UC: Network Security

TP1 Report – Simplified Risk Analysis /Análise de Risco simplificada

Students (Nº / Name):

a83899 - André Morais

a85367 - Francisco Lopes

a83819 - Miguel Oliveira

a84727 - Nelson Faria

a85853 - Pedro Fernandes

a84485 - Tiago Magalhães

Threats / Ameaças	Attacks / Ataques	Vulnerabilities / Vulnerabilidades
Uma sobrecarga no ponto de conexão entre a Internet e a instituição, pode provocar uma falha	Um atacante consegue conectar-se à rede e quebrar o único ponto de ligação com um ataque DoS	Único ponto de conexão entre a Internet e a instituição em si
O administrador de um server malicioso pode manipular a GC (*Global Configuration*), algo que não é notificado para entidades exteriores.	O administrador modifica a configuração de uma lista de pessoas "confiáveis", a GC (*Global Configuration*) é distribuída e aceite, posteriormente, esta é revertida	GC é usada em muitos protocolos, um input confiável. O problema está em confiar no modelo. GC atualiza periodicamente o nível de confiança de todos os seus membros. (*)
Atribuição errada de privilégios no uso de serviços	Aceder a informação restrita ou que não deveria ter acesso	A fuga de informação e a sua exposição a terceiros

Critical resource / Recurso crítico: (justified / justificado)

No nosso ponto de vista, o recurso crítico deste sistema são os médicos de emergência. A disponibilidade deste serviço é de extrema importância num contexto hospitalar, pois 1 ou 2 minutos podem ser cruciais. Deste modo, se houver uma falha de segurança devido a um Dos (como descrito na tabela acima na primeira linha) o serviço de emergência pode não ser capaz de dar resposta à população que necessita deste serviço.

Por outro lado, as bases de dados externas também poderão ser consideradas um recurso crítico, uma vez que caso haja uma falha de segurança que afeta a confidencialidade dos dados, informações confidenciais podem ser acedidas por atacantes.

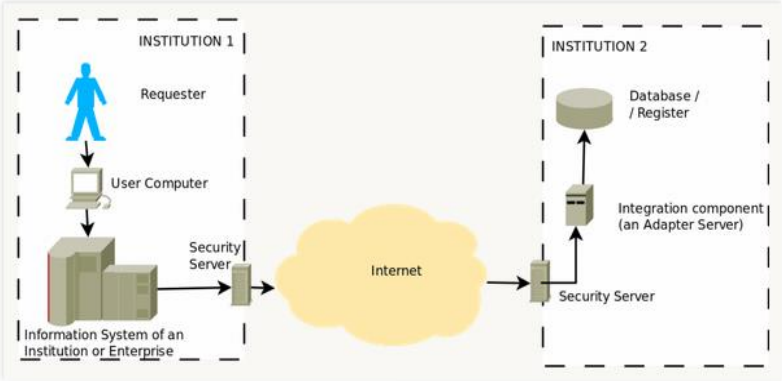
Para concluir, numa organização de saúde, aquilo que é mais importante é a disponibilidade para os utentes deste sistema, para que assim os profissionais de saúde disponham das funcionalidades de maneira mais eficaz possível. Contudo, se a informação que corre na organização de saúde não for confiável, não é possível prestar um serviço credível para a população, o que poderá ter graves implicações tanto a nível político, económico ou social.

Security control / Controlo de segurança: (justified / justificado)

Para ajudar no controlo de segurança, poderíamos fazer backups da base de dados e distribuição do serviço, para assegurar o acesso a informação em caso de falha ou ataques a este mesmo. A existência de alternativas nestes casos pode ser fundamental para que caso exista uma quebra de serviço se poder recorrer a outras fontes de informação. De certa forma, algo de extrema importância numa organização desta dimensão é o controlo de acesso aos utilizadores da organização, pelo que se não existirem mecanismos de deteção de intrusão no sistema, não será possível garantir a sua credibilidade ou segurança.

Existem ainda outros controlos de segurança, como a introdução de firewalls para impedir o acessos indevidos ao sistema, mesmo por equipamentos que pertencem a infraestrutura, mantendo assim o isolamento das várias partes envolvidas na organização. Outro controlo de segurança poderá ser a revisão dos sistemas de antivírus de forma a evitar contaminações nos vários dispositivos que possam aproveitar-se de possíveis vulnerabilidades.

(*)



Implementação de um *Security Server* é da responsabilidade de cada instituição desde que siga determinadas instruções. Logo, pode ser único e não está protegido contra ataques DoS.