ATITUS
EDUCAÇÃO

Ciência da
Computação

Ciência da Computação

Segurança da Informação

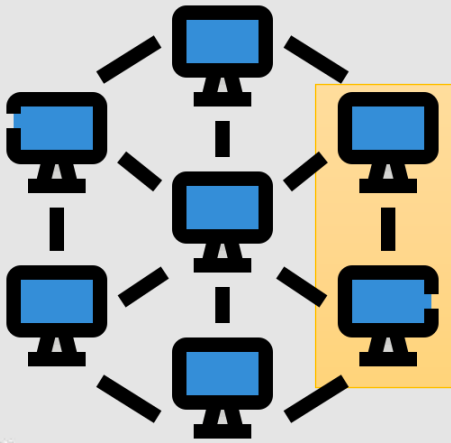
ATITUS EDUCAÇÃO

Prof(a). Vitória Paczek

vitoria.paczek@atitus.edu.br

Pré-Internet

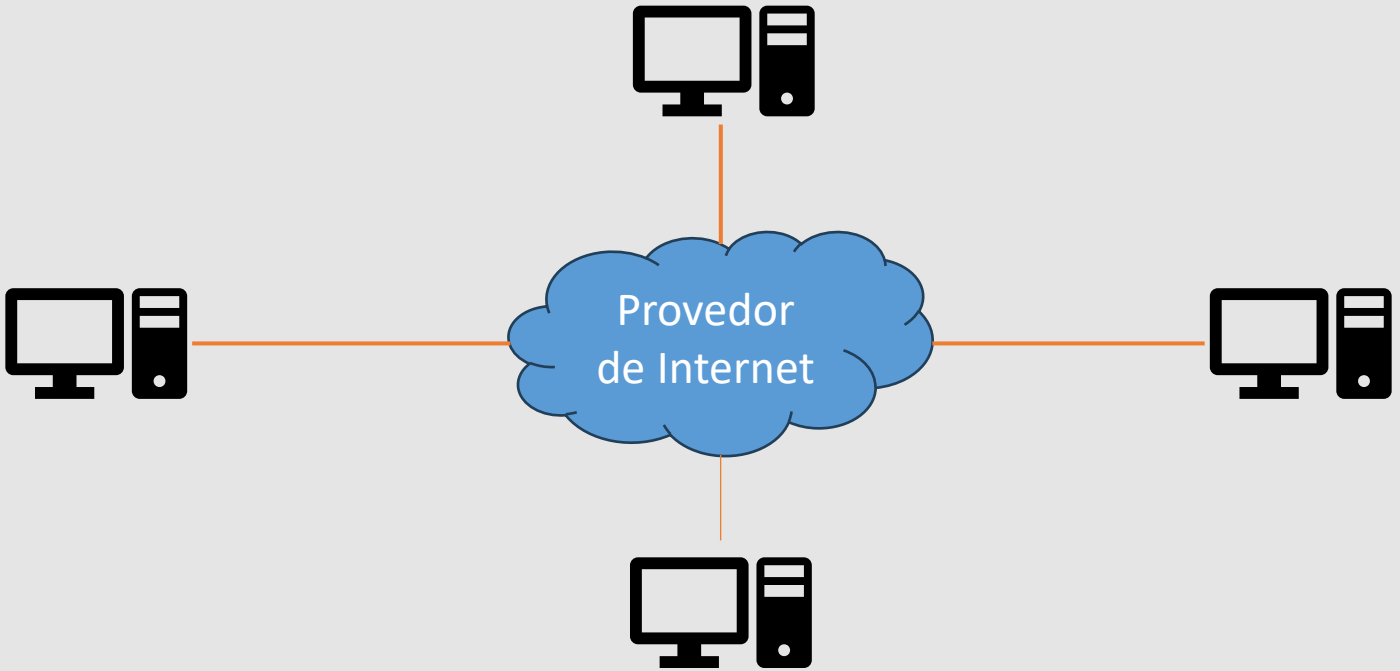
- Redes privativas
- Soluções proprietárias
- Recursos individualizados
- Poucos Computadores;



Poucas empresas e universidades se conectavam diretamente para trocar informações

Pós-Internet

- Compartilhamento de Recursos
- Adoção de padrões abertos de comunicação
- Muitos computadores conectados



Segurança da Informação: Conceito

"Proteção dos sistemas de informação contra acessos, uso, divulgação, interrupção, modificação ou destruição não autorizada, a fim de fornecer confidencialidade, integridade e disponibilidade" – NIST

Cibersegurança: Conceito

Práticas para atingir a integridade, confiabilidade e disponibilidade no meio digital.

Segurança da Informação: Lógico e Físico

Cibersegurança: Digital

Conceitos Básicos de Segurança da Informação

Ativo

- Qualquer coisa que tenha valor para um indivíduo. Hardware, Software, Pessoas,etc...

Ameaça

- Causa potencial de um incidente indesejado, caso ocorra vira um dano

Impacto

- Consequência de um incidente

Risco

- Probabilidade da concretização da Ameaça

Vulnerabilidade

- Fragilidade/limitação de um ativo que pode ser explorada pela ameaça

Segurança Digital: O problema!

- Dados que circulam na Internet passam por equipamentos de terceiros sem grande controle dos donos desses dados;

- Dados armazenados em computadores conectados contêm várias informações potencialmente valiosas;

Segurança Digital: O problema!

Nas décadas de 80-90 surgiram vários hackers por diversos motivos como fama, curiosidade, poder, desafio,etc...;

Os mais famosos foram: Adrian Lamo, Kevin Mitnick e Kevin Poulsen

Segurança Digital: O problema!

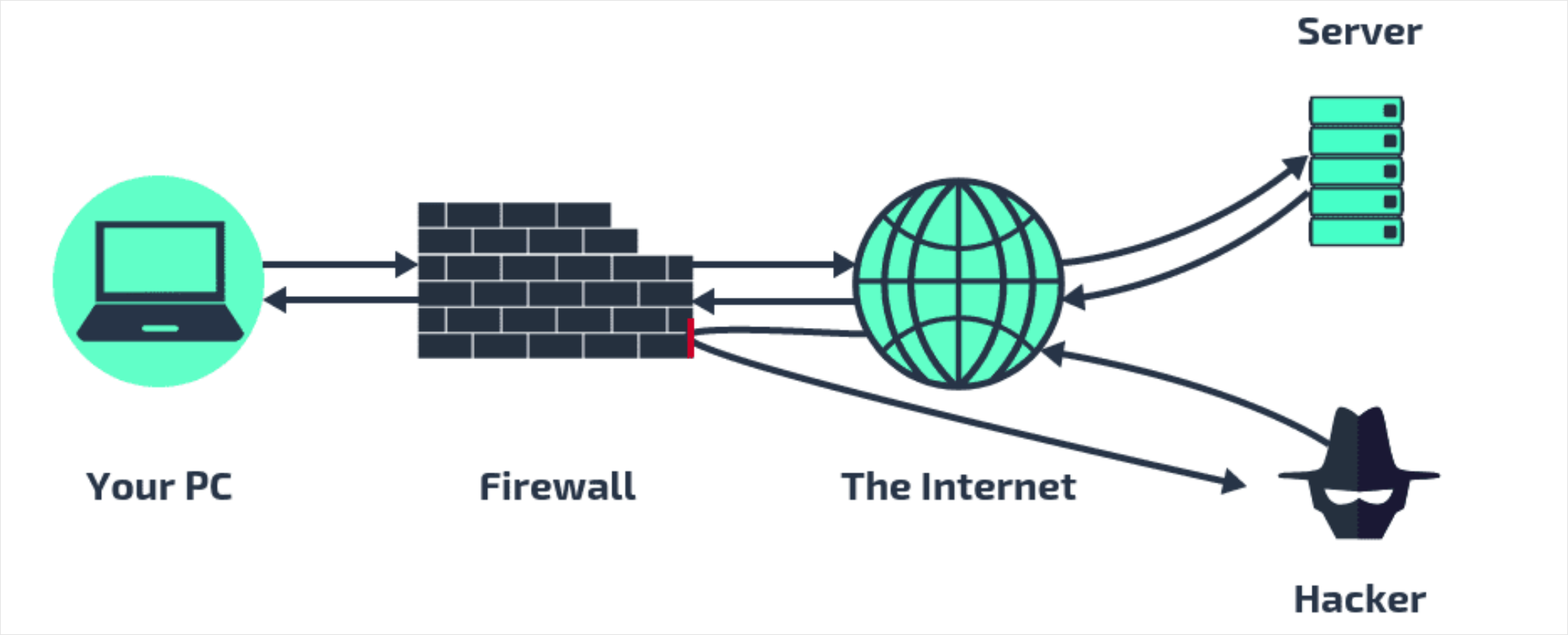
Quando a internet se popularizou um novo grupo de hackers foi formado com objetivo malicioso para ganhar dinheiro, espionagem, etc...

Esse grupo ficou conhecido como Crackers

Os mais famosos foram: Raphael Gray(23k cartões de crédito roubados/clonados), Vladimir Levin(Citibank, 10M Doláres desviados), Albert Gonzalez(1.5M de cartões roubados/clonados e vendas de dados pessoais(passaporte, identidades, etc...) em leilão

Modelo para segurança de redes

Modelo para segurança de redes



Ameaças – Fator Humano

É a **maior ameaça** à segurança cibernética empresarial.

Os usuários, em geral, de todas as áreas de uma organização são um buraco intrínseco de segurança.

Uma **ameaça interna** ou **Insider** é uma grande preocupação para todas as organizações. Geralmente, ela é consequência do acesso e do uso errado de dados sensíveis, incluindo o vazamento de dados aos fornecedores para minar os poderes de negociação da companhia.

Ameaças – Scan

É um ataque que **quebra** a confidencialidade com o objetivo de analisar detalhes dos computadores presentes na rede (como sistema operacional, atividade e serviços) e identificar possíveis alvos para outros ataques.

A principal forma de prevenção é a manutenção de um firewall na empresa e uma configuração adequada da rede.

Ameaças – Worm

Worms são alguns dos malwares mais comuns e antigos. Malwares são softwares com o intuito de prejudicar o computador “hospedeiro”.

Os worms são perigosos devido à sua **capacidade se espalhar rapidamente** pela rede e afetar arquivos sigilosos da empresa.

Ameaças – Rootkit

Tem como objetivo fraudar o acesso, logando no sistema como root, ou seja, usuário com poder para fazer qualquer coisa.

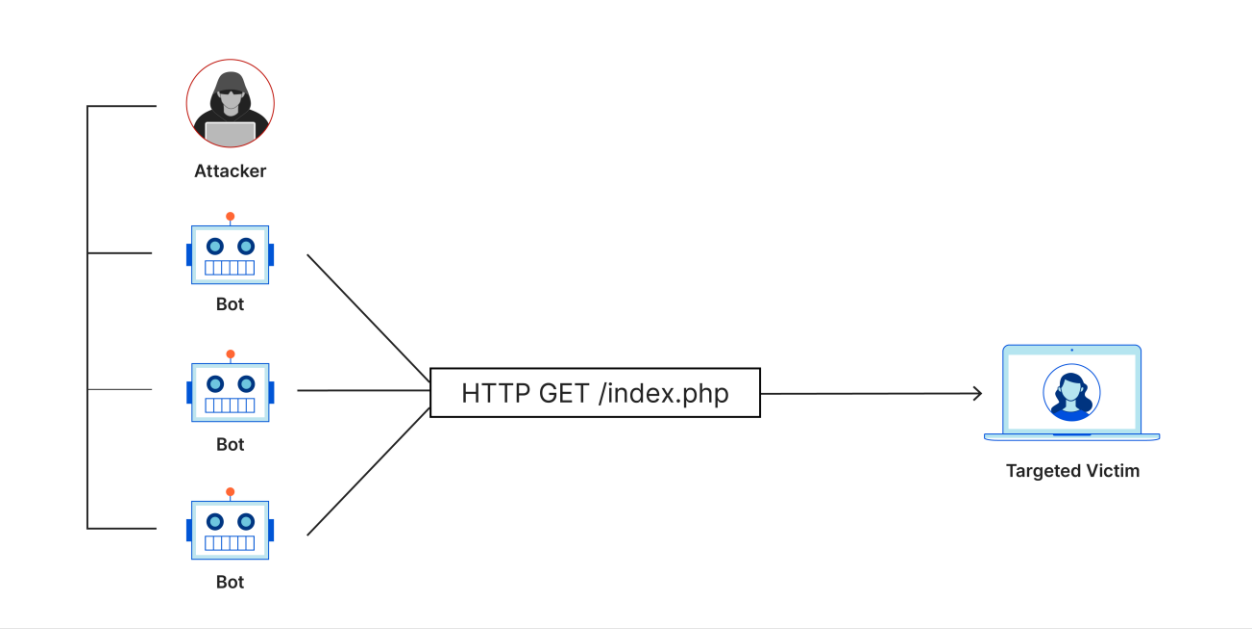
Quando a máquina é infectada, os arquivos maliciosos se escondem no sistema e, com essa discrição, liberam o caminho para os invasores agirem.

Apesar de seu surgimento no Linux, o malware é capaz de causar danos nos sistemas operacionais Windows e Mac. Sem dúvidas, trata-se de um grande perigo para ambientes corporativos.

Ameaças – DDoS (Distributed Denial of Service)

São os ataques mais frequentes.

Tem como objetivo tornar o sistema, infraestrutura ou servidores indisponíveis, causando a interrupção do serviço.



Ameaças – Ransomware

São hoje as maiores ameaças.

O modo como o ransomware age varia conforme a sua versão, pois cada malware lançado explora **uma diferente brecha do sistema operacional**. Esse detalhe, inclusive, é o que torna os ataques tão repentinos e, ao mesmo tempo, fatais.

Embora a maneira como o vírus se manifesta varie, a finalidade é a mesma: bloquear todos os arquivos do computador, impedindo que o sistema possa ser utilizado adequadamente, e encaminhando mensagens solicitando o pagamento pelo resgate.

Ameaças – Phising

A prática de phishing consiste no envio de mensagens de email, onde o invasor se passa por uma instituição legítima e confiável (geralmente bancos e serviços de transação online), induzindo a vítima a passar informações cadastrais.

Ameaças – Phising – Como identificar

Suspeite de ligações urgentes ou ameaças desconhecidas. O imediatismo no discurso dos phishers é uma das principais armas para conquistar a atenção da vítima. Por isso, nunca clique em links, abra anexos ou informe os seus dados rapidamente. Observe cuidadosamente o remetente da mensagem, o contexto da conversa e confirme a procedência da informação, antes de tomar qualquer atitude.

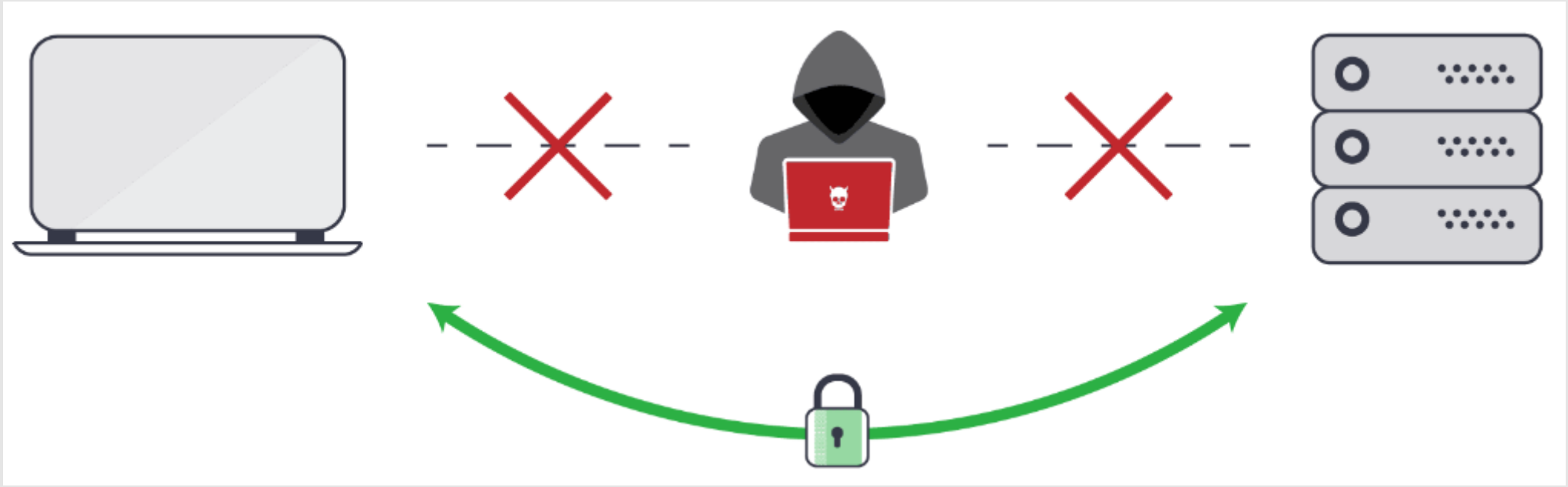
Linguagem genérica. Como o objetivo do phishing é atacar o máximo de vítimas possível, é comum que a abordagem utilizada seja generalizada.

Domínio ou número incompatíveis com os canais oficiais. Quando uma empresa legítima entra em contato com o cliente, ela utiliza seus canais e domínios oficiais. Para enganar o usuário, os criminosos costumam criar variações com pequenos erros ortográficos ou símbolos. Por isso, antes de agir, preste muita atenção no remetente da mensagem e por onde ela está sendo enviada. Acesse os sites e redes sociais oficiais para conferir a informação.

Links e anexos suspeitos. Se uma mensagem parece duvidosa, não clique ou baixe o conteúdo imediatamente. Avalie os sinais que citamos acima e para ter ainda mais segurança, passe o mouse sobre o link para conferir se a informação é compatível.

Ameaças – Man-In-The-Middle

Durante o ataque man-in-the-middle, a comunicação é interceptada pelo atacante e retransmitida por este de uma forma discricionária. O atacante pode decidir retransmitir entre os legítimos participantes os dados inalterados, com alterações ou bloquear partes da informação.



Como podemos nos prevenir?

- Identificar possíveis ataques;
- Tenha backups dos seus dados;
- Tenha um antivírus eficaz;

Em duplas!

Atividade!

Pesquise os maiores cibercrimes da história e qual foi o método utilizado.

Cite também qual foi o crime e prejuízo assim como a sua resolução penal(se houver).

Monte um material (word/pdf) e compartilhe com a professora através do e-mail vitoria.paczek@atitus.edu.br

OBRIGADA

Ciência da
Computação

Passo Fundo / Porto Alegre / Ijuí