Circular Normativa n.º 03/2017

Assunto: Medidas Excecionais de Segurança

Para: Todas as instituições do SNS/MS

No passado dia 12 de maio de 2017, várias empresas e outras instituições de vários países (sobretudo operadores de comunicações), incluindo Portugal, foram afetados por um vírus informático denominado de *Wcry* ou *WannaCry, que* se propagou pela rede via protocolo SMB – *Server Message Block* (internet-redes). Trata-se de um *software* malicioso do tipo *ransomware* que inviabiliza o acesso do utilizador aos ficheiros (encriptação dos documentos), pedindo o pagamento de um valor na divisa digital *bitcoin* para restabelecer o acesso. O ataque teve como porta de entrada uma falha do sistema operativo Windows da Microsoft. Apesar de em março a Microsoft ter disponibilizado uma atualização de segurança que oferece proteções adicionais contra esta vulnerabilidade, os *hackers* aproveitaram-se dos utilizadores (sobretudo empresas) que não tinham atualizado a versão do sistema, para aceder aos computadores.

Verifica-se que cada vez mais é necessário melhores mecanismos que garantam a confidencialidade, integridade, disponibilidade e privacidade da Informação. Isto obriga a que as nossas instituições, em especial do sector da saúde, tenham de evoluir numa visão de segurança orientada não só para a proteção do perímetro eletrónico da Entidade mas para abordagens mais alargadas de preparação, deteção, resposta e melhoria contínua na proteção.

Sabemos que a resposta a incidentes relacionados com ataques ciber requerem que sejam levadas a cabo abordagens sistémicas de adoção de boas práticas ao nível da **organização** de **processos** e das **pessoas**, mas dada a sua natureza a proteção dos recursos tecnológicos configura um elemento fundamental de controlo, nomeadamente ao nível das **aplicações, sistemas e redes e comunicações**

Neste sentido, e afim de aumentar a resiliência para incidente como o ocorrido dia 12 maio 2017, e outros antecipados pelos peritos para futuro próximo, que se determina que as entidades do SNS/MS sejam capazes de adotar um conjunto de ações eficazes para se protegerem das principais ameaças. Para esse efeito devem ser considerados na sua essência os seguintes controlos de cibersegurança: 1./ *proteção de Email e Web Browser*, 2./Defesas de Malware, 3./Capacidades de Recuperação de Dados, 4./Resposta e Gestão de Incidentes, 5./Utilização controlada de privilégios de administração, 6./ Defesa de Perímetro.

No imediato, devem ser cumpridas as disposições das duas circulares anteriormente emitidas bem como, adicionalmente:

1. Até dia 30 de Maio deve configurar todos os DNS forwards para utilizar os servidores de DNS da RIS permitindo assim implementar centralmente políticas de segurança transversais ao SNS, evitando a dependência com a internet do funcionamento dos seus sistemas críticos;

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

2. Até dia 30 de maio deve demonstrar possuir, ou ter processo de compra ou instalação em curso, de uma ferramenta automatizada na monitorização contínua dos postos de trabalho, servidores e dispositivos móveis através de antivírus, anti-spyware, firewalls pessoais e Intrusion Prevention Systems;

3. Até 30 de maio assegurar que os privilégios de administração de Servidores e postos de trabalho só devem ser utilizados por equipas que administrem os sistemas de informação dessa entidade. Retirar direitos de administração em postos de trabalho onde estes não sejam necessários ou que, pelas suas características, sejam mais vulneráveis em segurança.

4. Até dia 30 Junho mostrar evidência que possuiu uma Política aprovada e um sistema de backups (seja para disco, DVD, tape ou outro suporte) onde sejam efetuadas cópias de segurança (backups) automáticas dos sistemas servidores e postos de trabalho que sejam críticos para a organização. Deve garantir que os backups estão encriptados. O ransomware não encripta dados já encriptados.

5. Até 30 de Julho deve demonstrar que possui ou está em implementação serviços de diretório e a capacidade de controlo de políticas de domínio para a gestão de credenciais dos utilizadores e privilégios de acesso;

6. Até Setembro de 2017 deve demonstrar ter implementado uma solução centralizada de controlo de dispositivos e software. A solução deve a permitir a gestão destes assets tal como a disponibilização de updates de melhorias e de segurança. Deve verificar junto da SPMS a possibilidade de disponibilização de licença de software ou pedido de serviço, caso não tenham capacidade ou recursos para o fazer.

Solicita-se ainda que seja considerado o conjunto de recomendações de boas práticas constantes do anexo I da presente circular.

Para acesso a outras informações sobre esta matéria tal como alertas, deve consultar a informação no seguinte endereço eletrónico http://spms.min-saude.pt/alertas-e-seguranca/

A SPMS solicita assim a ajuda de todos os profissionais do SNS para colaborarem nestas iniciativas e assim protegermos melhor a disponibilidade e qualidade dos serviços de prestação de cuidados tal com os bens públicos.

Lisboa, 19 maio 2017

Presidente da SPMS EPE

Henrique Manuel Gil Martins

Assinado de forma digital por Henrique Manuel Gil Martins
Dados: 2017.05.19 19:23:06 +01'00'

Henrique Martins

ANEXO I – Recomendações de Boas Práticas de Ciber-Segurança

A. DEFESAS DE MALWARE ("ANTI-VIRUS"), CCS eSIS #8

1) A Entidade deve implementar ferramentas automatizadas para monitorizar continuamente os postos de trabalho, servidores e dispositivos móveis através de antivírus, anti-spyware, firewalls pessoais e Intrusion Prevention Systems. Todos os eventos de deteção de malware devem ser enviados para as ferramentas de administração de anti-malware e servidores de logging da Entidade.
2) Deve implementar-se software *anti-malware* através de infraestrutura centralizada que compile informações de reputação de ficheiros ou garantir que os administradores efetuarem atualizações transversais em todas as máquinas da rede. Depois de ser aplicada uma atualização, os sistemas automatizados devem verificar se cada sistema recebeu a assinatura de atualização.
3) Deve limitar-se o uso de dispositivos amovíveis apenas a quem tenha uma necessidade operacional devidamente justificada e aprovada. Monitorizar o uso e a tentativa de uso de dispositivos amovíveis. Configurar os portáteis, os postos de trabalho e os servidores para que não executem automaticamente os conteúdos armazenados em dispositivos amovíveis, tais como, USB tokens (por exemplo pendrives), discos externos, CDs/ DVDs, dispositivos FireWire, dispositivos de conexão de tecnologia avançada (eSATA) e partições de rede montados. Configurar os sistemas para que automaticamente realizem uma análise de *anti-malware*a dispositivos amovíveis quando inseridos.
4) Ativar deteção de *exploits* através de *Data Execution Prevention*(DEP), *Address Space Layout Randomization* (ASLR), virtualização, etc. Para uma maior proteção implementar recursos como *Enhanced Mitigation Experience Toolkit* (EMET) que devem ser configurados para aplicar proteções adicionais a um conjunto mais amplo de aplicações e executáveis.
5) Utilizar ferramentas *anti-malware* na rede para identificar executáveis mediante o tráfego observável e utilizar outras técnicas que não a da deteção baseadas em assinaturas para identificar e filtrar conteúdo malicioso antes do mesmo atingir o seu objetivo.

B. RECUPERAÇÃO DE DADOS (CCS eSIS #10)

1) Assegurar que para cada sistema são efetuadas cópias de segurança (*backups*) automáticas pelo menos uma vez por semana, sendo que para sistemas que armazenam informação crítica estas cópias devem ter uma periodicidade mais reduzida. Para garantir a recuperação rápida de dados de um sistema a partir dos *backups* do sistema operativo, das aplicações e dos dados devem ser estabelecidos procedimentos de backup transversais. Esses três componentes de um sistema não precisam ser incluídos no mesmo arquivo de backup ou usar o mesmo software de backup. Devem existir vários backups ao longo do tempo, de modo a que, no caso de infeção por malware, a recuperação pode ser feita de uma versão que se acredita ser anterior à infeção original. Devem haver políticas internas de backup e estar em conformidade com quaisquer requisitos legais, regulamentar e contratuais.

2) Realizar regularmente testes às cópias de segurança (*backups*) executando um processo de recuperação de dados para garantir que o *backups*são recuperados corretamente.
3) Garantir que as cópias de segurança (*backups)* estão devidamente protegidas por meio da encriptação e implementação dos controlos de segurança física enquanto armazenados ou em trânsito. Este controlo abrange também os *backups* remotos e serviços *cloud*.
4) Assegurar que os sistemas críticos têm pelo menos um destino de *backups* que não é continuamente endereçável por meio de chamadas efetuadas a partir do sistema operativo. A implementação deste controlo mitigará o risco de ataques de CryptoLocker que procuram encriptar ou danificar os dados em todos os repositórios de dados endereçáveis, incluindo os de backups.

C. GESTÃO E RESPOSTA DE INCIDENTES, CCS eSIS #19

1) Garantir que existem procedimentos documentados de resposta a incidentes que incluem a descrição de funções para a gestão de incidentes. Os procedimentos devem definir as fases de gestão de incidentes.
2) Nomear os gestores responsáveis que irão suportar o processo de gestão de incidentes, atuando enquanto decisores.
3) Estabelecer na Entidade as regras e prazos para reporte por parte dos administradores de sistemas e de outros envolvidos na gestão de eventos de segurança da informação à equipa de gestão de incidentes. Os mecanismos para tal notificação e o tipo de informação que deve ser incluída na notificação de incidente devem da mesma forma estar especificados.
4) Implementar o procedimento interno para reporte de incidentes relevantes da equipa de gestão de incidentes de segurança ao Responsável pela Notificação Obrigatória da Entidade para garantir a Notificação Obrigatória de Incidentes de Cibersegurança ao Elemento da Coordenação Operacional de Segurança (ECOS) da Saúde de acordo com o Despacho n.º 1348/2017, publicado em Diário da República n.º 28/2017, Série II, de 2017-02-08-Saúde -Gabinete do Secretário de Estado da Saúde.
5) Manter atualizada e comunicar aos colaboradores da entidade e terceiros a informação de contato da equipa de gestão de incidentes para reportar os incidentes de segurança (por exemplo, manter um endereço de e-mail de seguranca@entidade.min-saude.pt ou por exemplo página online http://entidade.min-saude.pt/seguranca).
6) Publicar a informação disponível para todas as partes envolvidas, incluindo colaboradores internos e externos, sobre os procedimentos de reporte de eventos e incidentes de segurança da informação à equipa de gestão de incidentes. Essa informação deve ser incluída nas ações de sensibilização a colaboradores.
7) Realizar exercícios periódicos associados aos diferentes cenários de incidentes com as diversas partes envolvidas no processo de gestão de incidentes de forma a garantir que compreendem as ameaças e riscos atuais, bem como as responsabilidades no apoio à equipa de gestão de incidentes.

D. CONTROLO E MONITORIZAÇÃO DE CONTAS, CCS, eSIS #16

1) Deve existir capacidade para controlo de políticas de domínio para a gestão de credenciais dos utilizadores e privilégios de acesso. As Entidades deverão possuir um serviço de diretório com o objetivo de se dotarem de mecanismos de defesa permitindo ao mesmo tempo contribuir para uniformizar uma Identidade única de utilizar para o SNS. Com esta arquitetura espera-se poder usufruir de um conjunto de funcionalidades nomeadamente no que diz respeito à gestão de domínios.

E. INVENTÁRIO DISPOSITIVOS E SOFTWARE AUTORIZADO E NÃO AUTORIZADO, CCS eSIS #1, #2

1) Adoção de solução centralizada de controlo de dispositivos e software. A solução deverá a permitir a gestão destes assets tal como a disponibilização de updates de melhorias e de segurança. Deve verificar junto da SPMS a possibilidade de disponibilização de licença de software.

F. DEFESA DE PERIMETRO, CCS, eSIS #12

1) Devem as entidades efetuar todos os procedimentos necessários para garantir a permanente atualização dos sistemas de segurança de rede no seu perimetro. O firmware de equipamentos devem sempre estar o mais atualizados possível para garantia das proteções a ameaças emergentes. A existência de sistemas de segurança de rede com idade avançada potencialmente não estarão dotados de ferramentas capazes de responder aos riscos atuais. Devem ainda efetuar-se uma reavaliação periódica das listas ACLs das firewalls.
2) Deve contribuir para a adoção de uma estrutura única e hierárquica de DNS para todo o SNS. Todos os DNS forwards das entidades deverão passar a utilizar os servidores de DNS da RIS permitindo assim implementar centralmente políticas de segurança transversais ao SNS, evitando a dependência com a internet do funcionamento dos seus sistemas críticos.

G. **UTILIZAÇÃO CONTROLADA DE PRIVILÉGIOS DE ADMINISTRAÇÃO, CCS eSIS #5**

1. 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.
2. As senhas dos colaboradores deve seguir requisitos de segurança recomendados orientados por uma Política de Segurança da Informação;
3. As direções de informática, devem garantir que os utilizadores com credencias de Administração de Domínio, não efetuam login nos postos de trabalho sendo assim mais fácil preservar a utilização deste privilégio de acesso.

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