Política Anti-Malware

Conteúdo

1 Introdução

A ameaça representada pelo malware nunca foi tão séria como atualmente. Os sistemas e usuários estão sob constante bombardeio de tentativas de contornar a segurança, a fim de obter algum tipo de ganho ou interromper o funcionamento normal da organização.

Essa ameaça pode vir de várias fontes, incluindo:

- Gangues organizadas que tentam roubar dinheiro ou cometer chantagem
- Organizações concorrentes tentando obter informações confidenciais
- Grupos politicamente motivados
- Funcionários desonestos dentro da organização
- Unidades de "guerra cibernética" patrocinadas por outros locais
- Indivíduos com curiosidade ou testando suas habilidades

Seja qual for a fonte, o resultado de uma violação de segurança bem-sucedida é que a organização e seus interessados são afetados, podendo causar dano.

Uma das principais ferramentas usadas por esses invasores é o malware, e é essencial que sejam tomadas precauções efetivas pela Cobmais para se proteger contra essa ameaça.

Este documento define a política da organização em relação à defesa contra malware. Seu público-alvo é o pessoal de gerenciamento e suporte de TI e segurança da informação que implementará e manterá as defesas da organização. As informações e conselhos relacionados a malware para usuários estão incluídos nos documentos de políticas referenciados abaixo.

Esse controle se aplica a todos as operações, pessoas e processos que constituem os sistemas de informações da organização, incluindo membros do conselho, diretores, funcionários, fornecedores e outros terceiros que têm acesso aos sistemas da Cobmais.

As políticas e procedimentos a seguir são relevantes para este documento:

- *Política de Dispositivos Móveis*
- *Política de Aceitação pelo Usuário*
- *Política de Mensagens Eletrônicas*
- *Procedimento de Resposta a Incidentes de Segurança da Informação*

2 A Ameaça Malware

2.1 Definição

Não existe uma definição única do termo "Malware", mas para os propósitos desta política é usada a seguinte definição:

"Malware é qualquer código ou software que possa ser prejudicial ou destrutivo para as capacidades de processamento de informações da organização"

O termo é derivado da expressão "Software Malicioso" e também pode ser chamado de código malicioso ou comumente (mas imprecisamente) "um vírus".

2.2 Tipos de Malware

2.2.1

O malware pode ser de várias formas e está em constante mudança, já que os ataques anteriores vão se extinguindo e novos são encontradas. Os tipos mais comuns de malware encontrados hoje são:

- ***Vírus*** – um programa que executa uma função indesejada no computador infectado. Isso pode envolver ações destrutivas ou a coleta de informações que podem ser usadas pelo invasor
- ***Trojan*** – um programa que finge ser um código legítimo, mas que esconde outras funções indesejadas. Muitas vezes disfarçado como um jogo ou programa utilitário
- ***Worm*** – um programa capaz de se copiar em outros computadores ou dispositivos sem interação do usuário
- ***Logic bomb*** – código malicioso que foi configurado para ser executado em uma data e hora específica ou quando certas condições são atendidas
- ***Rootkit*** – um programa usado para disfarçar atividades maliciosas em um computador, ocultando os processos e arquivos do usuário
- ***Keylogger*** – código que registra as teclas digitadas pelo usuário
- ***Backdoor*** – um programa que permite acesso não autorizado ao invasor

Geralmente, esses tipos de malware serão usados em combinação uns com os outros.

2.3 Como o Malware se propaga

Para que um software mal-intencionado execute sua finalidade, ele precisa ser instalado no dispositivo ou no computador de destino. Há várias

maneiras principais de o malware infectar computadores e redes, embora novas formas estejam sendo criadas o tempo todo.

As técnicas de infecção mais comuns são as seguintes.

2.3.1 Phishing

Esse método envolve enganar o usuário para realizar alguma ação que faça com que um programa malicioso seja executado e infecte o computador que está sendo usado. Geralmente é através do envio geral de e-mails não solicitados (Spam) com anexos de arquivos ou links da web. Quando o usuário abre o arquivo ou clica no link, a ação mal-intencionada é acionada.

Os ataques de Phishing se tornaram mais sofisticados nos últimos anos e podem ser muito convincentes e atraentes para o usuário. Versões mais segmentadas de Phishing apareceram, como o Spear Phishing (destinado a uma determinada organização) e até a Whaling (destinada a um indivíduo).

2.3.2 Websites e Código Móvel

O uso disseminado de códigos móveis, como o JavaScript, forneceu outra rota para infectar computadores com malware. Muitas vezes sites são criados para hospedar o malware que é ativado ou clicando em um link ou, em alguns casos, simplesmente visitando o site.

Cada vez mais, sites legítimos são comprometidos e feitos para hospedar malware sem o conhecimento do proprietário, o que facilita muito esse tipo de ataque para o usuário.

2.3.3 Mídia Removível

Cartões de memória USB, CDs, DVDs e outros dispositivos de mídia removível fornecem uma maneira eficaz de espalhar malwares em computadores. Quando a mídia é inserida na máquina, o malware é executado e infecta o alvo ou fica na mídia removível para se preparar para infectar a próxima máquina em que for conectado.

2.3.4 Hacking

Ou "Cracking", é um método mais direcionado e, portanto, menos comum de introduzir malware em um computador ou rede, obtendo acesso não autorizado à rede de fora (e às vezes dentro) da organização. Este método requer mais conhecimento por parte do agressor e, muitas vezes, explora as vulnerabilidades existentes no software ou nos dispositivos de rede

utilizados. Depois que o acesso for obtido, o malware será instalado remotamente na máquina comprometida.

3 Política Anti-Malware

Para evitar a infecção de computadores e redes da Cobmais e evitar as consequências potencialmente terríveis de tal infecção, há uma série de controles importantes que serão adotados como política.

O conceito chave adotado nesta política é "defesa em profundidade" e nenhum controle individual deve ser usado para fornecer proteção adequada. Portanto, esta não é uma escolha entre os controles, mas uma lista de controles necessários, os quais devem ser implementados sempre que possível para proteger contra as ameaças anteriormente descritas.

3.1 Firewall

Um firewall será instalado em todos os pontos em que a rede interna estiver conectada à Internet.

Sempre que possível, os firewalls individuais serão ativados nos computadores. As permissões de acesso devem ser definidas de forma que o usuário não possa desabilitar o firewall.

3.2 Antivírus

Uma plataforma antivírus comercial com suporte será instalada na organização em locais chave:

- Firewall
- Servidores de e-mail
- Servidores proxy
- Todos os outros servidores
- Todos os computadores do usuário
- Dispositivos móveis, incluindo laptops (telefones e tablets, sempre que possível)

Todos antivírus serão configurados para obter atualizações de assinatura regularmente, diretamente do site do fornecedor ou de um servidor central da organização.

Por padrão, a varredura de acesso deve estar ativada para fornecer proteção em tempo real. Varreduras completas regulares também devem ser realizadas pelo menos uma vez por semana.

Os usuários não devem poder desativar a proteção configurada centralmente.

3.3 Filtragem de Spam

Um sistema será instalado para filtrar e-mails não solicitados e potencialmente prejudiciais (spam). Os tipos de anexos que costumam conter malware devem ser bloqueados ou removidos antes da entrega ao usuário.

3.4 Instalação do Software e Digitalização

Os usuários não devem ter acesso administrativo ao computador para permitir que instalem software nele. Somente software aprovado será permitido e isso deve ser instalado pelo departamento de TI mediante solicitação autorizada.

A varredura regular de computadores de usuários para detectar software não autorizado deve ser realizada.

3.5 Gestão de Vulnerabilidade

Informações sobre vulnerabilidades de software serão coletadas de fornecedores e fontes de terceiros e atualizações aplicadas quando disponíveis.

A varredura de vulnerabilidades deve ser realizada regularmente, particularmente em redes e servidores críticos para os negócios.

Para novas vulnerabilidades identificadas pelos funcionários da Cobmais, será aplicada uma política de divulgação coordenada.

3.6 Treinamento de conscientização do usuário

Os usuários devem estar cientes quando começarem a trabalhar na organização da política de segurança da informação e receberem treinamento para evitar serem vítimas de ataques.

Esse treinamento de conscientização deve ser repetido regularmente para todos os funcionários que fazem uso de equipamentos de TI.

3.7 Monitoramento de ameaças e alertas

Informações sobre ameaças emergentes serão obtidas de fontes adequadas e usuários alertados sobre possíveis ataques, fornecendo o máximo de detalhes para maximizar a chance de reconhecimento.

3.8 Revisões Técnicas

Avaliações regulares serão realizadas em redes e servidores essenciais aos negócios para identificar qualquer malware que tenha sido instalado desde a última revisão.

3.9 Gestão de Incidentes de Malware

No caso de um malware ser detectado em um servidor, cliente, rede ou outro componente de TI, um incidente de segurança das informações será gerado. Isso será gerenciado de acordo com os procedimentos estabelecidos no *Procedimento de Resposta a Incidentes de Segurança da Informação*.