



Projeto n.º 47210

A2 - Requisitos e Especificações Técnicas

E2.4 – Requisitos e especificações técnicas para o módulo de cibersegurança

Autor	Francisco Falcão [Armis], Bruno Pinho [Armis], José Querido [Armis], Ana Cristina Aleixo [Efacec], Nuno Rodrigues [Efacec]
Nível de Divulgação	Confidencial
Data	2022-05-26
Revisão	1.0
Páginas	31
Palavras-Chave (<i>keywords</i>)	

Resumo do Projeto

O projeto SCALE perspetiva o desenvolvimento de uma plataforma para subestação de distribuição digital, que permita o controlo, monitorização e proteção de redes energéticas de média tensão de forma centralizada. Esta solução, projetando e desenvolvendo sistemas de proteção centralizados para subestações, desafia, não só, as arquiteturas de subestação digital atuais, baseadas em comunicações óticas, mas também outras temáticas basilares, como as infraestruturas e soluções cloud-based, big data e data privacy. A solução a desenvolver consistirá, assim, numa arquitetura inovadora e de alto valor acrescentado face aos atuais sistemas disponibilizados.

Projeto SCALE é financiado por



UNIÃO EUROPEIA
Fundo Europeu
de Desenvolvimento Regional

Documento

Projeto	SCALE	
Nome do Projeto	<i>Scalable Centralized Grid Protection, Automation and Control</i>	
Número do Projeto	47210	
Título do Documento	Requisitos e especificações técnicas para o módulo de cibersegurança	
Revisão e Data	1.0	2022-05-26
Editor	Bruno Pinho [Armis]	
Revisor	Francisco Falcão [Armis], Bruno Pinho [Armis], José Querido [Armis], Ana Cristina Aleixo [Efacec], Nuno Rodrigues [Efacec]	
Autores	Francisco Falcão [Armis], Bruno Pinho [Armis], José Querido [Armis], Ana Cristina Aleixo [Efacec], Nuno Rodrigues [Efacec]	
Páginas	31	

Copyright © Promotores do Projeto SCALE.

Todos os direitos reservados.

Este documento contém informações proprietárias dos Promotores do Projeto SCALE, legalmente protegidas por direitos do autor e de propriedade industrial e, como tal, este documento não pode ser copiado, fotocopiado, reproduzido, traduzido ou convertido para o formato eletrônico, na íntegra ou em parte, sem a autorização prévia por escrito dos proprietários. Nada neste documento deve ser interpretado como concessão de licença para fazer uso de qualquer software, informação ou produtos mencionados no documento.

Revisões

Rev.	Data	Comentários	Autor
1.0	2022-05-26	Lançamento do documento.	Francisco Falcão [Armis], Bruno Pinho [Armis], José Querido [Armis], Ana Cristina Aleixo [Efacec], Nuno Rodrigues [Efacec]

Sumário Executivo

O presente documento pretende apresentar um conjunto de soluções a problemas da área de cibersegurança, a implementar durante o desenvolvimento do projeto SCALE. Durante a fase de planeamento do projeto foram delineados requisitos e processos chave para a implementação da CPC. Neste documento é descrita a análise feita aos requisitos identificados, com o intuito de apoiar o desenvolvimento dos componentes de segurança do sistema.

Depois da análise é recomendada a implementação de *firewalls* para filtragem de dados em trânsito e segmentação dos componentes da rede. Será implementado também um servidor LDAP que servirá para autenticação dos utilizadores do sistema, assim como um servidor *syslog* que será utilizado como repositório central de *logs*. As comunicações serão encriptadas com chaves públicas, para garantir a confidencialidade das mensagens face a ataques. É também recomendada a implementação de um sistema de deteção de intrusões, ou *Intrusion Detection System (IDS)*. Adicionalmente, será implementado um sistema de *White-listing*, para evitar a execução de aplicações não aprovadas.

Em suma, garantir a segurança das infraestruturas críticas relacionadas com os equipamentos inteligentes e subestações contra os riscos e vulnerabilidades inerentes é de máxima prioridade. *Hardening* dos equipamentos e a adoção de técnicas de defesa em profundidade são exemplos de mecanismos de mitigação de danos ao sistema e aos dados em circulação.

Índice

1.	INTRODUÇÃO	10
2.	ANÁLISE DE SEGURANÇA	11
2.1	RISCOS	11
2.2	MODELO CIA	12
2.3	VETORES DE ATAQUE	12
3.	SOLUÇÕES DE SEGURANÇA	14
3.1	INFRAESTRUTURA CRÍTICA	14
3.2	DEFESA EM PROFUNDIDADE	14
3.2.1	ARQUITETURA.....	14
3.2.2	SEGMENTAÇÃO DE REDE.....	14
3.2.3	<i>FIREWALL</i>	15
3.2.4	PROTOCOLOS SEGUROS	16
3.2.5	<i>HARDENING</i> DOS DISPOSITIVOS	16
3.2.6	GESTÃO DE CONTROLO DE ACESSO	16
3.2.7	MONITORIZAÇÃO DO TRÁFEGO	17
3.2.8	<i>WHITE-LISTING</i>	17
3.2.9	<i>BACKUP</i>	17
3.3	AUTENTICAÇÃO	18
3.3.1	RADIUS	18
3.3.2	TACACS+.....	18
3.3.3	LDAP	19
3.4	SIEM	19
3.5	CONTROLO E MONITORIZAÇÃO DE TRÁFEGO.....	20
3.5.1	<i>FIREWALL</i>	20
3.5.2	IDS/IPS	20
3.6	CHAVES DE SEGURANÇA E GESTÃO DE CHAVES	20
3.6.1	REQUISITOS PARA PRIVATE KEY INFRASTRUCTURE (PKI)	21
3.7	ENCRIPTAÇÃO	22
4.	APLICABILIDADE NO PROJETO	22
4.1	<i>FIREWALL</i>	22
4.2	SERVIDOR LDAP.....	23
4.2.1	APLICAÇÃO NO PROJETO.....	25
4.3	SERVIDOR SYSLOG.....	25
4.3.1	PRI	26
4.3.2	<i>HEADER</i>	28
4.3.3	MSG (MENSAGEM)	28
4.3.4	APLICAÇÃO NO PROJETO.....	28
4.4	AUTENTICAÇÃO SSH	28

4.5	<i>PUBLIC KEY INFRASTRUCTURE</i>	29
4.5.1	CRITOGRAFIA DE UMA CHAVE PUBLICA.....	29
4.5.2	CERTIFICADOS DIGITAIS.....	30
4.5.3	APLICAÇÃO NO PROJETO.....	30
4.6	IDS (<i>INTRUSION DETECTION SYSTEM</i>).....	30
4.7	<i>WHITE-LISTING</i> DAS APLICAÇÕES	31
4.7.1	<i>WHITE-LISTING</i> EM LAN	31
4.7.2	<i>WHITE-LISTING</i> EM FIREWALLS.....	31
4.7.3	<i>WHITE-LISTING</i> EM APLICAÇÕES	31
5.	CONCLUSÕES	31