IT-ONE

POLÍTICA DE SEGURANÇA DA INFORMAÇÃO

PC09 - Política de Combate a Softwares Maliciosos

1. HISTÓRICO DE VERSÕES

DATA	VERSÃO	DESCRIÇÃO	AUTOR
02/06/21	1.0	Criação do documento	Peterson Pires

INTRODUÇÃO

Um dos principais problemas relacionados à segurança da informação é a infecção por softwares maliciosos, que são programas escritos com objetivo de comprometer um dos pilares da segurança, confiabilidade, disponibilidade e integridade ou utilizar o ambiente tecnológico infectado, como base para atacar outros ambientes em massa. Desta forma, para garantir a continuidade das atividades e blindar o ambiente tecnológico, a IT-One investe em recursos necessários que viabilizem a proteção necessária para manter as atividades dos seus colaboradores sempre monitorada e dando uma resposta rápida aos incidentes.

Com a finalidade de assegurar a proteção necessária, tem-se a presente Política Complementar de Combate a Softwares Maliciosos, com as diretrizes acerca do tema.

OBJETIVO

Assegurar que medidas preventivas de proteção, detecção e correção sejam estabelecidas corporativamente, para resguardar o ambiente tecnológico da IT-One contra softwares maliciosos (vírus, worms, spyware, spam).

ABRANGÊNCIA

Esta política se aplica a todos os colaboradores da IT-One, quais sejam: funcionários servidores ou comissionados, estagiários, menor aprendiz, terceirizados ou indivíduos que direta ou indiretamente utilizam ou suportam os sistemas, infraestrutura ou informações da IT-One. Todos esses colaboradores serão tratados nesta política como usuários

DIRETRIZES DE COMBATE A SOFTWARES MALICIOSOS

1. Diretrizes Gerais e Infraestrutura

    a) Todos os equipamentos que têm a funcionalidade de servidores (dispositivos que disponibilizam informações a outros ligados em rede), tanto físicos quanto virtuais, equipamentos de mesa (PCs), dispositivos móveis e de segurança da informação, devem estar protegidos com sistemas de proteção contra softwares maliciosos e serem atualizados periodicamente, conforme recomendação de disponibilização do fabricante;

    b) Devem ser estabelecidos procedimentos que visem os controles de detecção, prevenção e combate a softwares maliciosos;

    c) Caso o usuário perceba que no seu equipamento de trabalho os sistemas de proteção, como antivírus e firewall, não estejam instalados ou funcionando adequadamente, este deve entrar em contato com a Central de Serviços para as devidas providências;

    d) Apenas a área técnica da IT-One deve realizar instalação de softwares ou aplicativos no ambiente tecnológico da IT-One, com a finalidade de manter o controle, evitando a introdução de vulnerabilidades e possível vazamento de informações, perda de integridade ou outros incidentes de Segurança da Informação, além da violação de direitos de propriedade intelectual;

    e) Os sistemas de proteção contra softwares maliciosos devem ser instalados com controles que não permitam alteração de sua configuração ou remoção da ferramenta, por usuários não autorizados;

    f) Os equipamentos não homologados pela área técnica da IT-One na rede local não devem ser utilizados, conforme Política de Ativos de Dispositivos Móveis, evitando a entrada de possíveis infecções por equipamentos nocivos ao ambiente tecnológico da IT-One;

2. Diretrizes de Tratamento de Arquivos, Softwares e Aplicativos

    a) Todos os arquivos recebidos por meio de redes, em qualquer mídia de armazenamento, correio eletrônico, arquivos baixados (download) ou em páginas web, devem ser verificados automaticamente quanto à presença de códigos maliciosos, antes de serem utilizados;

    b) Para minimizar o risco de infecção por softwares maliciosos, os usuários devem usar, exclusivamente, softwares homologados, licenciados e instalados pela área técnica da IT-One;

3. Análise de Vulnerabilidade

    a) Periodicamente devem ser realizadas análises de vulnerabilidades de softwares, aplicativos e infraestrutura que suportam os processos críticos do ambiente tecnológico da IT-One;

    b) A resposta às vulnerabilidades críticas detectadas nos sistemas e ambientes da IT-One deve ser tratada imediatamente pela equipe de Resposta a Incidentes, conforme descrito na Política de Resposta a Incidentes de segurança da informação;

    c) Deve ser mantido e atualizado o procedimento de análise, testes e implementação de contramedidas que visem reduzir vulnerabilidades, que possam ser exploradas por códigos maliciosos;

    d) Caso não seja possível realizar os testes adequados para implementar a correção, deve ser realizada uma análise de risco associado a correção, considerando experiências de outros ambientes tecnológicos e aguardar um período mais longo para a implementação;

    e) Deve ser definido o procedimento de obtenção de informações relativas aos códigos maliciosos e vulnerabilidades, que deve incluir entre outras, as ações, riscos associados à implementação, às responsabilidades e ao prazo para a reação as notificações de potenciais vulnerabilidades técnicas relevantes;

4. Indisponibilidade do Ambiente

    a) Deve ser realizada uma análise de impacto e elaborado um Plano de Recuperação de Desastre (PRD), como forma de manter as atividades críticas da IT-One que considere casos de indisponibilidade do ambiente tecnológico por ataque de códigos maliciosos;

    b) Durante as manutenções e procedimentos de emergência, deve se ter um cuidado específico para evitar a introdução de códigos maliciosos no ambiente tecnológico, os quais podem ultrapassar os controles comuns de proteção.

5. Atualização e Monitoramento

    a) A área técnica da IT-One é responsável por gerir e manter os ativos de softwares vigentes com as correções mais recentes, além de suportar os mecanismos de controle e combate a softwares maliciosos, mantendo estes e aqueles com licenças, vacinas e devidas correções atualizadas;

b) Regularmente, a área técnica da IT-One deve apresentar ao Comitê de TI, relatórios com tentativas e ataques e ações tomadas, os maiores ofensores, equipamentos desatualizados ou vulneráveis, equipamentos gerenciáveis e não gerenciáveis, controle das licenças utilizadas e disponíveis e prazo de licenças a vencer, entre outros;

c) Os relatórios específicos de resposta a incidentes relacionados a softwares maliciosos devem apresentar correlação de informações e detalhes (por exemplo: endereço de origem e destino, ação detectada, usuários afetados, data e hora do incidente, entre outros), que viabilize ações corretivas e preventivas;

d) A área técnica da IT-One deve fazer o monitoramento e análise constante do tráfego da rede local, de forma que se identifiquem, entre outras, ameaças relativas a tráfego malicioso ou atividades incompatíveis com as políticas de uso e segurança da rede, viabilizando a tomada de providências.

6. Ações disciplinares

a) A intenção de introduzir ou espalhar softwares maliciosos no ambiente tecnológico da IT-One poderá acarretar sanções administrativas disciplinares e/ou contratuais aos seus respectivos usuários, sem prejuízo das responsabilidades nas esferas civil e criminal