Alunos: Lucas E. Testoni, Eduardo Zirbell e Guilherme Kunhen

Análise dos Pilares (CID + A):71

1 – Confidencialidade:
O primeiro fator de confidencialidade foi quebrado quando o enfermeiro deixou a tela do computador desbloqueada concedendo acesso involuntariamente para o suposto “técnico de impressora” às informações delicadas, já o segundo fator foi quebrado pois o usuário de login do sistema administrativo estava exposto em um post-it.

2 – Integridade:
O fator de integridade foi quebrado quando o invasor conseguiu escalar o acesso administrativo por credenciais de login, expostas anteriormente no post-it, conseguindo acessar pela rede dos hospedes do hospital a tela de login do sistema administrativo podendo manipular os dados das consultas e prontuários.

3- Disponibilidade:
Não houve impacto direto na disponibilidade, mas houve um risco em potencial onde o invasor poderia impactar em diversos aspectos, incluindo a exclusão de diversos dados ou até mesmo deixar serviços inacessíveis alterando a senha dos usuários do sistema, dependendo da forma que ele funciona.

4- Autenticidade:
O fator de autenticidade foi quebrado quando o usuário mal-intencionado conseguiu o acesso, tornando impossível verificar a veracidade dos dados do sistema, visto que eles podem ter sido alterados.

Falhas de Controle:

Falha Física:
Foi violada quando o usuário mal-intencionado conseguiu acesso a uma área restrita onde pode conseguir acesso a informações sensíveis.

Falha Lógica:
Foi violado quando o firewall não bloqueou o acesso ao sistema administrativo em uma rede de convidado.

Classificação da Informação:

Prontuário do Paciente:
Confidencial, pois o prontuário possui informações delicadas do paciente contendo dados básicos de cadastros e até mesmo informações de remédios alérgicos.

Senha de Admin:

Alunos: Lucas E. Testoni, Eduardo Zirbell e Guilherme Kunhen

Secreta, pois permite acesso a controle total do sistema, podendo manipular diversas informações de pacientes e prontuários, caso ocorra um vazamento dela o sistema está comprometido.

Remediação e PSI:

Primeiramente, deve ser incluído um acesso com login único e MFA no sistema administrativo. Também pode ser adicionado um sistema de políticas nos computadores do hospital, restringindo o tempo de inatividade na tela. Por último, a criação de uma segregação nas redes do firewall separando os acessos, com o intuito de bloquear qualquer acesso a rede administrativa pela rede de convidados.