UC: Cibersegurança

Relatório TP1– Análise de Risco simplificada

Estudantes (Nº /Nome):

- ✓ A84913 - Inês Barreira Marques
- ✓ A85497 - José Carlos Peixoto Ferreira
- ✓ A84481 - Marcos Alexandre Ferreira Martins
- ✓ PG47639 - Rui Filipe Ribeiro Freitas
- ✓ PG47692 - Tiago João Pereira Ferreira

1.1- Vulnerabilidade

É o que se refere a uma falha ou um conjunto de fraquezas de um sistema que pode ser explorada de forma a causar eventual dano no sistema. Esta característica deixa os sistemas abertos a ataques. Quantas menos vulnerabilidades um sistema tiver, melhor.

1.2- Ameaça

É a possibilidade de pessoas estranhas ao sistema, explorarem as vulnerabilidades do mesmo, podendo causar-lhes danos. Uma ameaça pode não causar dano diretamente ao sistema, no entanto, é uma forma de atingir outros objetivos que tenham.

1.3- Ataque

É uma ação que pode levar à obtenção, alteração e destruição de informação sem que se tenha acesso ou permissão. Os ataques podem acontecer a nível de empresas como ao nível de um utilizador individual.

Ameaças	Ataques	Vulnerabilidades	Risco
DISPONIBILIDADE Destruição, Dano e Contaminação no *"Management Centre"*	- Inserção de *malware* (Trojan) por um utilizador da empresa de forma a destruir dados o que faz com que outros serviços importantes da cidade não funcionem direito.	*Personal*- Contratação de trabalhadores sem a devida investigação do passado.	Médio/Alto
DISPONIBILIDADE Recusa ou atraso de acesso nos servidores do *"Cloud application, computing and data centre (PaaS, SaaS, IaaS)"*	-DDOS/DOS que consiste em um atacante enviar diversos pedidos para os servidores, de forma que estes sobrecarreguem e não consigam responder a mais pedidos.	*Software*- Código não preparado para estes ataques ou desatualizado *Hardware*- Servers antigos que não possuem a capacidade suficiente para aguentar um aumento de pedidos	Médio
CONFIDENCIALIDADE - Cópia Ilícita, observação, monitorização ou interferência de dados dos cidadãos	- Um cidadão com acesso aos computadores do serviço público "*Taxes and fees payment"* consegue aceder às declarações IRS e dívidas de todos os cidadãos registados.	*Software* - Falta de uma firewall entre o IoT Information Centre e o Management Centre	Alto
CONFIDENCIALIDADE - Transferência indesejada de controle ou custódia de certos setores fulcrais da cidade	- "*Social Engineering"* que permite persuadir a segurança do Management Center de forma a revelar informações críticas, as quais permitem a transferência de controlo como por exemplo IoT que possui acesso a diversas partes cruciais da cidade.	*Personal*- Pessoas que expõem demasiados aspetos da sua vida que não têm noção de segurança no local de trabalho.	Médio/Alto

INTEGRIDADE **- Alteração da representação de dados em serviços criticos, tal como os serviços médicos**	- Um ex-trabalhador, acede a uma sessão de um computador através de uma backdoor deixada quando trabalhava nos serviços ou no Management Centre.	*Personal* – Má gestão no controlo de software e empregabilidade de funcionários. *Software* – Uso de Bilbliotecas ou software de fontes não verificadas.	Médio
INTEGRIDADE **Inserção ou produção de dados**	- Este tipo de ataque consiste na criação ou alteração de dados ou documentos não genuínos. Um exemplo deste tipo de ataque seria o acesso não permitido aos serviços médicos da cidade, através de um email mal-intencionado ou ataque à base de dados. Com isto, o atacante poderia aceder a registos médicos das pessoas para proveito próprio.	*Software/Personal* – Software com falhas de segurança ou trabalhadores sem o conhecimento básico de cibersegurança	Médio

Recurso crítico: (justificado)

O recurso crítico que consideramos o mais importante são os funcionários da smart city, pois são eles que controlam e que possuem acesso aos vários ficheiros e informações dos cidadãos, bem como o conhecimento dos pontos críticos da cidade. O funcionário pode recolher as informações, e usá-las de forma indevida, sendo quase impossível ter controlo sobre este acontecimento. Outra situação, seria o trabalhador ser alvo de um ataque, onde o atacante consegue manipular informação que passa nos pontos críticos da cidade.

Controlo de segurança: (justificado)

Um processo para controlo de segurança, seria por exemplo investigar melhor o funcionário a contratar, de forma a aferir se este possui algum tipo de vulnerabilidade que potencie uma ameaça ou até mesmo um ataque aos serviços em que o mesmo iria trabalhar. De certa forma, avaliar a viabilidade do funcionário para a função que vai exercer e de que forma o mesmo pode pôr em causa a segurança dos serviços.