

Reunião CSI 31/08/2022

1 Participantes

Hebert Pinheiro, Antonio Ferreira, Gualter Gonçalves, Leana Neves, Gustavo Adriano, Daniele Cavaignac, Wellington Silva, Alysson Cristiano,

2 OSINT

2.1 Busca de informações em Fontes Abertas (OSINT)

2.1.1 Redes sociais

2.1.2 Sites Jurídicos

2.1.3 <https://www.tre-ma.jus.br/o-tre/conheca-o-tre-ma/organograma-contatos>

2.2 No tripé da SegInfo, formado por tecnologia, processos e pessoas, estas representam, provavelmente, o principal ponto de fragilidade (no jargão da área, são “o elo mais fraco da corrente”). A título de exemplo, é bem mais fácil um invasor ter sucesso induzindo o usuário a clicar em um link ou abrir um anexo de e-mail e, com isso, instalar um software malicioso no próprio computador, do que explorando alguma vulnerabilidade de rede.

2.3 Componente chave para realização de invasão

2.3.1 Perfil da empresa/instituição

2.3.2 Perfil das pessoas

2.3.3 Investigação de falhas conhecidas

2.3.4 Infraestrutura voltada para internet

2.4 Técnicas

2.4.1 Engenharia Social

2.4.1.1 *Conceito*

2.4.1.1.1 é o ato de persuadir uma pessoa a revelar informações necessárias para a realização do seu ato criminoso

2.4.1.1.2 tem como alvo o elo mais fraco da segurança da informação, que é o ser humano

2.4.1.1.3 formas mais antigas de manipulação da confiança de uma pessoa com a finalidade de obter informações privilegiadas

2.4.1.1.4 utiliza de manipulação psicológica

2.4.1.2 *Estudo do comportamento humano*

2.4.1.2.1 Evitar exposição: redes sociais

2.4.1.2.2 Roubo de identidade

2.4.1.2.3 Fato ou Boato - TSE

<https://www.justicaeleitoral.jus.br/fato-ou-boato/>

2.4.2 Phishing

2.4.2.1 É uma técnica utilizada por pessoas mal-intencionadas cujo único propósito é conseguir informações confidenciais como: nome de usuário, senha, códigos de acesso, números de conta corrente ou dados de cartão de crédito

2.4.2.2 Normalmente a mensagem vem acompanhada com uma ameaça com ultimato: bloqueio de conta bancária: ter sua senha desativada, perda de acesso a algum sistema, etc

2.4.2.3 Envio de e-mails, ligações, SMS

2.4.2.3.1 Remetente desconhecido

2.4.2.3.2 Links desconhecidos no corpo da mensagem

2.4.2.3.3 Erros de escrita

2.4.2.3.4 Mensagens suspeitas (ex.: "Hora-Extra", "Aumento Salarial", "Super promoção até hoje", "você está sendo traído", "sua conta foi invadida")

2.4.2.4 4 fases

2.4.2.4.1 1 - Envio da mensagem por e-mail para a vítima;

2.4.2.4.2 2 - Recepção da mensagem pela vítima para que ela tome uma ação rapidamente sem pensar muito sobre o assunto

2.4.2.4.3 3 - Acesso ao site falso (réplica) pela vítima

2.4.2.4.4 4 - Digitação das informações requeridas pelo atacante no site falso.

2.4.2.5 Tipos

2.4.2.5.1 Por voz - Vishing

2.4.2.5.2 Pessoalmente

2.4.2.5.3 Digital

2.4.2.6 Formas de Evitar

2.4.2.6.1 Caso não tenha solicitado nenhum e-mail considere que esse e-mail é uma tentativa de phishing.

2.4.2.6.2 Caso não tenha solicitado o arquivo anexo não abra

2.4.2.6.3 Não envie informações confidenciais, como senhas, por e-mail.

2.5 Pontos de Atenção

2.5.1 Visibilidade do cargo

2.5.2 Comportamento em Redes Sociais

2.5.3 CIS

2.5.3.1 Estabelecer e manter programa de conscientização em segurança

2.5.3.2 Treinar os colaboradores para reconhecer ataques de engenharia social

2.5.3.3 Treinar os colaboradores em melhores práticas de autenticação de usuários

2.5.3.4 Treinar os colaboradores em melhores práticas de tratamento de dados

2.5.3.5 Treinar os colaboradores para evitar exposição não intencional de dados

2.5.3.6 Treinar os colaboradores para reconhecer e notificar incidentes de segurança

2.5.3.7 Treinar os colaboradores para identificar e notificar falta de atualização de segurança nos ativos corporativos

2.5.3.8 Treinar os colaboradores sobre os perigos de se conectar a redes inseguras e transmitir dados corporativos por meio delas

3 Ações Eleição 2022

- 3.1 Bloqueio de VPN
- 3.2 Forçar Expiração de senhas
 - 3.2.1 Aviso de mudança de senhas (reforçar a política)
- 3.3 Backup de configurações dos ativos críticos
- 3.4 Criar regra no firewall para verificar se cliente VPN atende a requisitos (SIS instalado, antivírus instalado, versão do SO)
- 3.5 Realizar cópias de máquinas virtuais chave para HD externo
- 3.6 Realizar backups extras de banco de dados para fora da rede
- 3.7 Verificar e instalar em estações e servidores: Antivírus e XDR
- 3.8 Restringir o número de computadores com acesso à rede no dia da eleição (precisa da lista de computadores)
- 3.9 Realizar monitoramento detalhado de firewall, antivírus, etc
- 3.10 Apontar ativos para Graylog
- 3.11 Liberar atualizações críticas e de segurança para servidores e estações (WSUS)
- 3.12 Configuração do NTP em ativos críticos segundo normativo
- 3.13 Reunião com empresa responsável pelo storage