

Presidência
SBS - Quadra 04 Lote 3/4
21º Andar
70.092-900 - Brasília - DF

Ofício CAIXA nº 274/2013

Brasília, 14 de novembro de 2013

A Sua Excelência a Senhora
Senadora VANESSA GRAZZIOTIN
Presidente da CPIDAESP
Comissão Parlamentar de Inquérito da Espionagem
Senado Federal
70.165-900 – Brasília/DF

Assunto: Requerimento nº. 62 CPI-ESP

Senhora Senadora,

1. Reportamo-nos ao Ofício nº. 55/2013 - CPIDAESP, por meio do qual essa Comissão Parlamentar de Inquérito encaminha o Requerimento nº. 62, para solicitar “informações ao Exmo. Sr. Presidente da CEF sobre as ações para minorar a possibilidade de ataques virtuais/digitais às atividades do governo brasileiro” nos termos seguintes.

1.1 *1 – Criptografia:*

- a) Qual empresa desenvolveu o referido sistema?
- b) Qual o sistema utilizado?

2- *Segurança da Informação:*

- a) Quais os dispositivos de segurança de informação utilizados?
- b) Qual a empresa ou empresas que forneceram tais dispositivos?

2. Apresentamos, a seguir, os esclarecimentos devidos, pertinentes às salvaguardas que garantem a confidencialidade de dados sensíveis no âmbito da CAIXA.

2.1 Informamos, em relação à Criptografia, que a CAIXA utiliza diversos algoritmos criptográficos simétricos e assimétricos, bem como algoritmos para cálculo de hash visando à proteção dos dados e informações críticas de clientes, usuários e parceiros.

2.1.1 Nesse contexto, usa algoritmos de hash tipo SHA-2, algoritmos simétricos DES, 3-DES e AES com chaves variando de 64 a 256 bits (dependendo do contexto) e algoritmos assimétricos RSA com chaves de 2048 bits, além de contarmos com as condições técnicas necessárias para fazer uso dos algoritmos de curvas elípticas.

2.1.2 Todo o tráfego de rede que possua dados sensíveis, por definição, é criptografado por protocolos distintos como SSL V3, IPSec, TLS, etc, os quais fazem uso dos algoritmos criptográficos acima descritos.



2.1.3 Os algoritmos assimétricos, como os supracitados, fazem uso de certificado padrão ICP Brasil V2 de suma importância pela guarda e manutenção dessa infraestrutura de chaves públicas por entidades sediadas em território nacional.

2.1.4 Além disso, a CAIXA é Autoridade Certificadora de primeiro e segundo nível e responsável pela emissão desses certificados, o que lhe propicia um maior grau de controle da veracidade destes.

2.1.5 É de se destacar que o sigilo das informações, em razão da utilização de algoritmos de criptografia, é garantido pelo tamanho e sigilo das chaves, bem como pela robustez do algoritmo e não pelo seu desconhecimento.

2.1.5.1 Na CAIXA, a guarda dessas chaves é feita em hardware especializado chamado HSM (Hardware Security Module) dos fornecedores IBM, SafeNet e Mais2x.

2.1.6 Além do tráfego de rede, o armazenamento de dados, por definição, faz uso da criptografia conforme o nível de criticidade do dado (servidores de arquivo, estações e SGBD).

2.1.6.1 Nesse caso, temos os algoritmos acima descritos implementados nas diversas plataformas - Microsoft, Oracle, IBM, CA, Postgree e Linux (RedHat e Debian).

2.2 Quanto à Segurança da Informação no âmbito CAIXA, esclarecemos que vários princípios mundialmente reconhecidos são considerados, entre os quais “a defesa em profundidade”, segundo o qual a proteção se dá por uma série de controles de segurança físicos, lógicos e em processos.

2.2.1 A infraestrutura tecnológica dessa proteção é construída em ambientes lógicos segregados e implantadas através de camadas isoladas dos ativos de TI e conforme funcionalidade e criticidade da informação existente.

2.2.2 Esses isolamentos são baseados em tecnologias distintas de proteção, incluindo fornecedores diferentes, visando aumentar o grau de dificuldade de perpetrar com sucesso uma invasão.

2.2.3 Quanto às camadas, considerando especificamente a garantia do pilar confidencialidade, são compostas de diversas soluções.

Controle de acesso de tráfego de redes (Firewall/ACL):

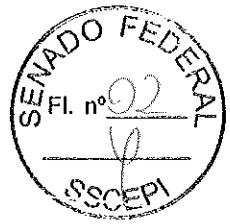
- Microsoft TMG
- CISCO PIX 535
- Checkpoint da Chekpoint
- F5 da BigIp
- Roteadores CISCO e Huawei

Detecção e barreira de intrusão:

- Snort software livre
- Sourcefire da Sourcefire

Bases de autenticação e autorização de controle de acesso:

- RACF da IBM
- Open LDAP software Livre
- Microsoft AD



Acesso Lógico a Sistemas:

- Definido por Matrizes de Perfis de Acesso (princípio da “Necessidade de Conhecer”)

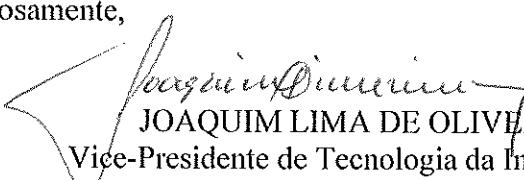
2.2.4 Ainda no contexto da segurança da informação e confidencialidade, mas não restrito a ele, a CAIXA atua de forma complementar a todos esses ativos tecnológicos de segurança com um Grupo de Resposta a Incidentes de Segurança Tecnológica – GRIST – que, entre outras funções, atua na monitoração dos eventos e tratamento dos incidentes de segurança, conforme preconizam as melhores práticas e normas governamentais.

2.2.5 As tecnologias e processos citados são, portanto, interdependentes e formam um todo pela sua atuação conjunta e complementar, propiciando controle de acesso, monitoração, análise dinâmica, bloqueio, tratamento e evolução/correção da proteção existente.

2.3 Ressaltamos, por fim, que a CAIXA busca continuamente a melhoria do seu processo de Segurança da Informação atuando não apenas na frente de tecnologias, mas também nos processos de negócio e na conscientização de seus empregados e parceiros.

3. Colocamo-nos à disposição para eventuais esclarecimentos que se fizerem necessários.

Respeitosamente,



JOAQUIM LIMA DE OLIVEIRA
Vice-Presidente de Tecnologia da Informação



JORGE FONTES HEREDA
Presidente

Subsecretaria de Apoio às Comissões
Escolares e Parlamentares de Inquérito
Recebido em 14/11/15
As 15:23 horas


Felipe Costa Geraldes
Técnico Legislativo
Matr. 229.869

