Laboratório - Recomendar Medidas de Mitigação de Ameaças

# Objetivos

Parte 1: Análise de um incidente em uma empresa de produção de vídeo

Parte 2: Revisão de um incidente em uma empresa de varejo

# Histórico/Cenário

O conhecimento das vulnerabilidades e dos ataques à rede é apenas parte da luta. A mitigação de ameaças é o objetivo final do pessoal de segurança da rede.

Neste laboratório, você lerá dois estudos de caso que descrevem incidentes de segurança de rede. É seu trabalho recomendar medidas de mitigação de ameaças para lidar com cada incidente.

# Recursos necessários

=    Acesso à Internet

# Instruções

## Parte 1: Revisão de um incidente em uma empresa de produção de vídeo

A All Time Video Inc. é uma empresa que produz vídeos para diversos clientes. Eles usam métodos de produção de vídeo digital e armazenam seu conteúdo em servidores de gerenciamento de conteúdo especializados. Eles estão muito orgulhosos de suas bibliotecas de conteúdo, que incluem uma ampla variedade de vídeos que podem ser usados em vídeos sobre diversos assuntos.

A gerência da empresa recebeu um e-mail de um grupo de agentes de ameaças. No e-mail, os agentes de ameaças afirmam que foram capazes de roubar vários terabytes de recursos de vídeo e projetos dos servidores de gerenciamento de conteúdo. Os agentes de ameaças ameaçam carregar os recursos de vídeo em vários servidores na Internet, a menos que a empresa pague uma quantia em dinheiro. O gerenciamento de vídeos All Time está preocupado com a possibilidade de perder vantagem competitiva se seus recursos forem tornados públicos.

A empresa contratou uma equipe de segurança externa para investigar o incidente. A investigação descobriu que um lote de unidades USB gratuitas que estavam disponíveis em uma recente feira de vídeos foi infectado com malware. O malware infectou vários hosts na rede All Time Video e também se espalhou pela rede para outras máquinas. O malware examinou a rede em busca de vários tipos de software de gerenciamento de conteúdo e determinou a versão do software. O malware então explorava vulnerabilidades em uma versão mais antiga e sem correção de erros para obter acesso. Quando o acesso foi obtido, o malware notificou os hackers que conseguiram instalar o software que usa o tunelamento de DNS para roubar dados dos servidores gradualmente. Isso foi usado para escapar da detecção. Ao longo de vários meses, os agentes de ameaças armazenam terabytes de recursos de vídeo.

### Etapa 1: Analisar o ataque.

Como membro da equipe de segurança All Video Video, você precisará contribuir com suas ideias sobre como um ataque como esse pode ser mitigado. Comece identificando as condições que levam ao ataque.

#### Pergunta:

O que tinha que acontecer para que esse ataque ocorresse?

Digite suas respostas aqui.

### Etapa 2: Recomendar técnicas de mitigação.

Para cada evento que ocorreu durante esse incidente, use seu acesso à Internet para investigar possíveis técnicas de mitigação. Você pode usar todas as fontes de informações que puder para recomendar técnicas práticas de mitigação de ameaças.

Digite suas respostas aqui.

## Parte 2: Revisão de um incidente em uma empresa de varejo

Uma empresa de varejo de médio porte especializada em componentes de violão personalizados. Um cliente é chamado para informar à empresa que seus dados pessoais e informações de cartão de crédito estão na Internet. Uma investigação mostra que os agentes de ameaças conseguiram se infiltrar na rede da empresa por meio de uma conexão de rede de um fornecedor de equipamentos. O objetivo da conexão é monitorar uma ferramenta de trabalho de madeira controlada por computador que é usada para criar colos e corpos de violão. A segurança fraca no fornecedor permitiu que os agentes de ameaças explorassem essa conexão. Os agentes de ameaças conseguiram localizar e acessar o servidor usado para aceitar pagamentos por produtos pela Internet. Os agentes de tratamento exploraram uma conta de usuário e uma senha fraca para acessar o banco de dados do cliente. Todos os detalhes do cliente estavam em um arquivo de fácil leitura. O arquivo foi carregado em um servidor usado por hackers e as informações foram vendidas para outros hackers.

### Etapa 1: Analisar o ataque

Leia a descrição do incidente e liste as etapas do ataque.

Digite suas respostas aqui.

### Etapa 2: Mitigação Recomendada

Para cada evento que ocorreu durante esse incidente, recomende medidas que possam atenuar o evento.

Digite suas respostas aqui.

# Reflexão

1.     Quais recursos específicos você encontrou na Web que o ajudaram a recomendar medidas de mitigação?

Digite suas respostas aqui.

2.     Pesquise na Web as 5 principais ameaças de segurança digital que enfrentam pequenas e médias empresas (SMB) ou empresas (SME). Liste as ameaças na tabela e sugira técnicas de mitigação que podem ajudar a combater cada uma delas. As respostas podem variar, com sites diferentes listando ameaças diferentes. Isso não é um problema. Apenas certifique-se de que as informações são recentes e investigue brevemente a origem das informações para verificar sua qualidade.

a.     Onde você encontrou suas informações? Copie e cole o URL abaixo.

Digite suas respostas aqui.

b.     Qual é o nome da empresa que forneceu as informações?

Digite suas respostas aqui.

c.     Qual é a natureza da empresa?

Digite suas respostas aqui.

d.    Preencha a tabela.

| Ameaça | Recomendações de Mitigação |
| --- | --- |
|  |  |
|  |  |
|  |  |
|  |  |
|  |  |

Linha em branco, sem informações adicionais

Linha em branco, sem informações adicionais

Fim do documento