Universidade do Minho

Trabalho Prático

Análise de Risco Simplificada

Mestrado Integrado em Engenharia Informática

Segurança em Redes

(1º Semestre - 2018/2019)

a70565 Bruno Arieira

a73974 Daniel Vieira

a73883 Cesário Perneta

a78494 José Dias

13 de Outubro de 2018

Resumo

"A Segurança de 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 a outras possam ser igualmente importantes."
Este trabalho, realizado no âmbito da unidade curricular Segurança em Redes, tem como fundamento diferenciar e/ou identificar as diversas **vulnerabilidades**, **ataques** e **ameaças**, baseadas numa Infraestrutura Crítica, bem como avaliar o risco de um determinado recurso.

Conteúdo

1 Introdução

Neste primeiro trabalho prático, com o tema de Análise de Risco Simplificada, pretende-se identificar, de forma clara, vulnerabilidades, ameaças e ataques, numa determinada rede de computadores e consequentemente cimentar estes três conceitos. Tem também como objetivo estimar o risco alusivo bem como mencionar controlos de segurança que o procurem atenuar.

Para tal, foi nos proposto para nos colocarmos no cargo de um *Chief of Security Officer* de uma determinada Infraestrutura Crítica, que tem como principal tarefa a análise de segurança de informação existente na infraestrutura, com objetivo de especificar possíveis vulnerabilidades, ataques e ameaças que se traduzem num maior risco.

Para o desenvolvimento deste trabalho, decidimos que todos os elementos deveriam participar na identificação de vulnerabilidades, ameaças e ataques, pois é um dos pontos fulcrais deste projeto, os quais são conceitos que devemos dominar principalmente nesta unidade curricular. Depois do estudo da infraestrutura em causa e de alguns termos imprescindíveis á realização deste trabalho , procedemos a uma discussão relativamente ás tarefas que nos foram propostas.

2 Contextualização

Antes de mais,há que diferenciar e bem os vários conceitos que temos pela frente.Para a realização deste trabalho temos que saber a diferença entre vulnerabilidade,ameaça e ataque.

2.1 Vulnerabilidade

> "Vulnerability is a cyber-security term that refers to a flaw in a system that can leave it open to attack. A vulnerability may also refer to any type of weakness in a computer system itself, in a set of procedures, or in anything that leaves information security exposed to a threat."[2]

Podendo ser chamado também como falha ou fraqueza num sistema informático que pode ser explorada para eventualmente causar dano. Esta é uma caraterística do que estamos a investigar sendo que quanto menor o numero de vulnerabilidades que existirem melhor

2.2 Ameaça

> "A threat, in the context of computer security, refers to anything that has the potential to cause serious harm to a computer system. A threat is something that may or may not happen, but has the potential to cause serious damage."[3]

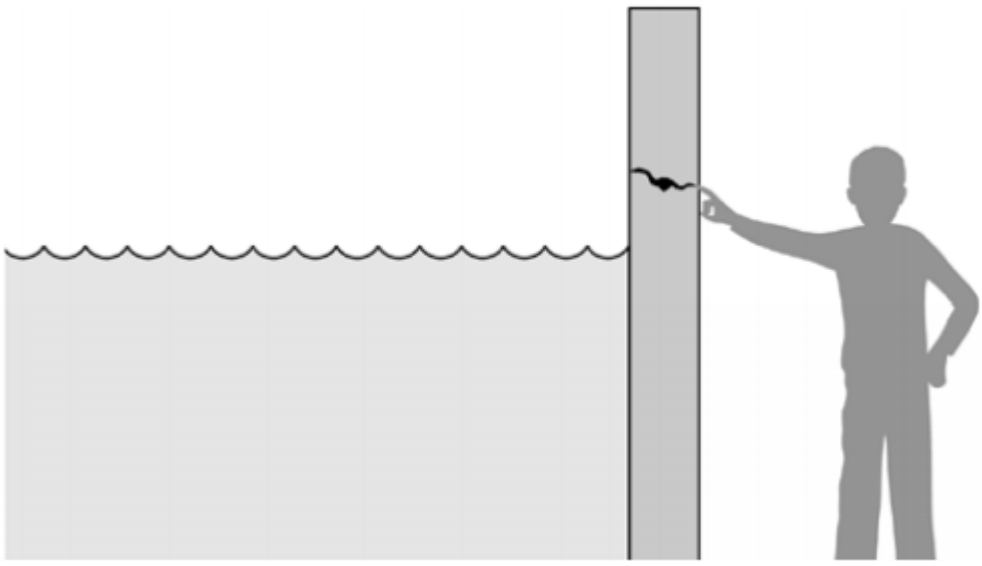
É a possibilidade de pessoas terceiras explorarem uma fraqueza ou qualquer coisa que possa causar danos ao sistema que estão a explorar. Também pode ser uma ameaça algo que não cause dano ao sistema diretamente mas que sirva para terceiros atingirem os seus próprios objetivos.

2.3 Ataque

> "An attack is an information security threat that involves an attempt to obtain, alter, destroy, remove, implant or reveal information without authorized access or permission. It happens to both individuals and organizations."[4]

É o ato que pode levar a destruir, obter informação. Informação confidencial que só está disponível para certas pessoas com um grau de hierárquico elevado na empresa.Também acontece com particulares.

2.4 Exemplo



[1]

Podemos ver na figura que entre um homem e uma quantidade elevada de água, se situa uma parede. Esta parede é o que impede o homem de morrer afogado, no entanto, a parede que protege o homem contém um brecha que se poderá vir a agravar, ou seja, é uma vulnerabilidade. O homem está a correr o perigo de afogar, sendo isto uma ameaça. Podemos então "usar"a vulnerabilidade para poder atacar o homem. Logo, usamos a

vulnerabilidade,isto é,aprofundamos ainda mais a brecha que contém na parede para esta cair e assim a água poder passar para o outro lado, acabando por atacar o homem. Através deste exemplo, que nada tem a ver com redes e segurança, explicamos a diferença destas palavras-chave, de modo a podermos explicar todo o nosso raciocínio no próximo capítulo.

3 Tarefas

3.1 Exercício 1: Vulnerabilidades, Ameaças e Ataques

Considerando que os *OT Systems* correm em *legacy software* que não possui qualquer autenticação por parte do utilizador e do sistema, nem recursos de verificação da integridade dos dados, logo existe aqui uma vulnerabilidade. Uma ameaça que aqui surge é a possibilidade do acesso descontrolado de atacantes ao sistema. Consequentemente pode ser efetuado um ataque onde ocorre o levantamento do "ambiente" por parte do invasor, para posteriormente empregar diferentes táticas para se conectar na rede destino, dando início a um *malware*.

Uma possível vulnerabilidade surge no caso de uma falha de segurança nas instalações ou através do excesso de confiança num funcionário. Como tal, a ameaça referente, poderá ser a perda de dados importantes no caso de um atacante injetar algum dispositivo que irá danificar o hardware.

Nesta rede podemos ver uma vulnerabilidade evidente, existe uma VPN externa que não passa pela *firewall*. Apenas a sua existência ameaça a rede pois pode ser enviado um vírus. Caso isto aconteça e um atacante tire partido então a rede poderá ficar comprometida.

Como mencionámos a inexistência de uma *firewall* para a VPN é uma vulnerabilidade, mas não é apenas aí onde a inexistência das mesmas é uma vulnerabilidade. Na rede interna também não existem *firewalls* entre dispositivos. Esta situação leva a que no caso de que um dispositivo seja infetado então todos os outros dispositivos da rede poderão seguir o mesmo caminho o que é uma ameaça séria á rede. Caso isto seja explorado então a empresa poderá perder dados importantes ou mesmo esses dados serem roubados e vendidos para competidores.

3.2 Exercício 2: Recurso Crítico

Entendemos que o recurso critico sejam as *Control Room Workstations*. Este tipo de recurso é responsável por definir e controlar pontos de acesso, tal como gerir o estado dos servidores. Como tal, é possível que algum *malware* se consiga estabelecer através de algum ponto de acesso definido para alguma máquina, podendo comprometer o bom funcionamento dos sensores e atuadores, assim como o sistema de segurança.

3.3 Exercício 3

Relativamente aos controlos de segurança que procure atenuar tal risco, a primeira medida a implementar, deveria ser uma política de controlo de tráfego, limitando o acesso aos *Wireless Access Points* apenas a computadores da empresa, reduzindo assim o risco de infeção do sistema.

Deveria-se ainda encriptar todos os ficheiros, tornando-os seguros e menos suscetíveis a possíveis roubos/alterações e criar um inventário/backup de todos os ficheiros da empresa.

4 Conclusão

Uma vez finalizado, cabe-nos fazer uma retrospetiva de todo o trabalho feito. Antes de efetuarmos o trabalho, tivemos alguma dificuldade em diferenciar ameaça e ataque no nosso dia-a-dia, porque sempre nos pareceu que pudessem ser sinónimos. Através da pesquisa para a realização deste trabalho e a devida realização do mesmo, podemos afirmar que temos conhecimento da sua distinção, o que se torna uma mais valia, em termos profissionais, relativamente a Segurança em Redes. Em relação ao outro critério a analisar, vulnerabilidades, já tínhamos conhecimento prévio, da aula prática em que nos foi proposto este trabalho. Outro contratempo que enfrentamos foi perceber como a rede funcionava para descobrirmos as vulnerabilidade que nela existiam, sendo que é um pouco complexo a arquitetura da infraestrutura em estudo.

Sendo que a nossa primeira entrega do trabalho prático, foi um documento onde apenas respondemos ás tarefas propostas no enunciado, reformulámos o nosso relatório, sendo que dividimos as devidas partes uniformemente por os quatros elementos que integram o grupo. Para respondermos ao enunciado, todos opinamos e discutimos entre nós, tal como já foi referido anteriormente.

Para concluir, podemos afirmar que foi um trabalho prático bastante vantajoso para nós, no sentido de expandir o nosso conhecimento nesta área, em especial ênfase á análise de segurança da informação da infraestrutura em causa. Consideramos que o trabalho está bem conseguido, apesar dos problemas iniciais (a não apresentação de um relatório sucinto).

Referências

[1] Shari L. Pfleeger, Charles P. *Security in Computing*. Prentice Hall PTR, 2007.

[2] Techopedia. https://www.techopedia.com/definition/13484/vulnerability.

[3] Techopedia. https://www.techopedia.com/definition/25263/threat.

[4] Techopedia. https://www.techopedia.com/definition/6060/attack.