POLÍTICA

MONITORAMENTO DA SEGURANÇA DA INFORMAÇÃO

REVISÃO		PÁGINAS ALTERADAS	ÁREA RESPONSÁVEL	DESCRIÇÃO DA ALTERAÇÃO
Nº	DATA			
01	08/02/18	-	TI	Publicação
02	29/05/19	-	TI	Revisão
03	30/09/21	-	TI	Revisão e alterações de propriedade

Esta Política será revisada a cada 24 (vinte e quatro) meses ou sempre que houver alguma alteração na diretriz descrita.

1. OBJETIVO

Está política define o ambiente e as circunstâncias que os sistemas de rede, sistemas aplicativos e o monitoramento das atividades de comunicação serão executados.

2. ABRANGÊNCIA

Esta política se aplica a prestadores de serviço ou parceiros comerciais licenciados diretamente ligados a StoneX, prestadores de serviço ou parceiros comerciais serão monitorados para o cumprimento dos termos da sua licença e a respeito das políticas de uso aceitável da StoneX.

3. LEGISLAÇÃO RELACIONADA

- Resolução nº4.658/18 de BACEN
- Política de Gestão de Incidentes de segurança da Informação (POL-052)
- Cadeia de Valor de Serviços Relevantes (BCAM e DTVM)
- Política de Privacidade de Dados (POL-054)
-

4. DEFINIÇÕES

4.1. SIGLAS & TERMINOLOGIA

4.1.1. TI - Tecnologia da Informação

4.2. ÁREAS ENVOLVIDAS NO PROCESSO

4.2.1. Área Responsável

4.2.1.1. Segurança da Informação

4.2.2. Áreas Suporte

4.2.2.1. Tecnologia da Informação

5. DISPOSIÇÕES

fa

A monitoração é uma ferramenta essencial para a obtenção da informação, que deverá ser usada para vários propósitos:

- Planejamento para expansão da rede e atualizações de serviço.
- Investigação de irregularidades e tratamento dos incidentes.
- Testes de conformidade com políticas ou normas vigentes de órgãos e agentes reguladores locais ou teste de aderência as políticas globais da StoneX.
- Pedidos da aplicação da lei.

O gerente de TI tem a seguinte autoridade:

Autorizar os analistas de TI para executar procedimentos de monitoração na rede, sistemas, aplicações e dados que estejam em conformidade com a política e todas as leis e regulamentos locais e internacionais aplicáveis.

Os usuários são informados de que a utilização dos serviços na StoneX, como comunicação de dados, serviços de infraestrutura, sistemas e aplicações podem ser monitorados por pessoas autorizadas conforme permitido pelas leis e legislação local e internacionais vigentes. Leis e legislação permitem o monitoramento de sistemas e tráfego de rede para fins legítimos

5.1. PESSOAS AUTORIZADAS

De acordo com as leis locais vigentes, o Gerente de TI tem a autoridade para autorizar os funcionários adequados para monitorar a infraestrutura, comunicação, serviços e sistemas aplicativos. Outros Gerentes podem solicitar a autorização para que os outros funcionários designados possam monitorar apenas os serviços para o qual o departamento seja responsável.

5.2. ÉTICA

As pessoas autorizadas, incluindo administradores de rede e administradores de sistemas devem executar suas funções em conformidade com as diretrizes estabelecidas, em especial o as pessoas autorizadas devem:

- Respeitar a privacidade dos outros.
- Não usar ou divulgar informações obtidas durante o monitoramento para fins diferentes daqueles para os quais o processo foi aprovado.

- Salvaguardar as informações recolhidas no processo de monitoramento
- Destruir as informações recolhidas no processo de monitoramento quando ela não é mais necessária.

5.3. SERVIÇOS E APLICAÇÕES DE REDE

Todos os serviços disponibilizados em rede ou aplicativos são monitorados quando:

- Armazenamento de arquivos – utilização, tipos e tamanhos de arquivos.
- Violações de licença de uso de software.
- Estatísticas de rede;
- Anomalias do sistema e log de segurança.
- Tentativas de acesso bem-sucedidas – conta de usuário, data/hora, duração da sessão.
- Tentativas de acesso sem sucesso.
- Tráfego de rede.

Esta informação deve ser usada para ajudar a determinar se os sistemas da StoneX estão operando como previsto. Logs do sistema e outras métricas são mantidas por um período tão longo quanto possível.

StoneX, tem o direito de examinar qualquer arquivo que esteja alocado em servidores ou estações de trabalho de propriedade da StoneX ou mesmo serviços de rede, instalações.

Esta política inclui computadores de propriedade da StoneX utilizados em residências dos funcionários e que estão conectados à rede da StoneX incluindo redes Wireless.

5.4. MONITORAMENTO FÍSICO

Em locais que a empresa instalou câmeras de segurança, as gravações dessas áreas devem ser armazenadas por um período mínimo de três semanas, no entanto, se houver um incidente sobre investigação, as gravações serão mantidas durante o tempo necessário para ajudar a resolver o incidente.

5.5. E-MAIL

Todos os e-mails recebidos via sistema de e-mail central estão sujeitos as seguintes medidas:

- Prevenção Vírus.

- AntiSpam.
- Prevenção de e-mails não autorizados.

Logs dos e-mails devem ser usados para acompanhar os problemas relatados para o Gerente de Data System. Os registros deverão ser mantidos por 5 anos.

Logs de e-mail devem registrar as seguintes informações:

- Horário, endereço de origem do e-mail, sistema de endereço IP, endereço de destino do e-mail, ID mensagem e tamanho da mensagem.
- Informações sobre protocolo SMTP associados com os diálogos iniciais e finais.

5.6. ACESSO WEB

Todo acesso à Web deve ser controlado através de aplicativo instalado nas máquinas dos usuários, impedindo o acesso a sites considerados indevidos.

Em casos de exceção, uma solicitação pode ser realizada através do Portal FreshService informando o motivo da exceção, impacto do bloqueio e usuários afetados.

5.7. MONITORAMENTO DE REDES

5.7.1. Tráfego de Internet

- O tráfego de entrada da Internet está sujeito as seguintes restrições implementadas nos firewalls que conectam à rede da StoneX:
- Portas especificas, IP, que estão associadas com os serviços que apresentam serias vulnerabilidades, são bloqueados.
- A lista atual de bloqueio de porta é derivada de conhecimentos locais, experiências e pelo conselho nacional CERT-BR.
- Alguns filtros são utilizados para bloquear endereços específicos seguindo as devidas solicitações.

Os firewalls de borda da StoneX disponibilizam informações de rede, que estão disponíveis para os seguintes propósitos:

- Investigação de falha.
- Tratamento de Incidente.
- Perfis de Tráfego.
- Alertas sobre atividades suspeitas.

Os Logs não gravam o conteúdo do aplicativo; eles simplesmente gravam determinados campos de IP e dados, ou seja, endereço IP de origem, endereço IP de destino, números das portas, volume e carimbo do tempo.

5.8. MONITORAMENTO DE TRÁFEGO

Pessoas autorizadas podem monitorar a rede da StoneX ou algum segmento específico para:

- Protocolos e aplicações em uso.
- Fontes e destinos – Padrões de tráfego.
- Métricas de desempenho.
- Bytes enviados e recebidos pelo Router e switch – uso de banda.
- Erros por Router e switch.
- Condições de falhas.

Registros estatísticos são mantidos durante o tempo em que sejam considerados úteis.

Em circunstancias excepcionais, ou seja, para ajudar a investigar incidentes ou condições de falha, interações especificas entre endpoints podem ser monitorados e gravados para análise.

Os registros são mantidos durante o tempo que o incidente ou falha está ativa, depois serão destruídos.

5.8.1. Sistema de Detecção de Intrusão

Onde há sistema de detecção de intrusão (IDS) da StoneX estes devem ser usados para identificar atividades maliciosas, incluindo computadores comprometidos localmente e derivar filtros adicionais de segurança para o roteador. Estes sistemas sempre buscam por assinaturas reconhecíveis de perfis de ataques comuns.

Quando uma assinatura é reconhecida, um evento de log deve prover detalhes da assinatura, exemplo: endereço IP de origem, endereço IP de destino, porta de origem, porta de destino.

Sistema de detecção de intrusão produzem registros extensos que exigem um exame minucioso para identificar com segurança a atividade maliciosa. Logs de Ids serão mantidos por curtos períodos.

5.8.2. Varredura Ativa

Pessoas autorizadas podem realizar varreduras em segmentos da rede para identificar vulnerabilidades ou computadores infectados.

Pessoas autorizadas devem exercer a devida diligência ao realizar qualquer atividade de verificação, em especial devem:

- Informar os administradores de rede e sistemas responsáveis pelos sistemas onde irão ser efetuadas as atividades de varredura planejadas e fornecer os seguintes parâmetros:
  - Horário, tempo de execução.
  - Sistema de varredura, (Endereço IP).
  - Objetos de varredura e quais vulnerabilidades devem ser testadas.
- Tomar medidas razoáveis para garantir a operação ou funcionalidade de qualquer sistema onde será efetuada a varredura.
- Identificar sistemas com vulnerabilidade relevante para os administradores do sistema.

Registros de varreduras ativas serão mantidas para ajudar a identificar áreas onde ações associadas a outras políticas da StoneX podem ser necessárias. Usuários que utilizam a rede Guestnet, possivelmente poderão passar por uma varredura da rede, mesmo utilizando computadores pessoais ou qualquer sistema ligado as instalações StoneX.

Qualquer usuário que não concorder autorização para a varredura, não deve conectar seu sistema a rede StoneX GuestNet.

5.9. RESPONSABILIDADES

O departamento de TI é responsável pela gestão e execução desta política. Administradores de sistema são responsáveis pelas tarefas do dia-a-dia associadas com esta política.

5.9.1 Segurança da informação

- Informar aos usuários medidas relacionadas as atividades na rede; interações, serviços, sistemas e métodos de comunicação podem ser monitorados.
- Identificar quais pessoas estão autorizados a executar funções de monitoramento.
- Destacar a ética, procedimentos e garantir que as pessoas autorizadas devem empregar antes, durante e após a realização das funções de monitoramento.
- Identificar quais informações podem ser obtidas pelo processo de monitoramento.
- Identificar o período que as gravações deverão ser mantidas.

Descreve as finalidades que podem ser usadas para "informações monitoradas", incluindo quaisquer ações que possam ocorrer.