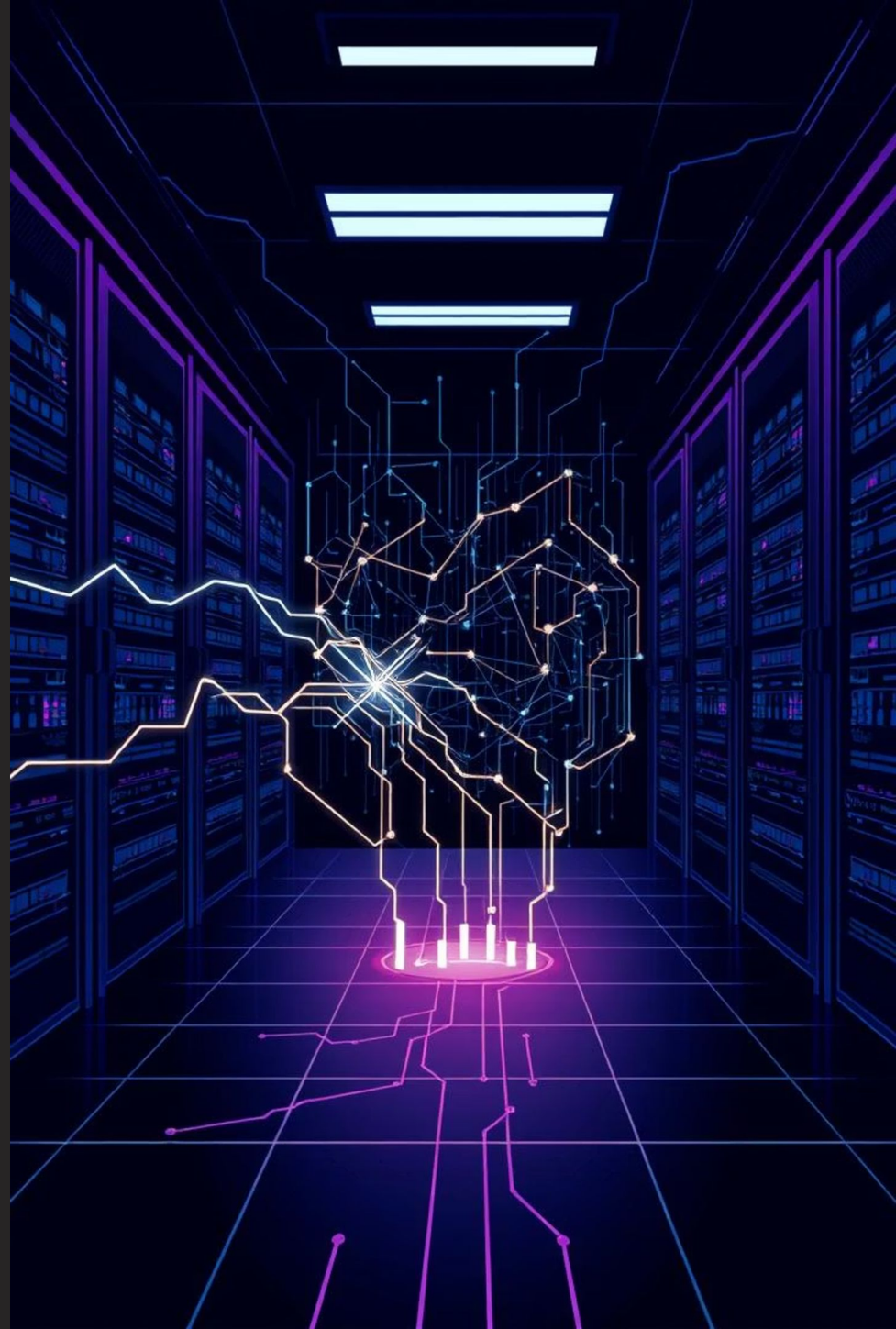
Anatomia de um Ataque Cibernético: Entenda as 5 Etapas Críticas

Nesta apresentação, vamos desvendar as complexas camadas de um ataque cibernético, explorando cada fase desde a motivação inicial até a extração final de dados. Compreender essa anatomia é crucial para fortalecer as defesas e proteger ativos digitais valiosos.



O Ponto de Partida

Por que os ataques acontecem?

Ganância Financeira

Atacantes buscam lucro através de resgates (ransomware) ou venda de dados sigilosos.

Espionagem Corporativa

Concorrentes ou grupos organizados visam informações confidenciais para vantagem competitiva.

Manipulação de Mercado

Informações vazadas podem ser usadas para influenciar preços de ações ou desestabilizar empresas.

Insatisfação Interna

Ex-funcionários ou insiders buscam vingança ou causar danos por descontentamento.

> Um ataque cibernético não é aleatório. Ele é precedido por um estudo minucioso da organização, suas pessoas e seus processos, visando identificar a porta de entrada mais vulnerável.

Reconhecimento e Coleta de Informações

Na fase inicial, o atacante coleta o máximo de informações sobre o alvo, atuando como um investigador antes de agir diretamente.

Mapeamento de Pessoas: Pesquisa de nomes, cargos, e departamentos de colaboradores-chave através de redes sociais (LinkedIn, Facebook), sites corporativos e outras fontes públicas. A ideia é criar um "organograma" informal da empresa e identificar quem possui acesso a informações sensíveis.

Análise de Processos e Setores: Busca por informações sobre o funcionamento interno da empresa, suas rotinas, tecnologias utilizadas e pontos fracos em processos de negócio.

Identificação de Credenciais Valiosas: O foco é encontrar qualquer rastro de credenciais de acesso que possam ser reutilizadas ou adivinhadas, abrindo caminho para áreas críticas como o setor financeiro ou administrativo.

Ferramentas Avançadas: Hoje, essa etapa é amplificada pelo uso de ferramentas automatizadas e até inteligência artificial, que podem compilar vastas quantidades de dados de fontes abertas (OSINT) em tempo recorde, tornando o reconhecimento mais eficiente e difícil de detectar.

Engenharia Social, Phishing e Comprometimento Inicial

Engenharia Social e Phishing

Com base nas informações coletadas na fase de reconhecimento, o invasor constrói um ataque altamente direcionado. A tática mais comum é o **phishing**, que pode ser geral ou um **spear phishing** personalizado.

E-mails Fraudulentos: Mensagens que imitam comunicações legítimas da empresa (TI, RH, gerência) ou de serviços conhecidos (bancos, redes sociais).

Páginas Falsas: Ao clicar em links maliciosos, o usuário é redirecionado para páginas que visualmente parecem idênticas às originais, mas que são projetadas para roubar credenciais.

Comprometimento Inicial

Com as credenciais em mãos, o cracker consegue o primeiro acesso à rede corporativa. Este é o ponto de virada, onde a teoria se torna ação.

Mapeamento de Sistemas: Uma vez dentro, o invasor começa a explorar a rede, identificando sistemas, computadores conectados, servidores e softwares.

Busca por Vulnerabilidades: O objetivo é encontrar falhas de segurança ou configurações incorretas que permitam escalar privilégios ou mover-se livremente pela rede.

Vulnerabilidades:

Segurança 360°

Implementar uma estratégia de segurança holística, que contemple desde a educação do usuário até a proteção de dispositivos IoT e segmentação de rede.

Treinamento Continuo

Capacitar funcionários para serem a primeira linha de defesa, reconhecendo e evitando ameaças comuns como engenharia social.

Varreduras

Realizar pentests e varreduras de vulnerabilidades regularmente para identificar e corrigir falhas antes dos atacantes.

Conclusão: Entender cada etapa de um ataque cibernético não é apenas conhecimento, é uma necessidade vital para empresas e indivíduos. Ao antecipar as táticas dos invasores, é possível implementar defesas proativas e mitigar prejuízos catastróficos, protegendo a integridade, a reputação e os ativos da organização.

Bruno de Oliveira Santos - 8232235123

Guilherme Dourado Nascimento - 825116419

Felipe Pereira do Nascimento - 825126069

Kauane Sandes Brandão - 825113309

Stephanny Ramos Rodrigues -825123391

Pedro Miranda Rabelo - 825243591