Universidade do Minho
Escola de Engenharia

Mestrado em Engenharia de Telecomunicações e Informática

Unidade Curricular de Cibersegurança

Docente: Henrique Santos

TP1: Análise de Risco Simplificada

Bárbara Fonseca PG53677

Camila Pinto PG53712

Eduarda Dinis PG53793

Gonçalo Dias PG53833

Guimarães, fevereiro de 2024

Índice de conteúdos

Lista de tabelas

Lista de acrónimos e siglas

HMI	Human Machine Interface
IC	Critical Infrastructure
IED	Intelligent Electronic Device
LAN	Local Area Network
PLC	Programmable Logic Controller
RTU	Remote Terminal Unit
SCADA	Supervisory Control and Data Acquisition

1. Introdução

O presente relatório está a ser desenvolvido no âmbito da Unidade Curricular de Cibersegurança do 2º semestre do 1ºano do curso de Mestrado em Engenharia Telecomunicações e Informática.

Neste primeiro trabalho prático, com o tema Análise de Risco Simplificada, pretende-se identificar, de forma clara, vulnerabilidades, ameaças e ataques, de forma a 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 proposto colocarmo-nos no cargo de um *Chief of Security Officer* de uma determinada Infraestrutura Crítica (IC – *Critical Infrastructure*), composta por componentes convencionais de Sistemas de Informação (*Corporate LAN)*, tecnologia SCADA (*Supervisory Control and Data Acquisition*) para controlo de sistemas industriais e componentes distribuídos junto a equipamentos específicos (*Field Devices*, como RTU (*Remote Terminal Unit*) , IED (*Intelligent Electronic Device*) , PLC *(Programmable Logic Controller*), de modo a realizar uma avaliação da análise de segurança da rede. Este exercício visa garantir a integridade, confidencialidade e disponibilidade dos recursos críticos, e promover uma abordagem proativa na gestão da cibersegurança.

2. Conceitos

2.1 Ameaça

A ameaça em sistemas de segurança é definida como a possibilidade de ocorrer um incidente indesejado que pode causar danos a uma organização ou aos sistemas que ela utiliza. Estas ameaças podem ser acidentais ou intencionais (com intenção maliciosa) e são caracterizadas por elementos ameaçadores, alvos potenciais e métodos de ataque [1].

2.2 Ataque

Qualquer tipo de atividade maliciosa que tenta recolher, perturbar, negar, degradar ou destruir recursos de um sistema de informação ou a informação em si [2].

2.3 Vulnerabilidade

A vulnerabilidade pode ser descrita como uma insuficiência, independente da natureza, que pode ser explorada por uma ou mais ameaças. A vulnerabilidade pode consistir numa omissão ou estar relacionada com uma insuficiência dos controlos no que se refere ao rigor, coerência ou exaustividade destes últimos, podendo ser de natureza técnica, processual, material, organizativa ou operacional [3]. Pode também ser definida como a fraqueza de um sistema informático, revelada por um exame à sua segurança (por exemplo, devido a falhas na análise, conceção, implementação ou operação), que se traduz numa incapacidade de fazer frente às ameaças informáticas que pesam sobre ele [4].

2.4 Risco

O risco é caracterizado pela possibilidade de uma ameaça específica explorar as vulnerabilidades internas e externas de uma organização ou de um dos sistemas por ela utilizados, causando assim danos à organização e respetivos ativos corpóreos ou incorpóreos. Mede-se pela combinação entre a probabilidade de as ameaças ocorrerem e o respetivo impacto [5]. Além disso, pode ser também uma circunstância ou um evento, razoavelmente identificáveis, com um efeito adverso potencial na segurança das redes e dos sistemas de informação [6].

3. Tarefas

Tabela 1. Tabela de ameaças, ataques, vulnerabilidades e valor do risco.

Threats / Ameaças	Attacks / Ataques	Vulnerabilities / Vulnerabilidades	Valor do Risco / Risk Value
Inacessibilidade no acesso a serviços, por exemplo, e-mails e website da empresa. (Disponibilidade)	Ataque de DoS, injetando uma enorme quantidade de dados a uma velocidade que a rede não consegue processar, resultando na sobrecarga da rede e bloqueio dos serviços.	Falta de autenticação [7], fracas medidas de segurança nos Web Servers e Email Servers.	Visto que existem organizações especializadas em cibercrime, existe conhecimento e ferramentas, portanto têm método; além disso, devido à falta de autenticação têm condições de acesso(disponibilidade). O risco é **Médio**.
Espionagem industrial; Roubo de dados confidenciais, que podem ser vendidos a outras empresas. (Confidencialidade e Integridade)	Ataque de *sniffing* no qual o invasor acede ao access point e monitoriza o tráfego de rede para capturar informações sensíveis.	A existência de um *access point*, conectado diretamente às redes internas (Control System LAN e Corporate LAN).	De igual forma, existe método e condições de acesso, devido à ligação direta do *access point* com as redes (disponibilidade). O risco é **Alto**.
Acesso indevido por trabalhadores não autorizados; Roubo de credenciais; Acesso ao controlo dos sistemas, máquinas e processos indústrias. (Confidencialidade e Integridade)	Ataque à HMI permitindo o acesso à interface gráfica usada para controlar os sistemas e ataque ao RTU, ficando sob controlo das máquinas e processos industriais da empresa.	A ligação direta das workstations e HMI (interface gráfica por meio da qual é possível interagir com sistemas de controlo industrial) ao RTU (monitoriza processos físicos remotamente) /PLC (controla máquinas e processos industriais).	De igual forma, existe método e condições de acesso, mas o risco é **Baixo.**

3.1 Critical resource / Recurso crítico: (justified / justificado)

O recurso crítico na segurança da infraestrutura da rede corporativa apresentada, é a ligação direta do ponto de acesso às redes *Corporate LAN* e *Control System LAN*. Este recurso é responsável por permitir que os dispositivos se conectem à rede e monitorizem a mesma. Como tal, ao conseguir aceder a este ponto de acesso, é possível infiltrar-se nas redes, ganhando controlo sobre as mesmas e comprometendo o sistema de segurança, dados confidenciais e o estado dos servidores.

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

Os mecanismos de controlo de segurança a implementar incluem:

- Implementar uma autenticação de dois fatores para reforçar a verificação de identidade.
- Encriptar os dados sensíveis, como ficheiros etc, bem como fazer *backup* dos mesmos.
- Implementar uma política de tráfego da rede, limitando o acesso ao W*ireless access point.*
- Implementar uma *firewall* para restringir o tráfego e criar uma barreira de acesso às redes.

4. Conclusões

Fazendo uma retrospetiva e análise do trabalho realizado, percebemos que tivemos alguma dificuldade em distinguir ameaça e ataque, após uma pesquisa sobre o assunto para nos preparar para a realização do trabalho e o esclarecimento de dúvidas com o docente, podemos afirmar que obtivemos a informação necessária para distinguir estes dois conceitos. Outro contratempo que enfrentamos foi perceber como a rede funcionava para expor as vulnerabilidades da mesma e definir o recurso mais crítico.

A realização do trabalho prático, foi executada em colaboração com os membros do grupo, cada um contribuindo com a sua opinião crítica durante as reuniões realizadas, o que nos permitiu alcançar um consenso.

Em suma, afirmamos que este trabalho prático provou ser vantajoso para nós, na medida em que expandiu o nosso conhecimento nesta área, incidindo mais na análise de segurança de informação na infraestrutura em causa. Desta forma, considerámos que atingimos os objetivos propostos e adquirimos o conhecimento pretendido para sermos capazes de realizar a análise de segurança de uma rede.

Referências

[1] Glossary of Key Information Security Terms, eds. Richard Kissel, National Institute for Standards and Technology, US Deparment of Commerce, NISTIR 7298, Revision 2 – 2001, citado em NATO CCDCOE.

[2] Decisão do Conselho n.º 2013/488/EU, de 23 de setembro de 2013, relativa às regras de segurança aplicáveis à proteção das informações classificadas da UE e Decisão (UE, Euratom) n.º 2015/444 da Comissão, de 13 de março de 2015, relativa às regras de segurança aplicáveis à proteção das informações classificadas da UE.

[3] Decisão do Conselho n.º 2013/488/EU, de 23 de setembro de 2013, relativa às regras de segurança aplicáveis à proteção das informações classificadas da UE.

[4] Decisão (UE, Euratom) n.º 2015/444 da Comissão, de 13 de março de 2015, relativa às regras de segurança aplicáveis à proteção das informações classificadas da EU;

[5] Associação para a Promoção e Desenvolvimento da Sociedade de Informação.Decisão do Conselho n.º 2013/488/EU, de 23 de setembro de 2013, relativa às regras de segurança aplicáveis à proteção das informações classificadas da UE.

[6] Diretiva (UE) n.º 2016/1148 do Parlamento Europeu e do Conselho, de 6 de julho de 2016, relativa a medidas destinadas a garantir um elevado nível comum de segurança das redes e da informação em toda a União.

[7] "Critical Infrastructure Security by Subodh Belgi," SlideShare. [Online]. Available: https://pt.slideshare.net/clubhack/critical-infrastructuresecuritysubodh-belgi. [Accessed: 14-Feb-2024].