Circular Normativa n.º 02 - SPMS

Assunto: Medidas excecionais cibersegurança

Para: Todas as instituições do SNS/MS

Como é do conhecimento geral, tem vindo a decorrer um ciberataque sem precedentes. A apreciação dos factos disponíveis levou a necessidade de medidas cautelares adicionais no sentido de proteger o SNS e de evitar qualquer disrupção de serviços. Após uma avaliação realizada à Conduta de utilização de acesso à internet foi detetado que diariamente são registados 390 000 malwares[1], existindo atualmente cerca 14 milhões de diferentes tipos de malwares. Neste sentido, é prioritário que cada uma das instituições adote comportamentos preventivos.

Assim, de forma a repor na totalidade o funcionamento dos serviços de email e acessos à internet, é necessário avaliar o nível de concretização das medidas de proteção já implementas na Circular Normativa n.º 01 (http://spms.min-saude.pt/wp-content/uploads/2017/05/Circular-Normativa-n%C2%BA1-SPMS-medidas-ciber-seguran%C3%A7a-v.2.pdf)

- Para a ativação do serviço de Email às instituições é necessário garantir que as medidas de proteção que foram recomendadas na Circular Normativa n.º 01 foram cumpridas pelas mesmas. Para este efeito já foi disponibilizado aos responsáveis de notificação obrigatória (RNO)/Direção de Sistemas de Informação, de cada instituição, um questionário que permite de forma rápida aferir por instituição qual o nível de adoção das recomendações;

- É com base no resultado desta avaliação que a SPMS disponibilizará por instituição o serviço de Email, tendo como prioridade disponibilizar o serviço às instituições já migradas para o EXCHANGE ONLINE;

- As instituições devem identificar e rever o nível de privilégios de administração de sistemas dos seus colaboradores internos, numa política base de acessos mínimos e com conta específica utilizada para esse efeito. Deve ser tido em conta que as credenciais de acesso nominativas dos utilizadores não devem possuir privilégios na administração de sistemas. Devendo ser criadas credencias especificas cuja lista, privilégios e nome e email institucional dos colaboradores com acesso às mesmas, deve ser remetida por email ao cuidado da SPMS até dia 18.05.17 ás 19h00;

[1] O software malicioso destina-se a ser executado sem o seu conhecimento

SPMS – Serviços Partilhados do Ministério da Saúde, E.P.E. Av. da República n.º 61 | 1050-189 Lisboa | Tel.: 211 545 600| Fax: 211 545 649

- No sentido das instituições melhor se protegerem de software malicioso, no que refere aos acessos à internet, deverão estas colocar na sua *blacklist* o acesso a sites que considerem ser nocivos para a sua organização, na sua máxima extensão;

- As contas de email utilizadas pelos profissionais deverão ser única e exclusivamente os emails institucionais. Prevendo-se a desativação do acesso a emails de outra natureza (ex: Gmail, Hotmail, etc) nos próximos dias;

- Todos os computadores com sistemas de informação que suportem sistemas críticos (gestão de pace-makers, bombas infusuras, ventiladores, etc) devem ser imediatamente desligados da internet caso não causem indisponibilidade do seu funcionamento, garantindo-se que só em caso extremo devem tais sistemas/aplicativos encontrar-se instalados em computadores com ligação a internet, nestas circunstâncias devem ser mantido atualizado um cadastro dos computadores, MAC address e sistema na direção de sistemas;

- As instituições devem proceder imediatamente à recolha automatizada de informação detalhada dos dispositivos. A SPMS disponibiliza o portal (vide https://snspt.sharepoint.com/sites/SAM/) que permite a recolha automatizada. Neste portal são disponibilizadas as ferramentas e as metodologias necessárias à recolha da informação, que permite o tratamento e análise de dados obtidos. O portal permite o acesso e a criação de relatórios pormenorizados que disponibilizam informação atualizada sobre as infraestruturas locais. As credenciais de acesso ao portal são as mesmas que são disponibilizadas para o Office 365. Relatórios preliminares devem ser remetidos no final do dia 17 maio, e 19 maio, e no final da analise;

- Com vista à otimização do sistema de filtragem de sites suspeitos de software malicioso da SPMS, será disponibilizado posteriormente um certificado digital a todas as instituições cuja instalação nos postos de trabalho deve ser efetivada até dia 19 maio;

- É responsabilidade de todas as instituições do SNS/MS sensibilizar imediatamente, imperiosamente os seus colaboradores para os comportamentos adequados em relação ao uso da internet e boas práticas a adotar para a prevenção de malwares (sugerem-se alguns exemplos de material já adotado noutras instituições). A fim de garantir a distribuição e adaptação á cultura institucional local, sugere-se a criação de versões originais com mesmo conteúdo a adotar e a distribuir a todos os profissionais nos próximos dias, as versões elaboradas devem ser remetidas á SPMS para partilha de melhores práticas. Exemplos:

  http://www.europarl.europa.eu/news/pt/news-room/20151207IFG06371/as-maiores-amea%C3%A7as-%C3%A0-ciberseguran%C3%A7a-em-2014

  https://www.iberdrola.pt/02sicb/corporativa/iberdrola/atencao-cliente/ciberseguranca/phishing

  https://www.iberdrola.pt/02sicb/corporativa/iberdrola/atencao-cliente/ciberseguranca/ransomware

Relembramos que logo que o email seja reposto deve ser utilizado o canal formal para a notificação de incidentes de segurança ecos.saude@spms.min-saude.pt e consultar a informação de alertas e segurança no seguinte endereço http://spms.min-saude.pt/alertas-e-seguranca/

A SPMS agradece desde já o empenho de todos os profissionais do SNS, nos últimos dias, e reitera o seu pedido para que juntos nos defendermos contra esta situação, e a compreensão dos utentes para qualquer pequena perturbação decorrente destas medidas de segurança que será sempre menor do que se não as tomarmos.

Lisboa, 15 maio 2017

Presidente da SPMS EPE

Henrique Manuel Gil Martins

Assinado de forma digital por Henrique Manuel Gil Martins
Dados: 2017.05.15 22:25:11 +01'00'

Henrique Martins

SPMS – Serviços Partilhados do Ministério da Saúde, E.P.E. Av. da República n.º 61 | 1050-189 Lisboa | Tel.: 211 545 600| Fax: 211 545 649