



Universidade do Minho
Escola de Engenharia

GESTÃO E VIRTUALIZAÇÃO DE REDES
SEGURANÇA EM REDES
NETWORK SECURITY
(SR) - HOMEWORK TP1

ANÁLISE DE RISCO SIMPLIFICADA

GRUPO 2

A85308	Filipe Miguel Teixeira Freitas Guimarães
A79799	Gonçalo Nogueira Costeira
A84912	Joana Isabel Afonso Gomes
A75480	Marco Matias Pereira Gonçalves
A42040	Miriam Miranda Pinto
A57041	Simão Pedro Santa Cruz Oliveira

Braga,
30-10-2020

Conteúdo

1	Introdução e Apresentação do Problema	2
2	Resposta ao problema proposto	2
2.1	Recurso crítico	4
2.2	Controlo de segurança	4
3	Conclusão e Análise de Resultados	4
4	Bibliografia/Webgrafia	5

1 Introdução e Apresentação do Problema

No âmbito da unidade curricular de Segurança de Redes foi proposta a análise da arquitectura de vários sistemas interligados de forma a entenderem quais seriam as suas vulnerabilidades, bem identificar a que tipos de ataques podem ser sujeitos.

A segurança de redes é um tópico cada vez mais em foco nos dias de hoje. Num mundo, onde tudo praticamente necessita de estar "online" existe a necessidade de um conjunto de condutas que devem ser realizadas de forma a minimizar os danos que possíveis ataques possam causar assim como, apostar na prevenção dos mesmos.

Nesse seguimento, foi então estudado um sistema *e-health* implementado, actualmente na Estónia sendo que será feita então uma análise arquitectural bem como o estudo das possíveis vulnerabilidades e riscos de ataque. Posteriormente, será feita então uma análise dos resultados obtidos.

Na figura seguinte está indicada a arquitectura do sistema em estudo.

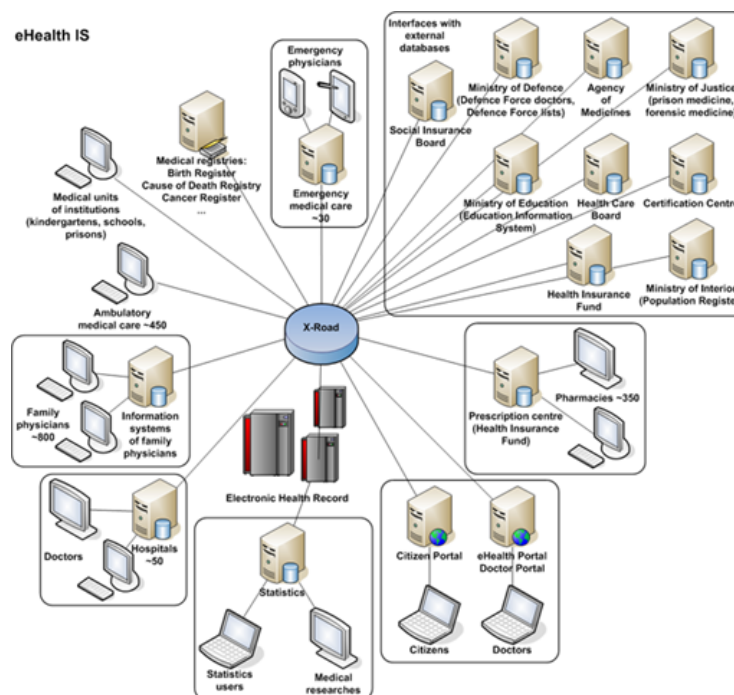

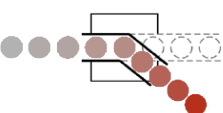
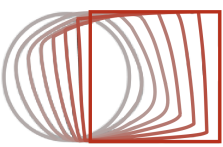


Figura 1: Arquitetura do SI para *e-Health*, implementado na Estónia, baseada em *X-Road* (version 4.0, 2006)

2 Resposta ao problema proposto

Ameaças	Ataques	Vulnerabilidades
<p>Excesso de pedidos ao server</p> <p>Interruption</p>  <p>ataque</p>	<ul style="list-style-type: none"> DoS (<i>Denial of Service</i>) 	<p>Falta de recursos no sistema e/ou uma arquitetura desadequada para sustentar uma sobrecarga de pedidos ou de informação pode dar origem a uma indisponibilidade de serviços aos seus utilizadores (<i>Denial of Service</i>). Outros fatores como a falta de cuidados e algumas má práticas na gestão do sistema são também vulnerabilidades notórias no que toca a este tipo de ataques.</p> <p><i>DoS attacks</i> acontecem geralmente de dois modos:</p> <ul style="list-style-type: none"> - o sistema é forçado a reinicializar ou a consumir todos os recursos (como memória ou processamento), impedindo-o de fornecer o seu serviço, - obstruindo a via de comunicação entre os <i>users</i> e o sistema, não permitindo que comuniquem corretamente.
<p>Espionagem (escuta não autorizada, <i>eardrop-ping</i>)</p> <p>Interception</p> 	<ul style="list-style-type: none"> <i>Man in the middle</i> Ataque mascarado ✗ Phishing <p>descrição de ataques</p>	<p>A existência, por exemplo, de um ponto WiFi não encriptado, pode levar um invasor dentro do seu alcance de receção a facilmente intercetar todas as mensagens, podendo retransmiti-las e possivelmente alterar a comunicação. Um exemplo notório é a escuta não autorizada, em que o atacante faz comunicações independentes com as entidades vítimas e transmite mensagens entre elas, fazendo-as acreditar que estão realmente a comunicar entre si.</p> <p>Evidências?!</p>
<p>Acessos e modificações não autorizadas a dados</p> <p>Modification</p> 	<ul style="list-style-type: none"> SQL Injection <p>idem</p>	<p>Se houver entradas de usuários vulneráveis numa página web (usando as entradas do usuário diretamente na consulta SQL), o invasor pode criar conteúdo de entrada (carga maliciosa). Depois de enviar esse conteúdo, comandos SQL maliciosos são executados no banco de dados, levando ao acesso não autorizado a dados confidenciais (<i>passwords</i>, dados de cartões e outras informações pessoais), acabando eventualmente por comprometer a reputação da instituição.</p>

2.1 Recurso crítico

Após uma análise cuidada da topologia apresentada consideramos que *Medical units of institutions* e *Ambulatory medical care* são os recursos igualmente críticos. Como estes têm um acesso directo ao *X-Road* e que a partir desta *network* conseguem aceder à informação dos outros recursos. Caso estes recursos sejam utilizados por algum *cracker* estes podem levar à perda da confidencialidade do sistema que é um *security goal*. Com estes dados o *cracker* poderá violar os direitos de privacidade e personalidade da comunidade Estoniana utilizando os mesmos para algum fim indevido.

pouco objetivo

Estes recursos podem ser utilizados por um *cracker* através do roubo ou descoberta das credenciais de autenticação dos utilizadores deste recurso. Este roubo pode ocorrer através de *Bruteforce* caso estas tenham um baixo nível de complexidade e *phishing* caso os utilizadores sejam descuidados fornecendo as suas credenciais de autenticação.

2.2 Controlo de segurança

Para impedir que tal vulnerabilidade seja explorada deve-se recorrer a medidas de consciencialização, instruindo os utilizadores a utilizar as plataformas de forma mais segura.

De modo a dificultar a vida do *cracker* deve instruir-se o utilizador a criar palavras-passes seguras e que as troquem periodicamente, ter cuidado com websites ou aplicação duvidosas, desconfiar sempre de emails que peçam algum tipo de autenticação.

falta de coerência

Estas formas de agir parecem básicas mas a maioria da população necessita de ser consciencializada visto que uma grande parte dos utilizadores caem neste tipo de *traps* criadas para lhes poderem aceder ao dados e quando o conseguem fazer, não conseguimos saber qual a finalidade que lhes dão.

3 Conclusão e Análise de Resultados

Depois de abordadas as temáticas apresentadas ao nível das teóricas foi possível de uma melhor forma estruturar a forma como foram abordados os temas propostos nas tarefas a sua respectiva resolução.

Durante o desenvolvimento deste projecto foi realizada uma avaliação do caso de estudo, dividida em várias etapas separadas entre a análise, pesquisa e síntese onde foi constatada a já "clássica" dificuldade de promover a segurança num sistema informático. Cada sistema possui a sua respectiva funcionalidade e complexidade, por exemplo, conforme o aumento de dispositivos, aplicações e serviços disponibilizados na rede.

Devido ao facto de o avanço tecnológico ser uma constante nos dias de hoje, é crucial que exista de modo continuado uma monitorização deste sistema *e-health*, bem como uma actualização das ferramentas constante de forma a minimizar, mas sobretudo prevenir ao nível da segurança. É sem dúvida necessário por parte de uma equipa de segurança uma constante análise de todos os equipamentos que constituem a empresa em questão, pois estes evoluem constantemente, bem como as vulnerabilidades e explorações encontradas. Isto é, quanto mais educados estiverem estes especialistas nos mais recentes e eficientes métodos de ataque, estarão melhor prevenidos a encontrar estas ameaças, já que complementemente preparados nunca estamos...

Ao longo da pesquisa realizada foram adquiridos conhecimentos sobre a importância da segurança informática, sobre ataques informáticos, como reconhecer ameaças e vulnerabilidades, e desta forma foi possível construir uma base teórica introdutória que será essencial no avanço académico e de forma a que possamos dar início a uma eventual actividade como profissionais de segurança.

4 Bibliografia/Webgrafia

<https://portswigger.net/web-security>

<https://us-cert.cisa.gov/ncas/tips>

<https://www.imperva.com/learn/application-security>