REGIÃO AUTÓNOMA DOS AÇORES
PRESIDÊNCIA DO GOVERNO
Gabinete do Subsecretário Regional da Presidência

Exmo. Senhor Chefe do Gabinete
De Sua Excelência o Presidente da Assembleia
Legislativa da Região Autonoma dos Açores
Rua Marcelino Lima
9901- 858 Horta

S/Referência	S/Comunicação	N/Referência	Data
S/2221/2021	30/06/2021	SE/2021/1039	13/09/2021

ASSUNTO: Requerimento ao Governo dos Açores n.º 156/XII-BE – Ataques informáticos ao Hospital do Divino Espírito Santo

Em resposta ao requerimento mencionado em epígrafe, subscrito pelo/a Senhor/a Deputado/a António Lima e Alexandra Manes, do grupo parlamentar do Partido BE/Açores, sem prescindir quanto ao teor do preâmbulo, encarrega-me o Senhor Subsecretário Regional da Presidência de informar a V. Exa., relativamente às questões colocadas o seguinte:

1 Os problemas informáticos no HDES tiveram origem em dois incidentes que envolveram a paragem dos sistemas, sendo que o primeiro radicou em erro/inconsistência num sistema de base de dados, não estando relacionado com questões de segurança.

2 As evidências de problemas de segurança informática só surgiram entre 22 e 23 de junho p.p. e, foram logo tratadas com as medidas de segurança necessárias a este tipo de situações.

3 Não está identificada a origem da ameaça, pelo que não é possível efetuar a sua atribuição, como é comum nestas situações. Tratou-se de um ataque de *ransomware* que não chegou a ser consumado na sua totalidade. Não foi pedido resgate.

4 Foi desenvolvido um elevado número de medidas em várias áreas por várias equipas de recursos especializados que envolveu a Direção Regional das Comunicações (DRCOM), a Direção Regional da Saúde, a *Microsoft* e a MEO/ALTICE. Destas medidas, destacam-se as seguintes:

- Geração de novas credenciais de acesso com privilégios de administração de sistemas;
- Implementação da segmentação das redes do HDES por intermédio da instalação e configuração de um equipamento do tipo Firewall cedido pela DRCOM;
- Análise forense dos equipamentos e infraestruturas afetadas;
- Realização de backups aos sistemas de informação em produção, que eram inexistentes;
- Reparametrização da infraestrutura de virtualização de suporte aos sistemas de informação;
- Contacto com diversos fornecedores aplicacionais para suprir a falta de documentação dos sistemas em exploração e poder promover-se a reposição da sua ligação ao ciberespaço de forma segura;
- Reposição faseada da conetividade ao ciberespaço dos Sistemas de informação em exploração;
- Reinstalação de servidores do tipo *Domain Controller*;
- Aplicação de políticas de acesso por tipo de utilizador e políticas de rotação de *passwords*;
- Formatação dos equipamentos terminais e a sua reinstalação.

Neste momento, os sistemas informáticos do HDES estão numa situação muito próxima da normalidade.

5 Não existem evidências de ataques informático ao HDES que possam ter surgido em maio.

6 A infraestrutura informática física do HDES é dispersa e está suportada em servidores locais e em servidores alojados em *datacenter* alugado à MEO/ALTICE. A entidade responsável pela administração dessa infraestrutura e pela sua segurança informática é o HDES. Convém referir que, em *Cibersegurança*, nunca ninguém pode afirmar que está 100% seguro, pois configura um processo constante e dinâmico, que envolve a mitigação de vulnerabilidades, que exige capacidade tecnológica, de análise, de técnica, de planeamento, de rigor na implementação e sensibilização.

7 Conforme o respondido em 1, o primeiro incidente não se tratou de ciberataque. Em relação ao segundo, as situações de enorme fragilidade foram várias, agora mitigadas. No entanto, algumas que

se podem elencar, e que decorrem de problemas de gestão e exploração de redes, infraestruturas de suporte e de sistemas de informação, das quais são exemplo:

- Melhoria nos equipamentos do tipo firewall que permitissem a segmentação das redes;
- Instalação de equipamentos de separação do tráfego;
- Maior segurança nas passwords, de utilizadores e de acesso aos servidores;
- Redefinição de credenciais e de privilégios;
- Melhoria nos processos de backups;
- Atualização dos sistemas operativos em exploração nos servidores.

8 O primeiro responsável ao nível das fragilidades detetadas é o departamento que tem a seu cargo a gestão e exploração da infraestrutura de suporte, as redes e os sistemas de informação.

9 No que se refere às aplicações utilizadas pelo HDES e às empresas responsáveis pelo seu desenvolvimento, operação e manutenção, é de sublinhar que, à semelhança das restantes unidades que compõem o Serviço Regional de Saúde, são muitos os sistemas utilizados, entre eles: O RADIO da Glintt; Cardiobase da Infotucano e Docabse/RIS da Mobilwave; VNA da Siemens; PICIS da MedicineOne; Archibus da Procos; Connexall da GlobeStar; Astraia (Ginecologia); Sisqual RH; Microsoft; Helpdesk da Solarwinds; Danysoft – Alarmes – PRTG; Antivírus – Cortex – DRCOM; VMWare – Digibéria; Primavera – Contabilidade; Clinidata – Laboratory Information System, da Maxdata; Glintt (gestão hospitalar, interface médica, interface enfermagem, aprovisionamento e farmácia), RIS.

10 Quanto aos sistemas que tiveram problemas de operacionalidade, importa referir que, em geral, foram afetados todos os sistemas de informação do HDES, pois, por medida de segurança, foram limitadas todas as comunicações de e para o hospital. Por esse motivo, estiveram em contingência durante algumas semanas, com recurso a alternativas instaladas para este efeito.

11 Como consequência do ataque informático ao HDES, resultaram muitas dificuldades em relação à atividade programada em consultas e exames, mas ultrapassadas com o recurso a alternativas criadas em contingência, tendo sido minimizados os atrasos na respetiva resposta do HDES. Foi possível recuperar os atrasos em poucas semanas depois da reposição da maioria dos sistemas de informação.

12 O impacto do incidente no Certificado Digital manifestou-se através do atraso no registo de algumas inoculações efetuadas no HDES e teve por base a indisponibilidade temporária no acesso à plataforma de registo de vacinação da DRS, decorrente das medidas de segurança tomadas nesse período.

Com os melhores cumprimentos,

Assinado por: **DUARTE MANUEL CARREIRO PACHECO PIMENTEL**
Num. de Identificação: 06094670
Data: 2021.09.13 11:36:04+00'00'
Certificado por: **Governo Regional dos Açores.**
Atributos certificados: **Chefe do Gabinete do Subsecretário Regional da Presidência.**
CARTÃO DE CIDADÃO