COMUNICADO À IMPRENSA

Ataque informático à rede do Grupo José de Mello Saúde

Lisboa, 10 de agosto, 2018 – Na sequência do ataque informático que ocorreu no passado dia 3 de agosto, tendo tido como alvo os Hospitais da CUF, o Centro Nacional de Cibersegurança (CNCS) esclarece que, enquanto Autoridade Nacional de Cibersegurança, e no âmbito da sua missão e competências, está a acompanhar em estreita cooperação o incidente com as entidades envolvidas.

Esta cooperação tem sido alargada a outras entidades da área da saúde, nomeadamente com a SPMS — Serviços Partilhados do Ministério da Saúde, E. P. E. com objetivo de conter novas infeções.

No seguimento das dificuldades identificadas a algumas máquinas do sistema informático da rede do Grupo José de Mello Saúde, a infeção foi prontamente detetada e controlada, sendo que o CNCS continua a trabalhar em articulação na resolução desta situação.

Recorde-se que o ransomware em causa, é denominado SamSam, tendo sido espoletado após um ataque à infraestrutura-alvo. Existem vários vetores de ataque, como por exemplo, os de força bruta ou a exploração de vulnerabilidades a máquinas com acesso remoto (RDP), protocolo de transferência de ficheiros (FTP) ou alguns servidores aplicacionais. Numa fase posterior, o atacante cifra o conteúdo dos computadores que tenham instalado sistemas operativos Microsoft Windows, pedindo um resgate em Bitcoins.

O CNCS recomenda que, nestes casos, não seja efetuado qualquer tipo de pagamento. Em caso de infeção detetada, aconselha-se que as entidades entrem em contato com o CNCS, de forma a ajudar no processo de mitigação e alertar a comunidade envolvida.

Com objetivo de mitigar futuros ataques, devem ser seguidas diversas recomendações, tais como:

- Efetuar atualizações periódicas dos sistemas operativos, bem como de aplicações;
- Realizar de forma regular testes de intrusão dos sistemas e rede da entidade;
- Verificar junto de serviços, como o Shodan ou Censys, a existência de ativos publicamente disponíveis;
- Restringir o acesso à porta 3389 (RDP), permitindo que sejam acedidos apenas por VPN;
- Sempre que possível uso de duplo fator de autenticação;
- Incentivar o uso de gestores de palavras-chave, de passwords longas e complexas, incluindo a sua não reutilização em mais do que uma conta

Para mais informações, contatar:
Sílvia Santos
silvia.santos@cncs.gov.pt