

UC: Network Security

TP1 Report – Simplified Risk Analysis /Análise de Risco simplificada

Students (Nº / Name):

- 72362 – Miguel Costa
- 74413 – Gonçalo Pereira
- 75280 – José Silva
- 76234 – Matias Araújo

Threats / Ameaças	Attacks / Ataques	Vulnerabilities / Vulnerabilidades
Falha do serviço dos servidores por infeção (ameaça de maior risco)	Computador ligado à rede estar infetado e espalhar um malware	Wireless access points ligados diretamente à rede LAN da empresa
Alteração indesejada da base de dados da empresa	SQL Injection	Usar input não validado para gerar queries SQL
Acesso facilitado ao router, que por sua vez leva a que todo o sistema esteja comprometido	Modificação da tabela de routing Roubo de emails Hijacking dos web servers	Inexistência de firewall no acesso por VPN

Critical resource / Recurso crítico: (justified / justificado)

→ Os recursos criticos que identificamos neste caso são os PLC (programmable logic controller), pois no caso de um malware conseguir de alguma forma chegar aos PLC e alterar a sua lógica, podem então estar comprometidos os sensores e actuadores desse sistema.

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

→ Limitar o acesso aos Wireless Access Points apenas a computadores da empresa, reduzindo assim o risco de infeção do sistema. Como apenas com isto não se pode evitar tudo, como por exemplo a infeção por removable media; outra solução seria encriptar todos os ficheiros e criar um inventário de todos os ficheiros aprovados pela empresa.