**Proposta de Padrão Técnico para solução Anti Malware**

1. **Resumo**

Esse Padrão Técnico (PTEC) estabelece os requisitos mínimos que uma solução *antimalware* deve fornecer, para uso no âmbito dos órgãos da administração pública estadual.

1. **Introdução**

O termo *Malware* é na verdade uma contração da expressão *Malicious Software* ou Programa Malicioso. Um *Malware* é qualquer *software* ou parte de *software* que tenha sido escrito para causar danos, alterar ou roubar informações indevidamente. São compreendidos, mas não se limitam a vírus, “cavalos de Tróia”, *Worms, Spywares, Keyloggers*, entre outros. As estatísticas dos principais fornecedores *antimalware*, mostram que tanto a quantidade de amostras quanto o número de infecções têm aumentado a cada ano e, logo, é de extrema relevância que os órgãos da administração pública estadual estejam munidos de ferramentas eficientes para controlar esse tipo de ameaça.

1. **Escopo**

Esse PTEC é aplicável a todos órgãos da administração pública estadual que necessitam adquirir solução de segurança para seus sistemas e dispositivos sob abrangência da Política TICRS, incluindo, estações de trabalho (*desktops*), servidores e laptops, que utilizam as plataformas Microsoft Windows, Linux e Mac.

1. **Definições**

*- Ameaça: causa potencial de um incidente indesejado, que pode resultar em danos a um sistema ou organização;*

*- Antivírus: programa que tem o propósito de bloquear um vírus antes que ocorra uma infecção ou eliminar um vírus após ingressar no sistema;*

*- Antimalware: programa que tem o propósito de bloquear programas maliciosos antes de ocorrer uma infecção ou eliminá-los após ingressarem no sistema;*

*- Bot: um “bot” é um tipo de malware que permite ao criminoso, obter controle completo do sistema utilizando-o de forma remota, também conhecido como computador “zumbi”;*

*- Botnet: uma rede com vários “Bots” que executam autonomamente.*

*- Buffer Overflow: ou “estouro de pilha”, é uma anomalia onde um programa, ao escrever dados em um uma memória, ultrapassa os seus limites escrevendo indevidamente na memória adjacente;*

*- Controle: qualquer processo, política, dispositivo, prática ou outras ações que modificam o risco;*

*- Cookie: arquivo de texto que um servidor web pode armazenar no disco rígido do usuário visitante de forma a identifica-lo em futuras visitas ao site;*

*- Impacto: abrangência dos danos causados por um incidente de segurança sobre um ou mais processos de negócio;*

*- Keylogger: é um programa malicioso cujo objetivo é gravar todas as teclas digitadas no teclado de um computador geralmente com funcionalidades extras como prints de tela e envio de relatórios remotos;*

*- Phishing: técnica que emprega e-mails fraudulentos utilizados para roubo de credenciais bancárias, dados pessoais e outras informações;*

*- Risco: efeito da incerteza sobre os objetivos;*

*- Rootkit: um tipo de malware criado para esconder ou camuflar a existência de determinados processos ou programas dos métodos normais de detecção;*

*- Spyware: programa “espião” de computador que tem como objetivo observar e roubar informações do computador no qual está instalado para uma fonte externa na Internet, sem o conhecimento ou consentimento do usuário;*

*- Trojan: ou “Cavalo de Tróia”, como o nome sugere, é um malware que executa ações maliciosas num computador como se fosse um programa legítimo, geralmente abrindo portas para invasão;*

*- Worm: programa semelhante ao vírus, porém com características de auto replicação, criando cópias de si mesmo e infectando outros sistemas através de redes locais, anexos de e-mail entre outros;*

*- Vírus: um tipo de malware que consegue se replicar infectando outros arquivos no sistema;*

*- Vulnerabilidade: fraqueza de um ativo ou controle que pode ser explorada por uma ou mais ameaças;*

1. **Objetivos**

O objetivo desse PTEC é estabelecer os requisitos mínimos aceitáveis que uma solução *antimalware* corporativa deve conter, para atuar nos computadores desktops, servidores e laptops conectados aos sistemas ou redes computacionais dos órgãos da administração pública estadual, buscando dessa forma, detectar, prevenir e coibir a ação de códigos maliciosos nesse ambiente. É sabido que ativos de informação possuem vulnerabilidades em maior ou menor grau, estando sujeitos as ameaças dos meios internos e externos; o presente PTEC estabelece as configurações mínimas que esse tipo de controle deve possuir para minimizar os riscos associados a esse tipo de ameaça.

1. **Diretrizes Técnicas**

A ferramenta *antimalware* a ser utilizada nos recursos computacionais dos órgãos da administração pública estadual deve contemplar as seguintes especificações técnicas:

1. Toda a solução de segurança proposta deve ter sido desenvolvida por um único fabricante de modo que tanto o suporte da solução, quanto suas funcionalidades sejam integradas e administradas através de uma console de gerenciamento integrado;
2. A solução deve servir para estações de trabalho, dispositivos móveis (laptops) e servidores, englobando no mínimo as soluções de antivírus, *antispyware*, *firewall*, prevenção de ameaças e controle web; a solução deve ainda ser colaborativa, ou seja, os módulos devem ser capazes de enviarem informações à console de gerência para uma análise mais inteligente;
3. A solução deve possuir suporte aos sistemas operacionais baseados na plataforma Windows, Mac e Linux (incluindo ambientes virtualizados), especificados no anexo A deste documento; deve ter suporte para plataformas de 32-bits e de 64-bits considerando que os requisitos mínimos de hardware são: processador de 1GHz, 1GB RAM e 40GB HDD; todas as funcionalidades devem ser ativadas por agente único de forma a facilitar a instalação, a configuração e o gerenciamento; ainda, deve possuir integração com o Microsoft *Active Directory*, permitindo a criação de políticas por usuário;
4. Deve permitir a proteção durante a inicialização do sistema operacional e realizar a análise dos setores de boot dos equipamentos;
5. Todas as funcionalidades da solução devem ser geridas por uma console de gerenciamento integrado com as capacidades mínimas de: criação de relatório, exibição de *dashboards*, gestão de políticas, configurações da ferramenta e dos dispositivos clientes, instalação e desinstalação;
6. Deve fornecer atualizações automáticas das listas de definições de vírus a partir de local predefinido da rede ou de repositório na Internet (dando suporte a múltiplos repositórios); deve permitir atualizações incrementais das definições de vírus, ter frequência de atualização diária e com possibilidade de agendamento; ainda, deve permitir conexões através de servidores *proxy* para efetuar as atualizações;
7. Deve fornecer regras de proteção nativas no mínimo contra ataques (definidas pelo fabricante da solução) do tipo: acesso remoto a pastas locais; alteração de políticas de direitos dos usuários; alteração dos registros de extensão dos arquivos; criação de novos arquivos na pasta “Arquivos de Programas” do Windows; criação de novos executáveis na pasta Windows; criação e modificação remotas de arquivos portáteis de execução, INI, PIF e as localizações do sistema; criação e modificação remota de arquivos ou pastas; desativação do editor de registro e gerenciador de tarefas; execução de arquivos das pastas de usuários; execução de *scripts* pelo *host* de *script* do Windows; instalação de objetos de ajuda a navegação ou extensões de *shell*; instalação de novos CLSIDs, APPIDs e TYPELIBs; modificação das configurações de rede; modificação dos principais processos do Windows; registro de programas para execução automática;
8. Quanto a varredura, a aplicação deve permitir a escolha da prioridade da CPU no processo de varredura, levando em consideração os níveis “alto”, “médio” e “baixo”; deve fornecer a varredura em tempo real de arquivos (leitura e gravação) e de processos em memória; deve permitir varredura manual configurável com interface do sistema operacional e opções de limpeza; todos os tipos de varredura devem possuir opções de escopo (drives locais, drives ou pastas específicas), ações (alertar, limpar/apagar automaticamente e quarentena), frequência (horária, diária, semanal ou mensal) e filtros (pastas, arquivos, tipos de arquivos e processos que devem ou não serem varridos); possibilitar a recuperação de arquivos da quarentena; realizar a análise durante a cópia de arquivos entre pastas locais;;
9. Ainda quanto a varredura, a solução deve permitir a análise em unidades de rede, arquivos abertos para backup, arquivos compactados (exemplo .jar) e arquivos codificados (exemplo MIME); deve detectar programas indesejados, ameaças em programas desconhecidos e ameaças em macro desconhecidas; deve possuir módulo capaz de interceptar e analisar *scripts* (*Javascript* e *VBSscript*) destinados ao Windows *Host Scripting*; ao detectar uma ameaça, a solução deverá ter a possibilidade de emissão de notificação ao usuário;
10. Deve gerar registros (*logs*) de varreduras localmente com posterior envio do conteúdo para uma interface de gerenciamento; deve prever que, sempre que uma estação não puder se comunicar com o servidor para o envio dos *logs*, estes devem ser armazenados localmente para posterior envio, quando o servidor estiver disponível;
11. A solução deve contemplar detecção e remoção de programas maliciosos como *bots, keyloggers, rootkits, spywares*, *trojans*, *worms*, vírus e *malwares* em geral, gerando notificações de eventos através de alertas na rede; deve conter módulo capaz de proteger contra *botnets,* negações de serviço, executáveis não confiáveis e conexões *web* maliciosas; deve contemplar solução para detectar *cookies* indesejáveis no sistema; deve ter prevenção contra o escalonamento de privilégios genéricos e prevenção de execução de dados no Windows, ambos com possibilidade de ativação/desativação por políticas;
12. A solução deve permitir bloqueio de aplicações, processos (pelo nome, caminho do arquivo ou *hash* MD5) ou módulo chamador (pelo nome, caminho, *hash* ou signatário digital); deve ter a possibilidade de reparar o registro do sistema após a eliminação dos programas maliciosos;
13. Deve permitir o bloqueio de portas virtuais (TCP e UDP); permitir a criação de regras baseadas em processos do sistema, o bloqueio de compartilhamentos da máquina em casos de epidemia, ter a capacidade de monitorar o comportamento do computador e bloquear possíveis invasões;
14. Oferecer proteção avançada do sistema contra ameaças como ataques remotos, injeções de SQL ou HTTP; bloquear ataques baseados em *web* como *Directory Traversal Attacks* e *Unicode Attacks*; detectar e bloquear tentativas de invasão; possuir proteção pronta contra ameaças desconhecidas como ataques do dia zero (*zero-day attacks*) ou estouro de pilha (*buffer overflow*);
15. Quanto à instalação, atualização e gerenciamento, deve possuir método de instalação “silenciosa” através da console de gerenciamento; deve permitir a instalação automática em novas estações da rede via console de gerenciamento; permitir atualizações automáticas do produto; forçar a reinstalação no cliente em caso de desinstalação (o agente deve “perceber” a desinstalação realizada por usuário desautorizado); possuir método de desinstalação sem a necessidade de reinicialização do sistema operacional (especialmente para servidores); todas as funcionalidades descritas anteriormente devem estar contempladas para instalações em máquinas físicas ou virtuais;
16. O módulo de gerenciamento da solução deve promover a gerência centralizada de todos os módulos do produto; deve permitir o gerenciamento centralizado da instalação nos clientes a partir de uma única central de gerenciamento, possibilitando que a solução seja instalada num grupo de máquinas, intervalo de endereços, numa máquinas exclusiva, etc; deve suportar o gerenciamento de múltiplos dispositivos a partir de um único servidor ou de um conjunto de servidores (dependendo do número de clientes que precisam ser atendidos, as especificações de hardware podem ser escalonadas); permitir o gerenciamento do servidor através de interface *web* utilizando os principais navegadores comerciais (Google Chrome, Mozilla Firefox e Safari), protocolos TCP/IP e HTTPS; deve permitir a alteração nas configurações dos antivírus das estações clientes de maneira remota e permitir a atualização incremental através do uso de políticas da lista de definições de vírus nos clientes a partir de um único ponto da rede;
17. O módulo de gerenciamento deve permitir ainda visualizar a configuração básica de todas as estações gerenciadas; permitir a criação de tarefas de atualização, verificação de vírus e *upgrade* de produtos em períodos de tempo pré-determinados,; permitir o armazenamento das informações coletadas dos clientes num banco de dados centralizado; deve possuir diferentes níveis de administração de console, distinguindo diferentes perfis (controle total e revisão), com possibilidade de delegação de administração entre perfis; possibilitar a imposição da configuração determinada para os clientes (qualquer alteração de configuração feita pelo cliente deverá retornar ao padrão pré-estabelecido no servidor);
18. A solução deve gerar relatórios gráficos com possibilidade de customização e permitir a exportação para os formatos html, csv, xls, xlsx, doc, docx, rtf e pdf; também deve ter a possibilidade de geração de trilhas de auditoria (geração de logs para a auditoria);
19. Deve gerar relatórios que contenham no mínimo o nome da máquina cliente, *malware* e arquivo infectado (com o caminho completo), possibilitando a ordenação por um desses campos; deve ainda, gerar relatórios customizáveis, que contenham coletivamente ou individualmente as seguintes informações: clientes com a lista de definições de vírus desatualizada; clientes sem o produto instalado; versão do produto instalado em cada cliente; os *malwares* detectados; os clientes que sofreram infecções num determinado período de tempo e resultados das varreduras;
20. A solução deve prever proteção integrada para o navegador, permitindo o filtro de sites, tanto para bloqueio quanto para desbloqueio, baseado em políticas; possuir módulo de monitoramento da navegação com sistema de classificação de códigos por cores; ter formato de *plugin* compatível com os principais navegadores; possuir integração automática com os sites de busca Google, Bing, Ask e Yahoo, possibilitando a classificação no próprio resultado da pesquisa;
21. **Data da Criação e Entrada em Vigor**

Esse PTEC foi criado em agosto de 2018 e entra em vigor na data de sua publicação.

1. **Papéis e Responsabilidades**

|  |  |
| --- | --- |
| Papéis | Responsabilidades |
| CGTIC – Comitê de Governança de Tecnologia da Informação e Comunicação | Gerir crítica e eficazmente a aplicação desse PTEC. |
| CETIC – Comitê Executivo de Tecnologia da Informação e Comunicação | Supervisionar a conformidade dos órgãos da administração pública estadual a este PTEC. |
| GT – Grupo Temático Segurança da Informação | Criar, revisar e manter a atualização desse PTEC. |
| GGTIC – Grupo de Gestores de Tecnologia da Informação e Comunicação | Promover a conformidade dos órgãos da Administração Pública estadual a este PTEC. |

1. **Resultados Esperados**

Com a aplicação do presente Padrão Técnico espera-se atingir os seguintes resultados:

- Diminuir a quantidade de incidentes relacionados a *malware* nos sistemas dos órgãos da administração pública estadual;

- Aumentar a disponibilidade dos servidores, *desktops* e demais dispositivos computacionais dos órgãos da administração pública estadual;

- Facilitar o gerenciamento de dispositivos, centralizando-os numa console administrativa;

- Prevenir custos com *malwares* que sequestram dados (*ransomwares*);

- Garantir níveis de segurança aceitáveis durante a navegação dos servidores públicos alertando-os sobre possíveis links de phishing;

- Diminuir riscos associados a fraudes bancárias;

1. **Referência a Outros Documentos e Anexos**
2. Norma ABNT NBR ISO/IEC 27001:2013 Requisitos para um Sistema de Gestão da Segurança da Informação;
3. Norma ABNT NBR ISO/IEC 27002:2013 Código de Prática para Controles de Segurança da Informação;
4. Norma ABNT NBR ISO/IEC 27003:2011 Diretrizes para Implantação de um Sistema de Gestão da Segurança da Informação;