**Atividade: Use a estrutura de segurança cibernética do NIST para responder a um incidente de segurança**

Nesta atividade, você usará o conhecimento adquirido sobre redes ao longo deste curso para analisar um incidente de rede. Você analisará a situação usando a Estrutura de Segurança Cibernética do Instituto Nacional de Padrões e Tecnologia (NIST CSF) e criará um relatório de incidente que poderá incluir como parte da documentação do seu portfólio de segurança cibernética. O CSF é uma estrutura voluntária que consiste em padrões, diretrizes e melhores práticas para gerenciar riscos de segurança cibernética. Criar um relatório de incidentes de segurança cibernética de qualidade e aplicar o CSF ​​pode ajudá-lo a construir confiança e melhorar as práticas de segurança em sua organização.

**Cenário**

Você é analista de segurança cibernética e trabalha para uma empresa de multimídia que oferece serviços de web design, design gráfico e soluções de marketing de mídia social para pequenas empresas. Sua organização sofreu recentemente um ataque DDoS, que comprometeu a rede interna por duas horas até ser resolvido.

Durante o ataque, os serviços de rede da sua organização pararam repentinamente de responder devido a uma inundação de pacotes ICMP. O tráfego normal da rede interna não conseguiu acessar nenhum recurso da rede. A equipe de gerenciamento de incidentes respondeu bloqueando os pacotes ICMP recebidos, interrompendo off-line todos os serviços de rede não críticos e restaurando os serviços de rede críticos.

A equipe de segurança cibernética da empresa investigou então o evento de segurança. Eles descobriram que um agente mal-intencionado enviou uma enxurrada de pings ICMP para a rede da empresa por meio de um firewall não configurado. Essa vulnerabilidade permitiu que o invasor mal-intencionado sobrecarregasse a rede da empresa por meio de um ataque distribuído de negação de serviço (DDoS).

Para resolver esse evento de segurança, a equipe de segurança de rede implementou:

* Uma nova regra de firewall para limitar a taxa de pacotes ICMP recebidos
* Verificação do endereço IP de origem no firewall para verificar endereços IP falsificados em pacotes ICMP recebidos
* Software de monitoramento de rede para detectar padrões de tráfego anormais
* Um sistema IDS/IPS para filtrar algum tráfego ICMP com base em características suspeitas

Como analista de segurança cibernética, você tem a tarefa de usar este evento de segurança para criar um plano para melhorar a segurança da rede da sua empresa, seguindo a Estrutura de Segurança Cibernética (CSF) do Instituto Nacional de Padrões e Tecnologia (NIST). Você usará o CSF ​​para ajudá-lo a navegar pelas diferentes etapas de análise deste incidente de segurança cibernética e integrar sua análise em uma estratégia geral de segurança:

* Identifique riscos de segurança por meio de auditorias regulares de redes internas, sistemas, dispositivos e privilégios de acesso para identificar possíveis lacunas na segurança.
* Proteja os ativos internos através da implementação de políticas, procedimentos, treinamentos e ferramentas que ajudem a mitigar ameaças à segurança cibernética.
* Detecte possíveis incidentes de segurança e melhore os recursos de monitoramento para aumentar a velocidade e a eficiência das detecções.
* Responder para conter, neutralizar e analisar incidentes de segurança; implementar melhorias no processo de segurança.
* Recuperar sistemas afetados para operação normal e restaurar dados e/ou ativos de sistemas que foram afetados por um incidente.

**Passo 1: Acesse o modelo**

Arquivo “*Análise de relatório de incidente*”

Arquivo “*Aplicando o NIST CSF*”

Arquivo “*Exemplo completo de Análise de relatório de incidente*”

**Passo 2: Identifique o tipo de ataque e sistemas afetados**

Pense em todos os conceitos abordados no curso até agora e reflita sobre o cenário para determinar que tipo de ataque ocorreu e quais sistemas foram afetados. Liste essas informações na planilha de análise do relatório de incidentes na seção intitulada “Identificar”.

**Passo 3: Proteja os ativos de sua corporação de serem comprometidos**

A seguir, você avaliará onde a organização pode melhorar para proteger ainda mais seus ativos. Nesta etapa, você se concentrará na criação de um plano de ação imediato para responder ao incidente de segurança cibernética. Ao criar este plano, reflita sobre a seguinte questão:

* Quais sistemas ou procedimentos precisam ser atualizados ou alterados para proteger ainda mais os ativos da organização?

Escreva sua resposta no modelo de análise de relatório de incidentes na seção “Proteger”.

**Passo 4: Determine como identificar incidentes parecidos no futuro**

É importante monitorar continuamente o tráfego de rede em dispositivos de rede para verificar atividades suspeitas, como pacotes ICMP externos recebidos de endereços IP não confiáveis ​​que tentam passar pelo firewall de rede da organização.

Para esta etapa, considere maneiras pelas quais você e sua equipe podem monitorar e analisar o tráfego de rede, aplicativos de software, rastrear usuários autorizados e não autorizados e detectar qualquer atividade incomum nas contas dos usuários. Escreva sua resposta na planilha de análise de resposta a incidentes na seção “Detectar”.

**Etapa 5: Crie um plano de resposta para futuros incidentes de cibersegurança**

Depois de identificar as ferramentas e métodos que você e sua organização utilizam para detectar possíveis vulnerabilidades e ameaças, crie um plano de resposta no caso de um incidente futuro. Isso normalmente acontece depois que o incidente ocorreu e foi resolvido por você e sua equipe. Neste caso, você criará um plano de resposta para futuros incidentes de segurança cibernética. Alguns itens a considerar ao criar um plano de resposta a qualquer incidente de segurança cibernética:

* Como você e sua equipe podem conter incidentes de segurança cibernética e dispositivos afetados?
* Quais procedimentos existem para ajudar você e sua equipe a neutralizar incidentes de segurança cibernética?
* Que dados ou informações podem ser usados ​​para analisar este incidente?
* Como o processo de recuperação da sua organização pode ser melhorado para lidar melhor com futuros incidentes de segurança cibernética?

Escreva sua resposta no modelo de análise de relatório de incidente na seção “responder”.

**Etapa 6: Ajude sua organização a se recuperar do incidente**

Considere quais medidas precisam ser tomadas para ajudar a organização a se recuperar do incidente de segurança cibernética. Reflita sobre todas as informações coletadas sobre o incidente nas etapas anteriores para considerar quais dispositivos, sistemas e processos precisam ser restaurados e recuperados.

Considere as seguintes questões:

* Quais informações você precisa para recuperar imediatamente?
* Quais processos estão em vigor para ajudar a organização a se recuperar do incidente?

Escreva sua resposta na parte “recuperação” da planilha.

**O que incluir em sua resposta**

Posteriormente, você terá a oportunidade de avaliar seu desempenho utilizando os critérios listados. Certifique-se de abordar o seguinte em sua atividade concluída.

Análise de relatório de incidente do Curso 3

* Identifica o tipo de ataque e os sistemas impactados pelo incidente
* Oferece um plano de proteção contra futuros incidentes de segurança cibernética
* Descreve métodos de detecção que podem ser usados ​​para identificar possíveis incidentes de segurança cibernética
* Inclui um plano de resposta para o incidente de segurança cibernética e um esboço para futuros incidentes de segurança cibernética
* Descreve planos de recuperação que você e a organização podem implementar em futuros incidentes de segurança cibernética.

**Exemplo Concluído**

Arquivo “*Incident report analysis exemplar*”

**Avaliação do Exemplo**

Compare o exemplar com a análise completa do relatório de incidentes e o relatório de incidentes. Revise seu trabalho usando cada um dos critérios do exemplar. O que você fez bem? Onde você pode melhorar? Use suas respostas a essas perguntas para orientá-lo à medida que avança no programa.

**Nota**: O exemplar representa um exemplo de como realizar a atividade. O seu pode diferir em alguns aspectos. O importante é que você tenha uma ideia de como deve ser sua análise de incidente.

O exemplar é acompanhado da atividade e apresenta uma análise completa do relatório de incidente para estabelecer:

* Que tipo de ataque ocorreu, o escopo do incidente e seu impacto para a organização
* Potenciais vulnerabilidades de rede e medidas de proteção
* Ferramentas de detecção para monitorar e proteger a rede
* Como responder a incidentes de segurança cibernética no futuro
* Planos de recuperação para restaurar as operações normais