BIM
Boletim Informativo Mensal
Comunicar para Educar
Abril/2022 – Ano 3 – nº 27

Conheça sobre *Keylogger*

Você sabia que tudo que é digitado no seu teclado pode estar sendo espionado por uma pessoa ou por sistema não-autorizado? E que estas informações podem estar sendo apropriadas e utilizadas de forma indevida?

O que é um *Keylogger*?

Keylogger pode ser um aplicativo ou mesmo um pequeno dispositivo (colocado entre o teclado e o PC), que monitora e registra as teclas digitadas.

Todo *Keylogger* é ameaça ou é irregular?

Não. Existem formas de "*keylogger*" que possuem uso legítimo. Há utilizações no mundo da tecnologia, no qual estas são normalmente intermediadas por sistemas inteligentes. Por exemplo, os corretores ortográficos utilizados em aplicativos. Também, os programas que monitoram atividades de filhos menores de idade, a fim de evitar que estes possam acessar sítios *web* maliciosos ou adultos.

Keylogger é uma ameaça?

Normalmente, o objetivo do cibercriminoso é conseguir senhas, números de cartão de crédito, informações bancárias, entre outras informações. Apesar de ser uma forma de vazar dados pessoais relativamente antiga, ainda hoje, é bastante utilizado.

Como cibercriminosos instalam *Keylogger* malicioso?

Normalmente, os *Keyloggers* são instalados da mesma forma que outros "vírus". Alguns exemplos:

- quando o usuário abre um arquivo ou *link* malicioso que veio anexado por um *e-mail*, o famoso *phishing*;
- em páginas da *Internet* maliciosas ou *sites* legítimos invadidos e modificados por "*hackers*" com este objetivo; e
- pode ser um pen drive "perdido", que o usuário encontre, conecte e automaticamente infecte a sua máquina.

Como se proteger de *Keylogger*

Dentre os principais pontos para se evitar ser monitorado por algum *Keylogger* malicioso, podemos sugerir o que segue:

- utilizar sistema genuíno (não "pirateado") e atualizado;
- desconfiar de *link* e anexo vindo por *e-mail* de origem desconhecida;
- manter o sistema antivírus ativado e atualizado na sua última versão;
- Usar solução de segurança para realizar varredura de uma unidade externa conectada aos seus dispositivos;
- evitar navegar em sítio *web* desconhecido;
- não baixar arquivo cuja fonte não seja conhecida ;
- utilizar o teclado virtual (ao invés do teclado físico) para inserir senha em banco *online*; e
- utilizar o aplicativo oficial da instituição bancária em seu celular.

Competências do Núcleo de Segurança e Credenciamento

O Núcleo de Segurança e Credenciamento (NSC) é o órgão central de credenciamento de segurança para o tratamento de informação classificada no âmbito do GSI/PR. As competências do NSC incluem habilitação de órgãos; credenciamento de segurança de pessoas naturais; e elaboração e acompanhamento de acordos internacionais.

Habilitação de órgãos é processo de credenciamento a que o órgão é submetido. Em geral, é avaliada a adesão aos requisitos mínimos impostos pela lei. Com isso, o órgão estará em condições de tratar e armazenar, de forma adequada, informação classificada.

No credenciamento de segurança de pessoa natural é efetuado um processo aberto de investigação, para conceder credencial a pessoa que possui necessidade de conhecer determinada informação classificada, em qualquer grau de sigilo (reservado, secreto e ultrassecreto).

Por fim, os Acordos Internacionais são firmados com a finalidade de assegurar a proteção da informação classificada trocada entre a República Federativa do Brasil e outros países.

Mapeamento de Ativos de Informação

Um dos importantes processos da gestão de segurança da informação previsto na Instrução Normativa (IN) GSI/PR Nº 3, de 28 de maio de 2021, é o processo de mapeamento de ativos de informação, ao qual aquela norma dedica um capítulo inteiro.

Para compreender o que significa esse processo, vamos mostrar inicialmente alguns conceitos relacionados, utilizando como base o Glossário de Segurança da Informação, aprovado pela Portaria GSI/PR Nº 93, de 18 de outubro de 2021.

Primeiramente, esclarecemos que **risco**, em sentido amplo, é a possibilidade de ocorrência de um evento que pode impactar ativos de informação da organização e, em última análise, o cumprimento de objetivos de negócio. O risco pode ser medido em termos de impacto e de probabilidade.

Ativos de informação são os meios, os equipamentos e os sistemas utilizados para armazenamento, transmissão e processamento da informação; os locais onde se encontram esses meios; as pessoas que têm acesso a esses meios; e o conhecimento ou o dado que tem valor para um indivíduo ou uma organização.

Vulnerabilidade é uma condição que, quando explorada por um criminoso, pode resultar em uma violação de segurança. Um exemplo de vulnerabilidade é uma porta aberta, pois ela pode ser utilizada para que alguém entre mais facilmente pela porta.

Ameaça é um conjunto de fatores externos com o potencial de causar dano para um sistema ou organização. Um exemplo seria ter um criminoso rondando pela vizinhança.

Conforme o previsto na norma, para a realização do processo de mapeamento de ativos de informação, deverá ser elaborado um **registro de ativos de informação** contendo:

- os responsáveis de cada ativo de informação;
- as informações básicas sobre os requisitos de segurança da informação de cada ativo de informação;
- os contêineres de cada ativo de informação; e
- as interfaces de cada ativo de informação e as interdependências entre eles.

Para isso, o agente responsável pela gestão dos ativos de informação do órgão ou da entidade, deverá:

- identificar e classificar os ativos de informação por nível de criticidade;
- identificar potenciais ameaças aos ativos de informação;
- identificar vulnerabilidades dos ativos de informação;
- consolidar em um relatório informações resultantes da análise do nível de segurança da informação de cada ativo de informação ou de grupos de ativos de informação ;
- autorizar a atualização do relatório; e
- avaliar os riscos dos ativos de informação ou do grupo de ativos de informação.

Sendo assim, destaca-se que o processo de mapeamento de ativos de informação tem o objetivo de estruturar e manter um registro de ativos de informação, destinado a subsidiar os processos de gestão de riscos, de gestão de continuidade e de gestão de mudanças nos aspectos relativos à segurança da informação.

Por fim, é necessário ter em mente que o processo de mapeamento de ativos de informação fornece elementos básicos para a adequada implantação e execução de outros processos de gestão de segurança da informação, que também constam da IN GSI/PR nº 3/2021 e sobre os quais falaremos em futuras edições deste Boletim.

Fonte: https://www.gov.br/gsi/dsi/ https://www.gov.br/ctir
Editorial/redação/diagramação: AssESI Sugestões: asscom.dsi@presidencia.gov.br