Nota Técnica nº 01/2018

Rio de Janeiro, 13 de agosto de 2018

Assunto: Tratamento de tráfego criptografado

I. Introdução

Nos últimos anos é possível observar o crescente volume de dados trafegando por canais criptografados. Em 2015 esse volume aumentou de 21% para 40% em 2015. Segundo o Gartner, em 2019 o volume de dados trafegando em canais criptografados pode chegar a 80%. O próprio Google noticiou que a partir de julho/2018 o Chrome classificará todos os sites que não sejam https como 'não seguros'. Se por um lado a adoção de criptografia sobre os dados trafegados traz tranquilidade e confiança para o usuário, por outro, tal recurso pode esconder ameaças a esses usuários. Uma pesquisa realizada pela Zscaler aponta que no primeiro semestre de 2017 a quantidade de ameaças escondidas em tráfego SSL dobraram. Segundo o Gartner, 50% de todos os malwares estarão escondidos em protocolos criptografados.

II. Avaliação

O uso do SSL em protocolos http provê um canal seguro para o tráfego de dados. Porém esse mesmo protocolo pode esconder ameaças como download de arquivos maliciosos, sessões criptografadas utilizadas para ataques, etc. Cabe ainda ressaltar que, neste cenário, não é possível aplicar as políticas institucionais de controle de acesso web a sites que utilizam https, permitindo que o usuário acesse conteúdo considerado como impróprio. Em junho de 2018, 74% do tráfego de dados na instituição já é sobre o protocolo https, ou seja, apenas 26% do tráfego de dados está sendo inspecionado e tratado adequadamente.

III. Recomendações

Entendo ser necessário avançar na implementação de ações que permitam a identificação e tratamento adequado das ameaças, bem como garantir o cumprimento da política de segurança da informação e comunicações da instituição, o Comitê de Segurança da Informação e

Comunicações, conforme consta na ata da sua 4ª reunião de 2018, realizada em 11 de julho de 2018, entende e ratifica a necessidade de inspeção de tráfego, porém respeitando pressupostos indiscutíveis como o sigilo das correspondências, privacidade dos dados pessoais, sigilo médico, entre outros. Assim, recomenda-se que as áreas de TI correlatas da Fiocruz, ao inspecionarem dados trafegando em canais criptografados, não inspecionem dados relacionados à bancos, operações financeiras, compras/leilão, organizações governamentais, educação, saúde/medicina, comunicações em geral (incluindo chats, webmail e telefonia usando Internet) e dados pessoais.

IV. Referências

- https://www.ibm.com/support/knowledgecenter/pt-br/SSHLHV_5.3.1/com.ibm.alps.doc/concepts/alps_outbound_ssl.htm
- http://g1.globo.com/tecnologia/blog/seguranca-digital/post/chrome-marcara-sites-sem-criptografia-como-nao-seguros.html
- https://www.zscaler.com/blogs/research/rise-ssl-based-threats-1
- https://www.defcon-lab.org/transicao-para-o-https-um-desastre-verde-e-amarelo-anunciado/

Misael Sousa de Araujo
Comitê de Segurança da Informação e Comunicações