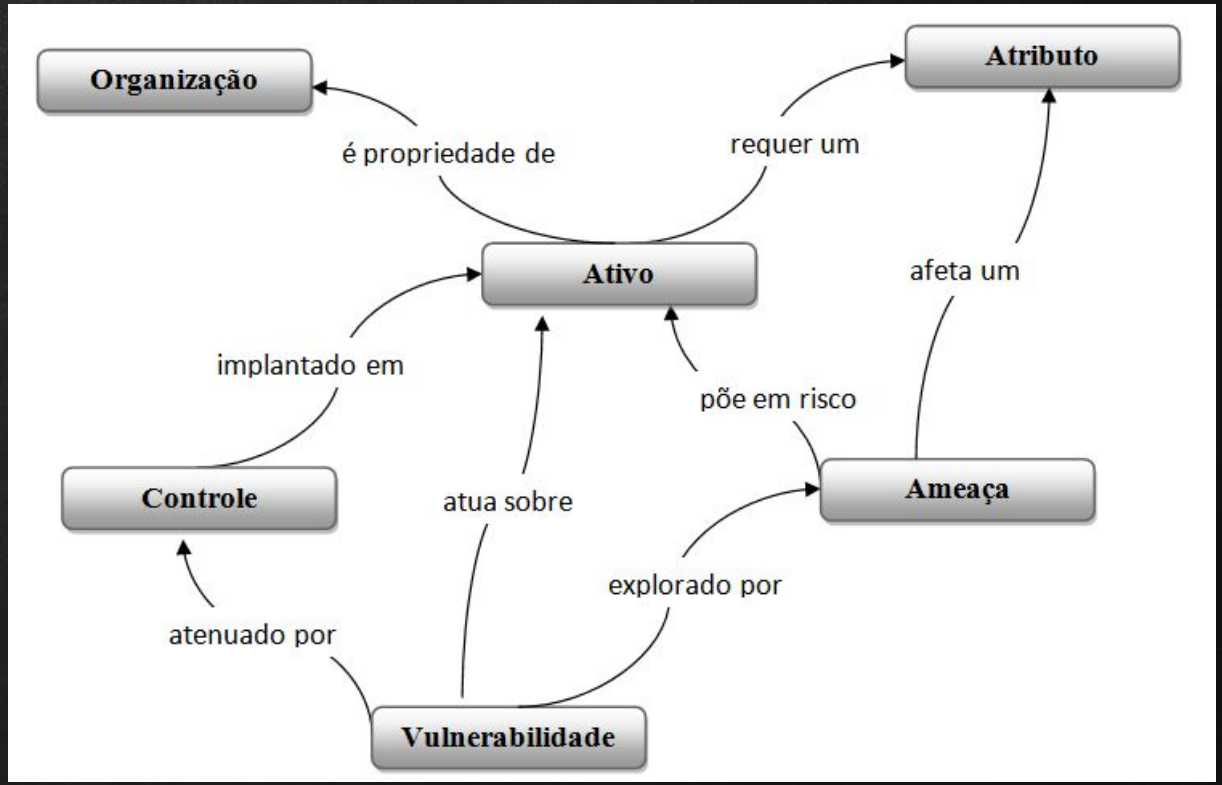
ALMEIDA, M. B.; SOUZA, R. R.; CARDOSO, K. Uma proposta de ontologia de domínio para segurança da informação em organizações. Informação e Sociedade: Estudos, v. 20, n. 1, p. 155-168, 2010.

Um **ativo** é um bem de propriedade da organização, utilizado para alcançar seus objetivos sociais. Pode ser um equipamento, estoque, imóvel, software, dentre outros.



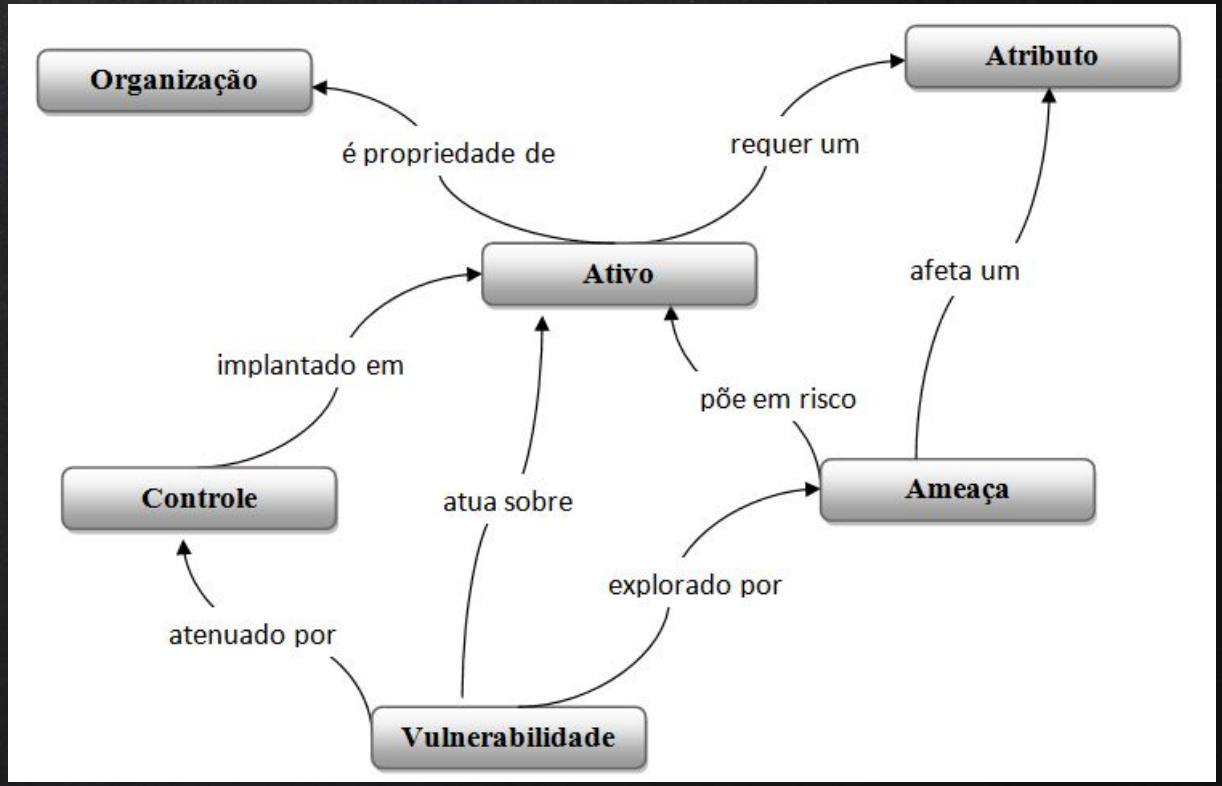
ALMEIDA, M. B.; SOUZA, R. R.; CARDOSO, K. Uma proposta de ontologia de domínio para segurança da informação em organizações. Informação e Sociedade: Estudos, v. 20, n. 1, p. 155-168, 2010.

Um **controle** é um procedimento padrão sistemático implementado para atenuar vulnerabilidades, bem como para proteger ativos através de medidas preventivas e corretivas.



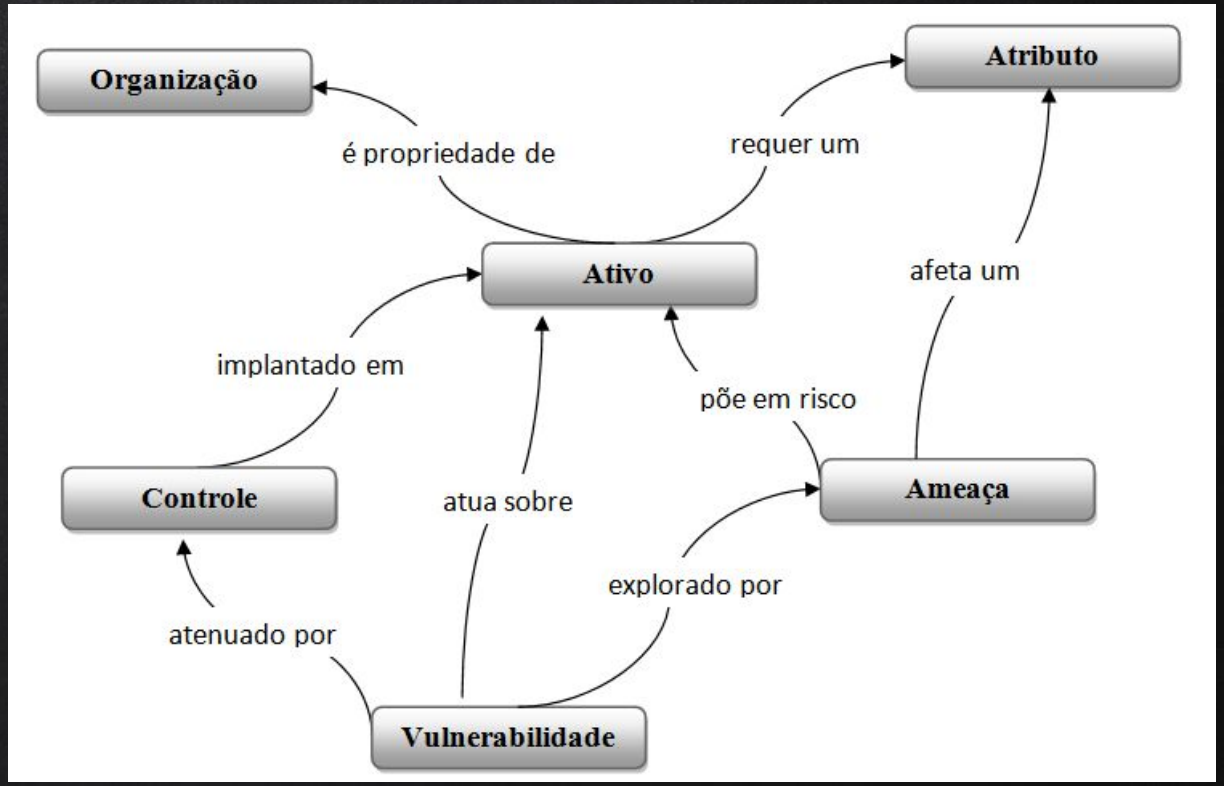
ALMEIDA, M. B.; SOUZA, R. R.; CARDOSO, K. Uma proposta de ontologia de domínio para segurança da informação em organizações. Informação e Sociedade: Estudos, v. 20, n. 1, p. 155-168, 2010.

Uma **ameaça** é uma possibilidade de dano aos ativos da organização, que afeta os atributos de segurança específicos e explora vulnerabilidades da organização. Pode ser de origem humana ou natural e ter como fonte um evento acidental ou uma ação deliberada.



ALMEIDA, M. B.; SOUZA, R. R.; CARDOSO, K. Uma proposta de ontologia de domínio para segurança da informação em organizações. Informação e Sociedade: Estudos, v. 20, n. 1, p. 155-168, 2010.

Vulnerabilidade é uma situação caracterizada pela falta de medidas de proteção adequadas.
Uma vulnerabilidade possui um grau de severidade associado (por exemplo, crítico, moderada ou baixo).
Pode ser uma vulnerabilidade de origem administrativa, técnica ou física.



ALMEIDA, M. B.; SOUZA, R. R.; CARDOSO, K. Uma proposta de ontologia de domínio para segurança da informação em organizações. Informação e Sociedade: Estudos, v. 20, n. 1, p. 155-168, 2010.

Medidas de Segurança

Medidas de Segurança

Físicas

Técnicas

Organizacionais

Medidas de Segurança Física

Prevenir acesso físico não autorizado, danos e interferências

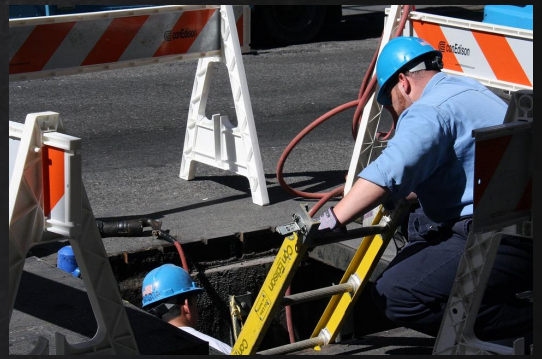
Perímetro de Segurança Física

Área Externa	Prédios	Área de Trabalho	Ativo
Barreiras Naturais Arquitetura Vigilantes Câmeras	Normas Bombeiros Fechaduras	Energia Filmagem Data Center	Armários Cofre corta-fogo Monitoramento
Pública	**Interna**	**Sensível**	**Muito sensível**

É extremamente importante definir de forma **clara** os perímetros de segurança!!!

Controles de Entrada Física

Visitantes



Terceiros

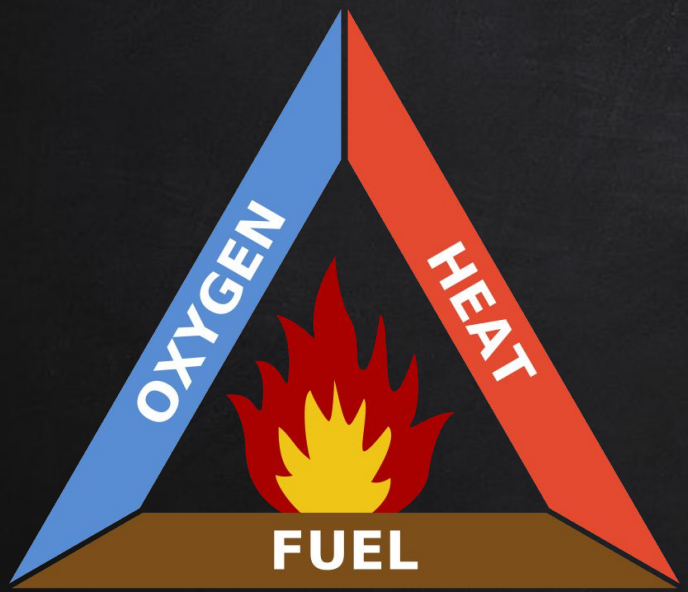
Autorização

Crachá

Projetar Escritórios, Salas e Instalações

- ✘ Aplicar Normas de Saúde
- ✘ Evitar acesso do público a instalações sensíveis
- ✘ Evitar letreiros desnecessários
- ✘ Acesso a listas de funcionários/departamentos/telefones/emails

Ameaças externas e do meio ambiente



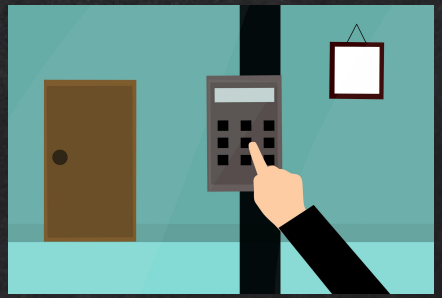
Áreas Seguras (ex: datacenter)

- ✘ Somente quem tiver acesso autorizado pode saber sobre áreas seguras e quais trabalhos são realizados nesses locais
- ✘ Evitar trabalho não monitorado
- ✘ Trancar áreas seguras não ocupadas
- ✘ Não permitir uso de gravadores, celulares, etc. sem autorização
- ✘ Não permitir alimentos / bebidas em áreas seguras

Acesso do público, áreas de entrega e carregamento

Devem ser controlados e se possível isolados das instalações de processamento da informação, para evitar acesso não autorizado

O que pode ocorrer se um controle de segurança física falhar???



BRASIL

| Cidades | Concursos | Educação | Política

01/02/2020 | domtotal.com

Prédio da Previdência pega fogo no Rio de Janeiro

Dataprev é responsável pela gestão da Base de Dados Sociais Brasileira especialmente a do INSS

https://domtotal.com/noticia/1419588/2020/02/predio-da-previdencia-pega-fogo-no-rio-de-janeiro/

Nota

A Dataprev informou, em nota, que o incêndio, que atingiu uma torre de refrigeração do prédio onde funciona a companhia, foi causado por um serviço de solda em uma obra de manutenção que está sendo realizada no local.

"O fogo foi controlado pela brigada de incêndio permanente da empresa, que atuou em parceria com a equipe de vigilância e segurança. A área foi isolada e, quando os bombeiros chegaram, o incêndio já havia sido debelado", diz a nota.

Medidas Técnicas

Mitigar riscos à integridade, confidencialidade ou disponibilidade de informações em formato eletrônico

Como fazer???

- ✘ Combinação de múltiplos controles técnicos, em diferentes camadas lógicas
- ✘ Garantir proteção sem onerar usabilidade
- ✘ Proteção compatível com riscos previamente identificados
- ✘ Nenhuma tecnologia trata todos riscos sozinha!

Camadas de Segurança Lógica

- ✘ Conceito semelhante ao de camadas de segurança física
- ✘ Controles técnicos específicos para cada camada
- ✘ Cloud / Mobile estendem perímetro de proteção lógica

Camadas de Segurança Lógica

Perímetro

Rede

Estações

Aplicações

Dados

- ✘ Contato da rede da organização com o mundo (ex: internet)
- ✘ Controles técnicos
  - Firewall
  - IDS/IPS
  - DMZ
  - DLP
  - Antivírus de borda
  - Honeypot
  - Criptografia

Camadas de Segurança Lógica

- Perímetro
- **Rede**
- Estações
- Aplicações
- Dados

- ✘ Rede interna da empresa
- ✘ Controles técnicos
  - Firewall interno
  - Proteção VOIP
  - Filtro Web
  - NAC
  - Controles de Redes Wireless
  - Controles de acesso remoto
  - DLP
  - Segmentação
  - Criptografia

Camadas de Segurança Lógica

- Perímetro
- Rede
- **Estações**
- Aplicações
- Dados

- ✘ Estações dos usuários da empresa
- ✘ Controles técnicos
  - Anti-malware
  - Firewall local
  - IPS/IDS local
  - Criptografia
  - Atualizações de Segurança
  - DLP

Camadas de Segurança Lógica

- Perímetro
- Rede
- Estações
- **Aplicações**
- Dados

- ✘ Aplicações usadas pela organização
- ✘ Controles técnicos
  - Revisão de código fonte
  - Análise de vulnerabilidade
  - WAF (Firewall de aplicação)
  - Criptografia
  - Atualizações de Segurança
  - DLP
  - Controle de acesso lógico

Camadas de Segurança Lógica

- Perímetro
- Rede
- Estações
- Aplicações
- **Dados**

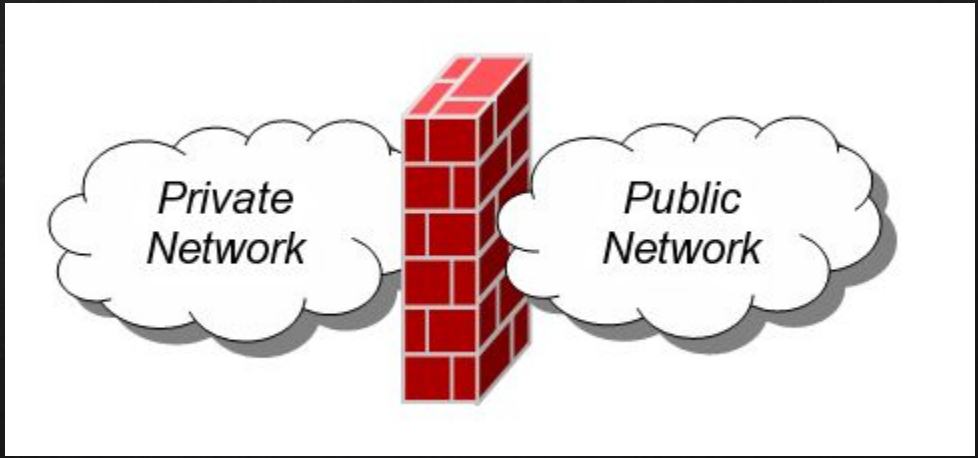
- ✘ Informações da organização
- ✘ Controles técnicos
  - Gestão de acesso
  - Backup
  - DLP
  - Criptografia

Camadas de Segurança Lógica

- ✘ Monitoramento e Resposta são transversais
- ✘ Controles técnicos aplicáveis:
  - SIEM
  - Threat Hunting
  - Threat Intelligence
  - Dashboards e Relatórios
  - Gestão de Incidentes
  - Forense Digital

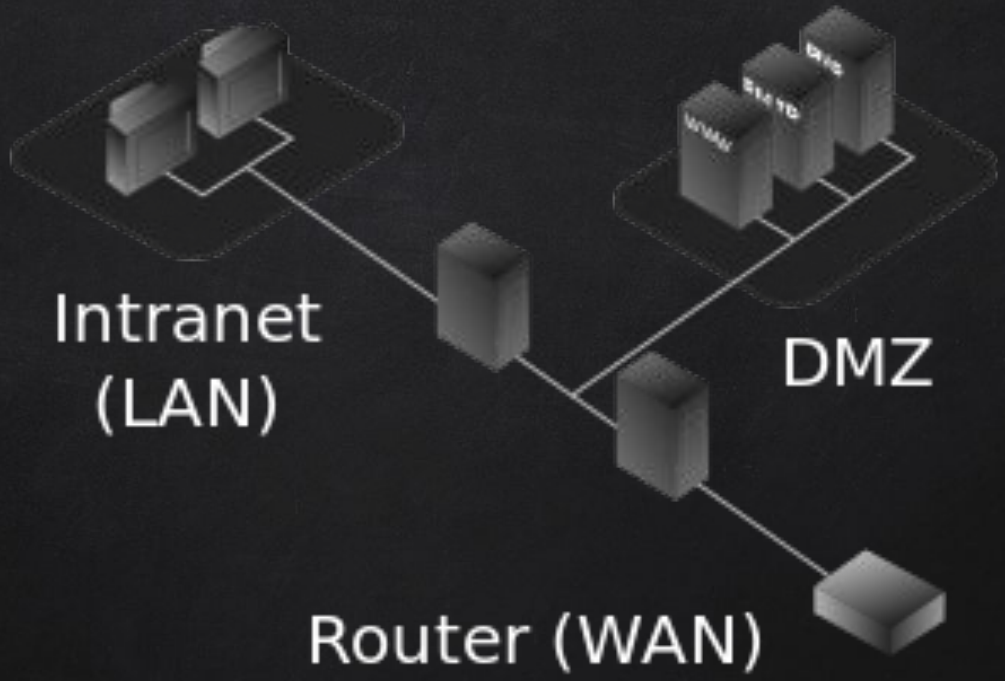
Firewall

- ✘ Dispositivo de segurança de rede
- ✘ Hardware / Software
- ✘ Monitoramento de tráfego de rede (entrada/saída)
- ✘ Conjunto de regras de segurança (permitir/bloquear)



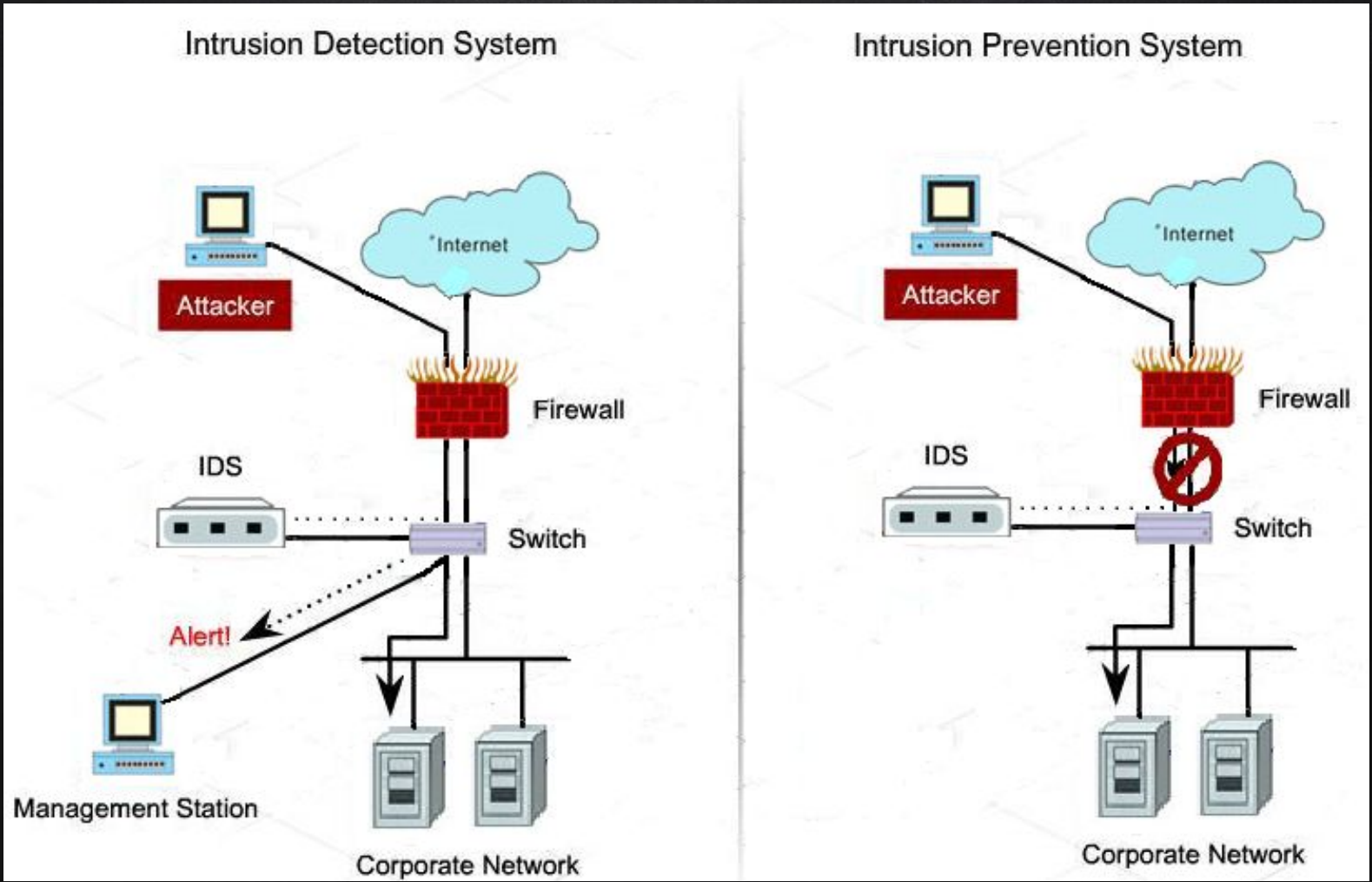
DMZ

- ✘ Segmento de rede que expõe serviços a uma rede não confiável



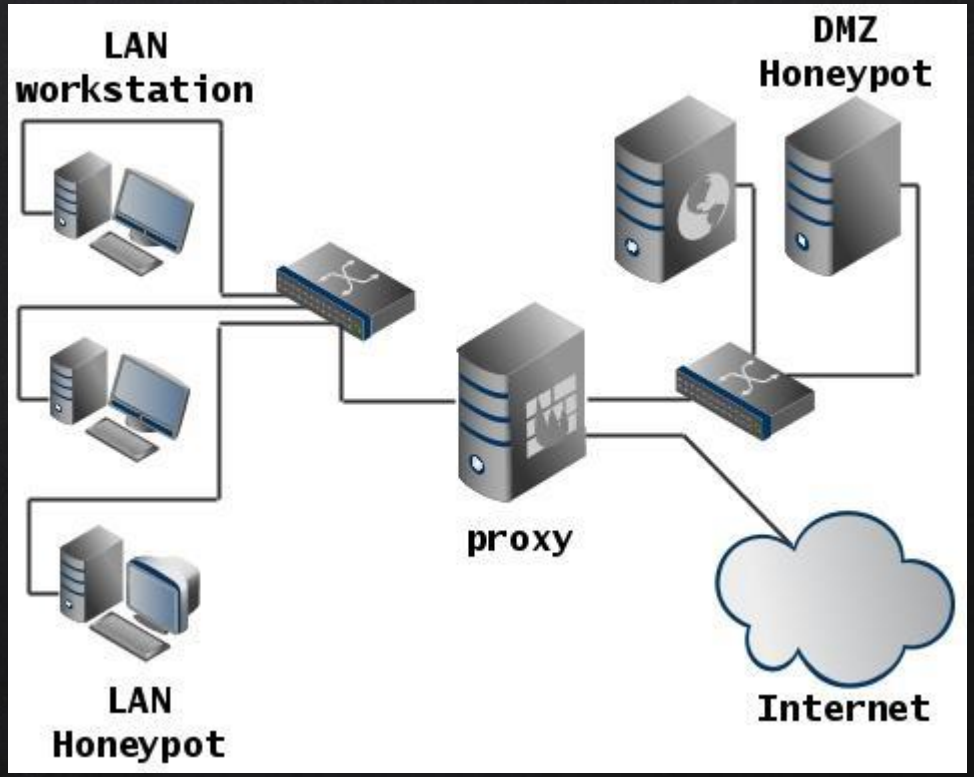
IDS / IPS (Detecção e prevenção de intrusão)

- ✘ Hardware / Software
- ✘ IDS – Intrusion detection system
  - detectar e alertar possíveis ataques e tentativas de acessos indevidos
- ✘ IPS – Intrusion prevention system
  - detectar e alertar possíveis ataques e tentativas de acessos indevidos
  - toma ações para bloquear a ameaça


Intrusion Detection System
Internet
Attacker
Firewall
IDS
Switch
Alert!
Management Station
Corporate Network
Intrusion Prevention System
Internet
Attacker
Firewall
IDS
Switch
Corporate Network

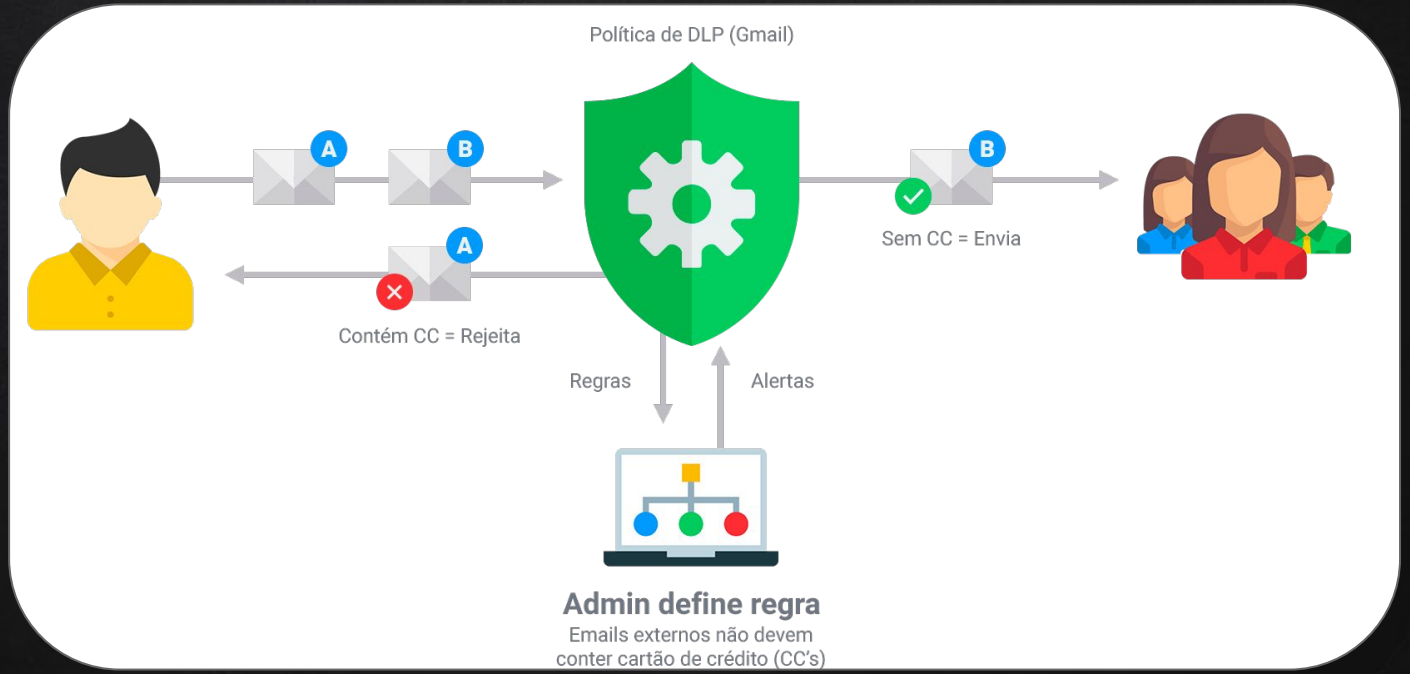
Honeypot

- ✘ Recurso de rede para ser atacada/invadido
- ✘ Identifica atacantes



DLP (Prevenção contra Vazamentos de informação)

- ✘ Data Loss Prevention
- ✘ Identifica e monitora dados
- ✘ Garantir somente acessos autorizados
- ✘ Prevenir tentativas de vazamento

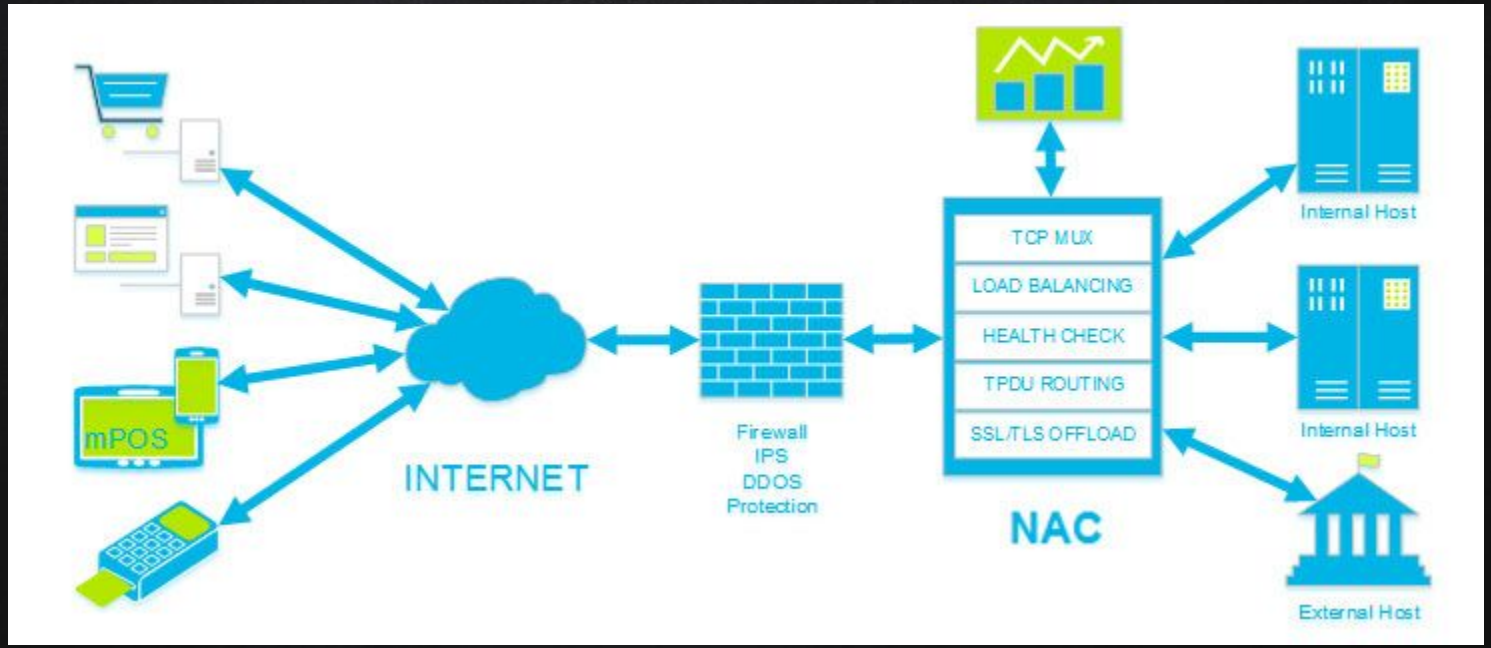


WebFilter

- ✘ Verifica se usuário pode ou não acessar determinados conteúdos

NAC (Controle de Acesso à Rede)

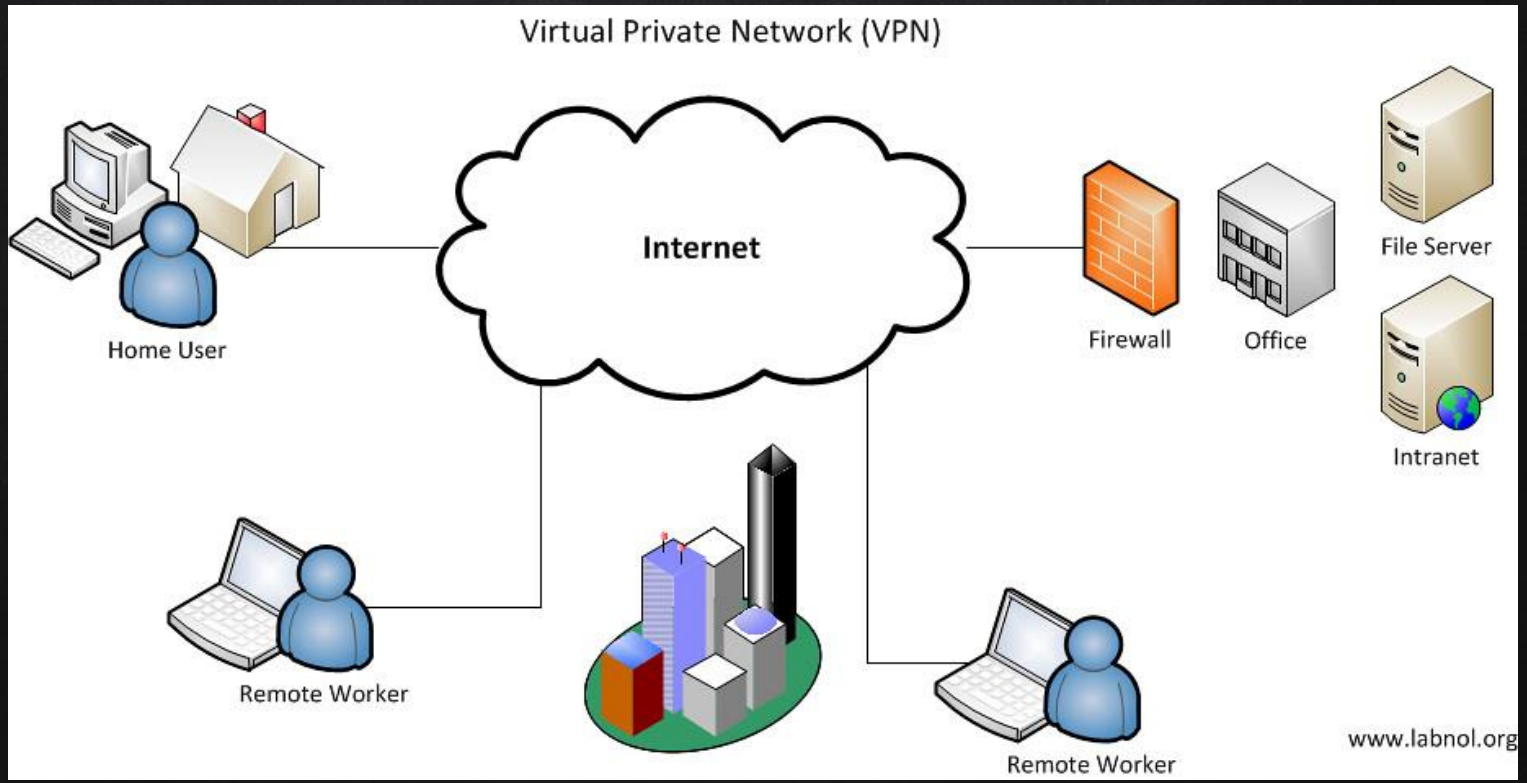
- ✘ Apenas dispositivos compatíveis com regras de segurança podem acessar rede
- ✘ BYOD (Bring Your Own Device)



https://www.diariodeti.com.br/controle-rede-nac-network-access-control/

VPN (Rede Privada Virtual)

- ✘ Conexão segura/criptografada em uma rede menos segura (Internet)



Revisão de Código-Fonte

- ✘ Examinar código fonte para identificar erros de segurança
- ✘ Manual / Automática
- ✘ Estática: ~~(execução)~~ / Dinâmica: (execução)

https://owasp.org/www-community/Source_Code_Analysis_Tools

Análise de Vulnerabilidades

- ✘ Definir, identificar, classificar e priorizar vulnerabilidades em softwares, apps e infra de rede
- ✘ Conscientização e histórico de risco
- ✘ https://www.zaproxy.org/

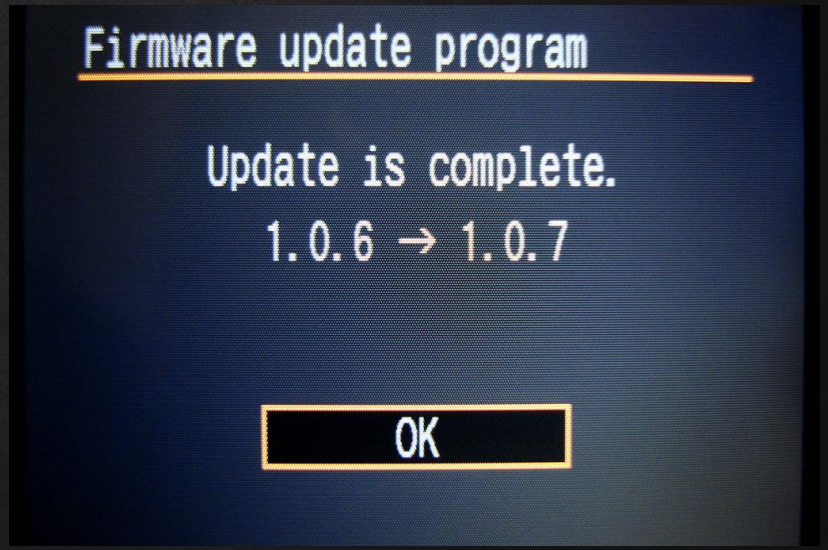
Teste de Intrusão

- ✘ Simular ataque para encontrar vulnerabilidades
- ✘ White / Gray / Black box

Análise de Vulnerabilidade X Teste de intrusão

- ✘ AdV
  - Reconhecimento
  - Varredura
  - Relatório
- ✘ TdI
  - Reconhecimento
  - Varredura
  - Exploração
  - Manutenção de acesso
  - Relatório

Atualizações de Segurança



Backups

- Processo de cópia de dados para que possam ser recuperados

Tipo	Dados copiados	Tempo de Cópia	Tempo de Restore	Espaço
Completo (Full)	Todos os dados	Lento	Rápido	Alto
Diferencial	Dados desde o último backup	Moderado	Rápido	Moderado
Incremental	Somente arquivos/pastas novos/modificados	Rápido	Moderado	Baixo

Outras medidas Técnicas

- ✘ Criptografia
- ✘ Certificado Digital
- ✘ Proteção contra códigos maliciosos

DÚVIDAS?

- ✘ Não esqueça de enviar sua maior dúvida pelo link que está no ClassRoom.
- ✘ Críticas/Sugestões: ezarpelao@unaerp.br
- ✘ Próxima aula: Medidas Técnicas

Credits

Special thanks to all the people who made and released these awesome resources for free:

- ✘ Presentation template by SlidesCarnival
- ✘ Photographs by Unsplash