INFORMATION SYSTEMS SECURITY ENGINEERING
ENGENHARIA DA SEGURANÇA DE SISTEMAS DE INFORMAÇÃO
SEGURAÇA EM REDES
NETWORK SECURITY
(ESSI/SR) - HOMEWORK TP#1

ANÁLISE DE RISCO SIMPLIFICADA

Henrique Santos

Departamento de Sistemas de Informação
Universidade do Minho

September 2020

Introdução

A Segurança da Informação pode ser definida como o processo conducente ao estabelecimento de um determinado nível de **confiança**, sobre um conjunto de propriedades consideradas relevantes. É quase universalmente aceite que, neste contexto, algumas propriedades são fundamentais, i.e., a **confidencialidade**, a **integridade** e a **disponibilidade**, não obstante outras possam ser igualmente importantes.

Um nível de confiança é traduzido por uma medida bastante subjetiva, dado o carácter pessoal do julgamento necessário, que se traduz na perceção do **risco**. Claramente, diferentes indivíduos considerarão aceitáveis diferentes níveis de risco e, consequentemente, o seu nível de confiança será diferente. Apesar desta evidente dificuldade existem modelos simples que permitem traduzir o nível de risco e que são fundamentais para conseguir planear conscientemente uma infraestrutura de segurança. Um desses modelos (simplificado) baseia-se na determinação do risco como sendo o produto do **valor do sistema em causa pela probabilidade de ocorrência de um evento** danoso:

$$R = V \times P$$

O valor V pode corresponder a um valor material facilmente calculado (e.g., o custo de um determinado equipamento), ou pode corresponder a um valor mais indefinido, como seja o valor de uma marca ou de uma informação (este tópico não será aqui considerado, por se enquadrar mais no âmbito da disciplina de Gestão do Risco).

Por seu lado, a probabilidade P da ocorrência de um evento danoso estará associada à(s) **vulnerabilidade(s)** existente(s) no sistema e que permitirá(ão) essa ocorrência, à(s) **ameaça(s)** pendentes sobre o sistema e que pode(m) desencadear o evento e ao(s) **ataque(s)** que poderá(ão) materializar a ameaça e gerar o evento. Sendo assim, numa perspetiva simplista da questão da segurança num Sistema de Informação, a abordagem segundo este modelo indica que deveremos começar por estudar as vulnerabilidades, as ameaças e os possíveis ataques (não necessariamente por esta ordem). Só depois desse exercício e usando o valor dos recursos em questão, poderemos avaliar o risco e tomar as decisões acertadas quanto à tecnologia e políticas a implementar, para atingir um certo nível de segurança[1].

Objetivos

No final deste trabalho deverá estar apto a:

1. Identificar ameaças, ataques e vulnerabilidades numa (típica) infraestrutura informática que suporta um determinado Sistema de Informação.

[1] Para mais detalhes relativamente a este modelo simplificado, por favor consulte os slides das aulas e a bibliografia associada

2. Explicar a diferença entre ameaça, ataque e vulnerabilidade.
3. Estimar o índice de risco, com base na análise das ameaças, ataques e vulnerabilidades.
4. Identificar alguns controlos básicos para a Segurança da Informação.

Material

Suponha que começou a trabalhar numa organização de saúde, para onde foi contratado como CISO (*Chief Information Security Officer*). Como primeira tarefa é-lhe pedido que realize uma análise de risco/segurança da informação, à **infraestrutura de processamento e comunicações**, com o objetivo de identificar as **vulnerabilidades**, as **ameaças** e os possíveis **ataques**. Numa primeira aproximação é-lhe dito que a infraestrutura tecnológica corresponde a uma arquitetura típica, como aquela que é mostrada na Figura 1, integrada com a tecnologia X-Tee/X-Road e descrita aqui (siga o link)[2].

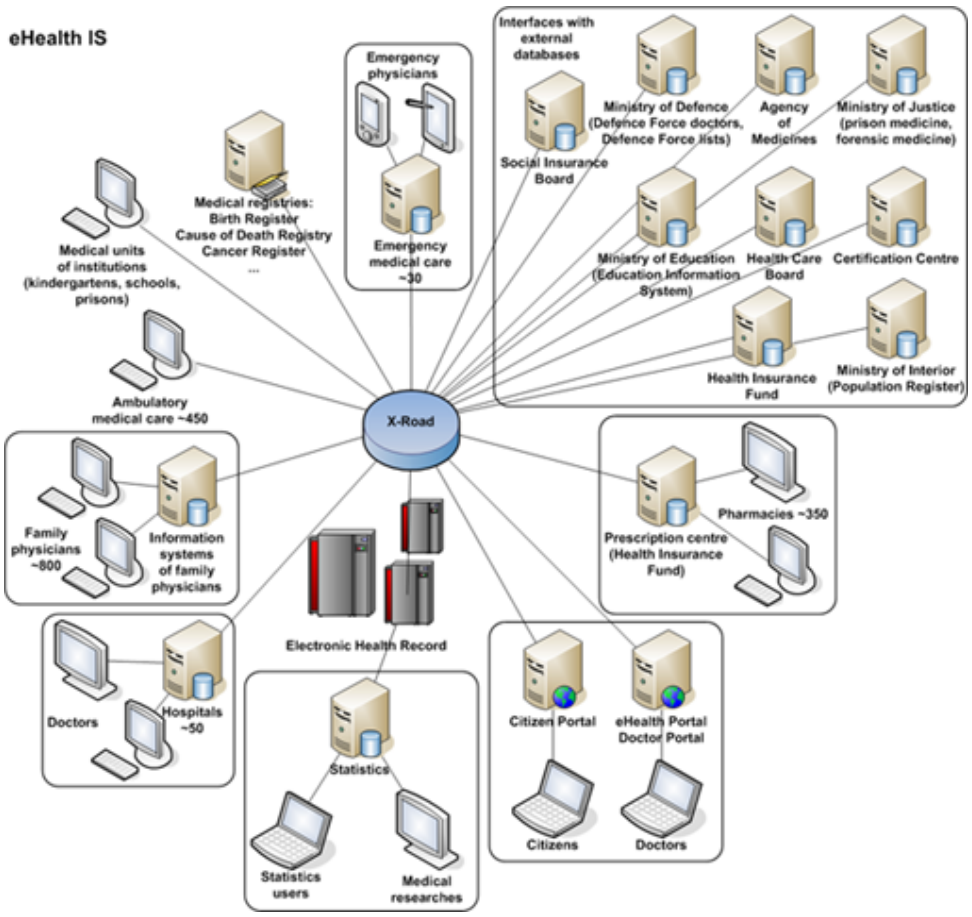

Figura 1: Arquitetura do SI para e-Health, implementado na Estonia, baseada em X-Road (version 4.0, 2006)

[2] A arquitetura aqui apresentada já não corresponde exatamente ao que está disponível no site. No entanto, a descrição geral mantém-se e a arquitetura apresentada desta forma é mais útil para o exercísio em questão.

Na execução do trabalho poderá ainda ser-lhe útil a leitura do capítulo 1 do livro "Security in Computing", do Pfleeger (indicado na bibliografia da UC).

Tarefas

Analisando a Figura 1 e a descrição associada (disponível no link acima indicado), indique, numa tabela:

1. Três ameaças que considera relevantes (que se traduzem em um maior nível de risco).
2. Um ou mais ataques que é capaz de imaginar e que materializam cada uma das ameaças anteriores.
3. As vulnerabilidades que são exploradas em cada um desses ataques.

Indique ainda qual o **recurso** que, segundo a sua opinião, evidencia o maior risco e justifique a sua escolha. Finalmente, identifique um **controlo de segurança** que procure atenuar esse risco.