ESP REC
000016

Supremo Tribunal Federal

Ofício nº 342/GP

Brasília, 13 de novembro de 2013.

A Sua Excelência a Senhora
Senadora VANESSA GRAZZIOTIN
Senado Federal
Brasília/DF

Assunto: Resposta ao Ofício nº 49/2013 – CPIDAESP

Senhora Senadora,

Ao cumprimentar Vossa Excelência, e em atenção ao Ofício nº 49/2013 – CPIDAESP, de 31 de outubro do corrente ano, encaminho as informações prestadas pela Secretaria de Tecnologia da Informação do Supremo Tribunal Federal, em que foram respondidos os questionamentos constantes do Requerimento nº 056/13, anexado ao Ofício em referência.

Aproveito o ensejo para renovar a Vossa Excelência protestos de elevada estima e consideração.

Ministro JOAQUIM BARBOSA
Presidente

Subsecretaria de Apoio às Comissões Especiais e Parlamentares de Inquérito
Recebido em, 14 / 11 / 2013
Às 16h10 horas.
Keny Cristina R. Martins
Analista Legislativo
Mat 221 664

SENADO FEDERAL
Fl. nº 01

SUPREMO TRIBUNAL FEDERAL
Secretaria de Tecnologia da Informação
Seção de Planejamento e Gestão

Memorando n.º 001/2013 – SPGE/STI

Requerimento n.: 056/2013

Assunto: Requerimento de informações sobre ações para minorar a possibilidade de ataques virtuais/digitais às atividades do governo brasileiro.

Senhora Secretária-Geral da Presidência,

O Supremo Tribunal Federal está envidando grandes esforços no sentido de buscar proteger as informações produzidas, obtidas e custodiadas na instituição. Nesse sentido, a Secretaria de Tecnologia da Informação publicou em conjunto com a Secretaria-Geral da Presidência e a Diretoria-Geral, no dia 28 de Junho de 2013, a Resolução 507/2013. Por meio dela, foi criado o Comitê Corporativo de Segurança da Informação que tem como principais objetivos:

I – indicar requisitos e necessidades corporativas de segurança da informação;

II – propor a elaboração e a revisão de políticas, diretrizes, normas e procedimentos inerentes à segurança da informação;

III – promover a definição, a implantação, o monitoramento e a revisão de um sistema de gestão de segurança da informação;

IV – propor a implementação de ações corporativas de segurança da informação, bem como o acompanhamento de seus resultados;

V – promover a divulgação de boas práticas de segurança da informação.

2. A partir da criação do referido Comitê, o STF tem tratado a questão de forma sistêmica, conforme preconizam as melhores práticas da série de normas ISO/IEC 27000, o framework de Governança de TI Cobit 5.0 e o código de melhores práticas ITIIL V3.

3. Especificamente quanto aos questionamentos sobre criptografia e segurança da informação, seguem informações:

I) Criptografia

- o STF utiliza o protocolo SSL/TLS na troca de informações referente aos sistemas de Peticionamento Eletrônico, Integração entre Órgãos e Integração entre Tribunais com o uso de certificados digitais ICP-Brasil[1], e com isso, todo o tráfego em trânsito é criptografado. Os servidores que implementam essa criptografia utilizam software livre desenvolvido pela empresa Apache;
- Os atos processuais de processo eletrônico são realizados por meio de assinatura digital, com uso de certificados ICP-Brasil – algoritmo RSA;
- O STF utiliza o Microsoft Outlook como solução para criptografia de e-mails – que utiliza certificados digitais ICP-Brasil com algoritmo RSA para troca de chaves e algoritmo 3-DES para criptografia simétrica dos dados. Entretanto, não há registros de uso dessa funcionalidade de forma massiva, para o que se mostra necessária a realização de treinamento, assunto de deliberação do Comitê Corporativo de Segurança da Informação;
- Não há solução institucional na criptografia de dispositivos móveis – como *pendrives*, laptops, celulares. Em suma, quando há utilização de criptografia, são utilizados algoritmos comerciais – AES, 3DES, RSA. Não há utilização de algoritmos de Estado.

II) Dispositivos de segurança utilizados:

- Firewall Fortinet Fortigate 1000C, Firmware 4 MR3 com funcionalidades de filtro de pacotes, IDS/IPS, Webfilter, Filtro de Aplicações, Load Balance, Antispam, Antivírus, VPN.

[1] Conforme instituído pela Medida Provisória 2.200-2, de 24 de Agosto de 2001.

- Firewall Fortigate 50B, Firmware 4 MR3 com funcionalidades de filtro de pacotes, IDS/IPS, Webfilter, Filtro de Aplicações, Load Balance, Antispam, Antivírus, VPN.
- Mail Relay OpenSource Postfix (2.7.1), Clamav (0.97.8), Amavisd-New (2.6.4), Spamassasin (3.3.1)
- Sistema de Antivírus para estações e servidores: Symantec Endpoint Protection (SEP), versão 12.1.2015.2015
- Sistema de Antivírus para correio eletrônico: Symantec Mail Security (SMS), versão 6.5.2.97
- Serviço de Autoridade Certificadora Microsoft
- Serviço de Proxy (Apache)

4. Além das informações prestadas sobre dispositivos de criptografia e segurança utilizados, entendemos que também seja importante prestar informações sobre os demais sistemas e tecnologias utilizadas, já que, como foi noticiado pela grande mídia, alguns elementos de rede, sistemas operacionais e aplicativos poderiam conter *backdoors*.

I) Dispositivos de rede utilizados:

- Switch Camada – Fabricante Extreme Networks; Modelo Summit x250e-24p; x250e-48p; x450a-24t; x460-48t. Firmware: 15.1.2.12 v1512b12-patch1-6;
- Roteador Cisco Networks 3845 Version 12.4(24)T3; Roteador Cisco Networks 2851 Version 12.4(23a)
- Access Point Cisco Networks 1242AG 12.4(23c)JA2
- Controladora Wi-Fi Cisco Networks 4400 Firmware 7.0.116.0

II) Ambiente de Servidores (Windows 2008 R2, Red Hat Enterprise Linux 6.3):

- Apache HTTPD 2.2
- Apache Tomcat 6
- BRS 8.0

- CAS EMC Centera
- Citrix Secure Gateway 3.2
- Citrix XenApp 6.0
- Citrix Web Interface 5.2
- Jboss 4.3 e 6.1
- Microsoft SQLServer 2008R2
- Microsoft Exchange 2010
- Microsoft Windows Media Services
- Microsoft Sharepoint
- Microsoft IIS 7.0
- Netbackup 7.5.0.5
- Storage VNX 5700
- Storage Symmetrix DMX3
- Oracle Databse Enterprise Edition 11gR2
- Oracle MySQL 5.1
- Openfire 3.8.2
- Postgres 8.3
- VMware vSphere Hypervisor 5.0 U2
- VMware ESXi 5.0 U2
- VMware vSphere Client 5.0

III) Aplicativos contidos nas estações de trabalho do STF, que executam os sistemas operacionais Microsoft Windows 7 (32-bits) e Microsoft Windows XP 32 bits:

- 7-Zip v9.2
- Adobe Acrobat Reader v10.1.0
- Adobe Flash Player v10.3.183.7
- BRS 7.0
- CDBurner XP v.4.3.8.2631
- Charismathic v.4.9.3
- eToken 5.1.66.0
- Java v7 u17

- K-Lite 8.2.0
- Landesk 9.0
- Libre Office v.3.3.2
- Microsoft Office Professional 2003 ou 2010.
- PDF Creator 1.0.2
- SafeSign 3.0.11
- SigNext 3.2.2
- Spark 6.5.3

IV) Aplicativos instalados em apenas algumas estações, de acordo com a necessidade e licenças disponíveis:

- Acrobat Standard 7.0
- Acrobat Pro 11.0
- Captivate 5.5
- Dreamweaver CS5
- Dreamweaver CS6
- Fireworks CS3
- Fireworks CS5
- Flash Professional CS5
- Flash Professional CS6
- Font Folio 11
- Illustrator CS6
- Incopy CS6
- Indesign CS6
- Photoshop CS6
- Photoshop Lightroom 4
- Premiere Pro CS4
- Premiere Pro CS5
- Presenter 7
- AutoCAD Revit Architecture Suite 2012
- AutoCAD Revit MEP 2012

- 3Ds MAX Design 2012
- Corel Draw Suite X4
- Aurélio 6.0
- Houaiss 2009
- Michaelis
- Heritage
- Longman
- Sound Forge 9.0 (Rádio Justiça)
- Sound Forge 9.0
- CD Architect 5.0 (Acompanha o Sound Forge 9.0)
- Sound Forge 10
- CD Architect (Acompanha o Sound Forge 10)
- Vegas 5.0
- Acid 4.0 (Acompanha o Vegas 5.0
- Vegas 7.0
- Cd Architect 4.0 (Acompanha o Vegas 7.0)
- Nero 6.0
- Easy Dental 7.0
- Vídeo Farma 2.51
- Folio Views 4.5
- Folio Views 4.7
- Radio News Play
- Extra Personal Client 6.7
- SPSS PASW Statistics 18
- ABBYY Recognition Server 3.0
- Diet Win Professional 2008
- Alceste
- Centura Web Developer 1.1.1
- Jaws Professional 12
- Extensis SuitCasse Fusion 4
- OCR 9.0

SUPREMO TRIBUNAL FEDERAL
Secretaria de Tecnologia da Informação
Seção de Planejamento e Gestão

Brasília, 13 de novembro de 2012.

RAFAEL RABELO NUNES
Gerente de Segurança da Informação[2]

EDMUNDO VERAS DOS SANTOS FILHO
Secretário de Tecnologia da Informação

[2] Gerente de Segurança da Informação indicado pelo Secretário de Tecnologia da Informação, conforme descrito pela Resolução 507/2013 do Supremo Tribunal Federal