Segurança Cibernética no Setor Elétrico
Panorama e Sugestões

Rodrigo Jardim Riella – Pesquisar Sênior

Lactec
62 anos

unindo o protagonismo das
pessoas e da tecnologia

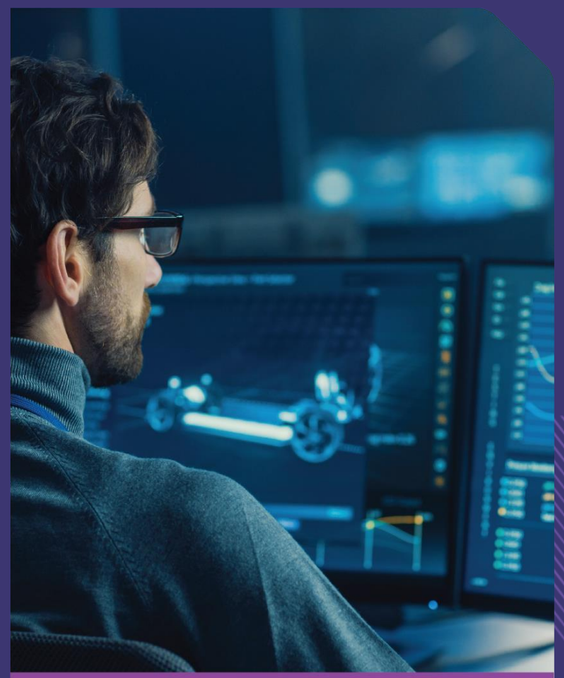
ÁREAS DE NEGÓCIOS

+600 colaboradores

05 unidades em Curitiba
01 unidade em Salvador

+400
Projetos P&D

PESQUISA,
DESENVOLVIMENTO E
INOVAÇÃO

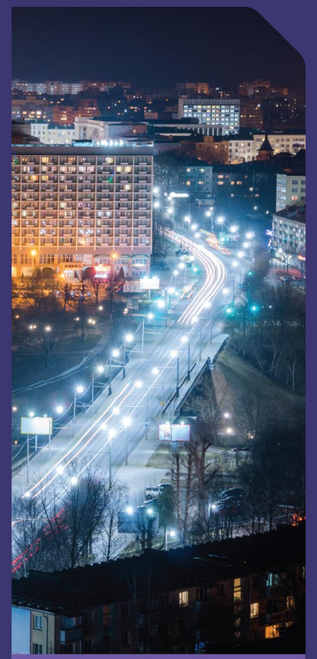


SERVIÇOS
TECNOLÓGICOS E INOVAÇÃO

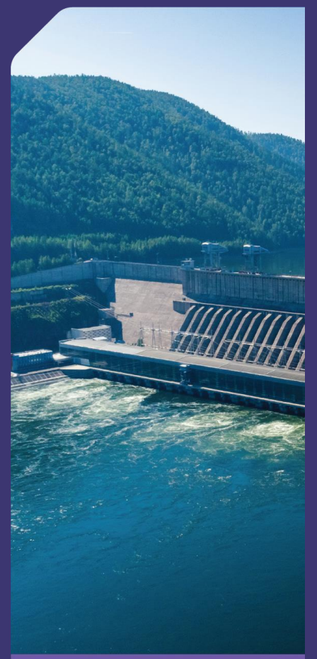
ENSAIOS
E ANÁLISES LABORATORIAIS

ÁREAS DE ATUAÇÃO

Infraestrutura

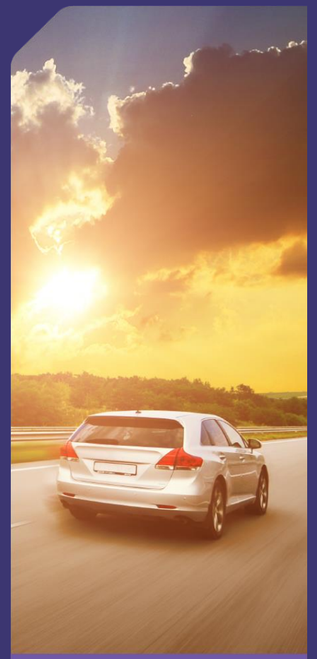


Setor Elétrico



Setor Hídrico

Petróleo e Gás



Setor Automotivo

Tecnologia da Informação

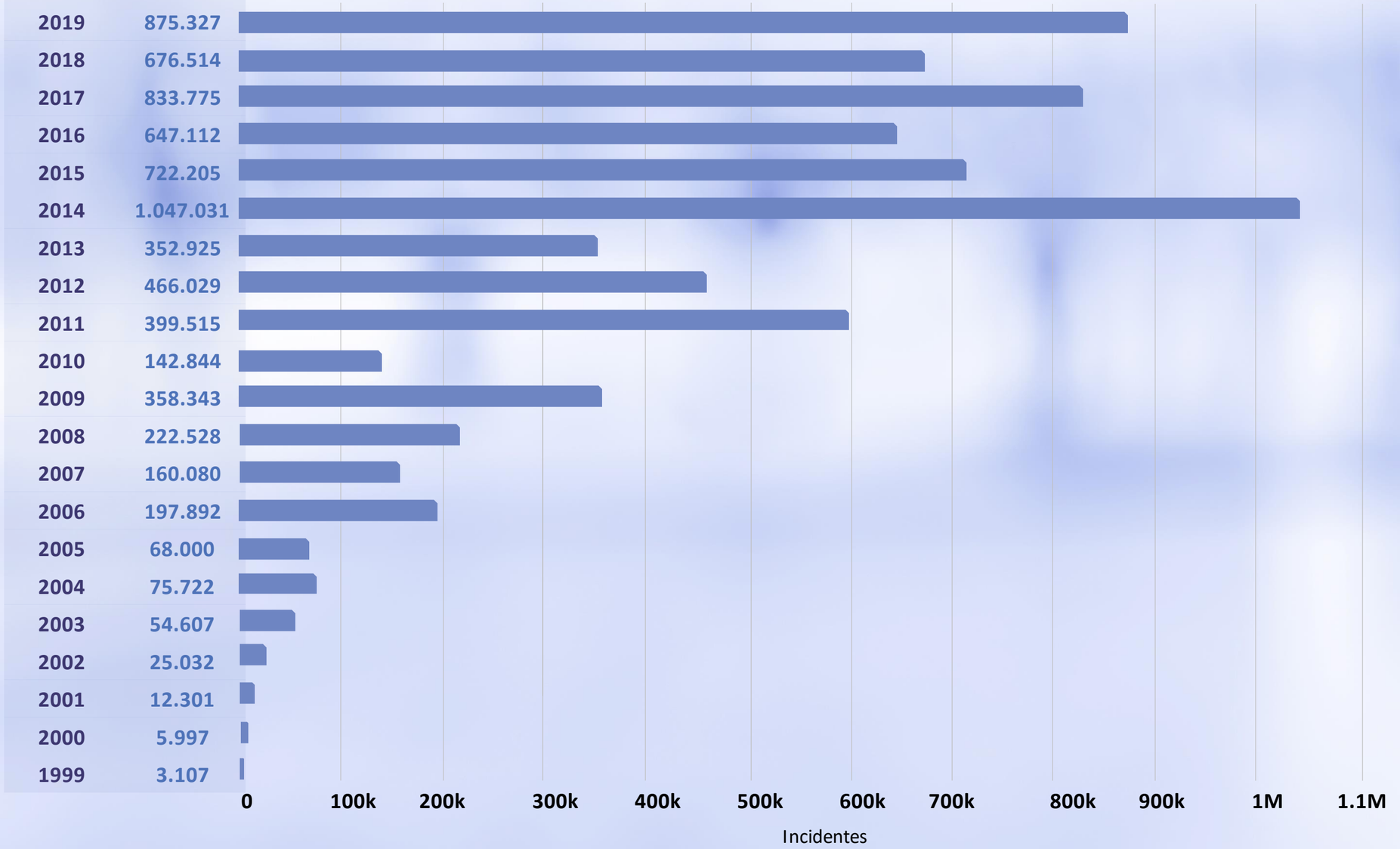
Meio ambiente

+ Diversos outros Setores

Incidentes reportados no Brasil

Total de Incidentes Reportados ao CERT.br por Ano

Ano	Total
2019	875.327
2018	676.514
2017	833.775
2016	647.112
2015	722.205
2014	1.047.031
2013	352.925
2012	466.029
2011	399.515
2010	142.844
2009	358.343
2008	222.528
2007	160.080
2006	197.892
2005	68.000
2004	75.722
2003	54.607
2002	25.032
2001	12.301
2000	5.997
1999	3.107



Ataques Cibernéticos a **Infraestruturas Críticas**

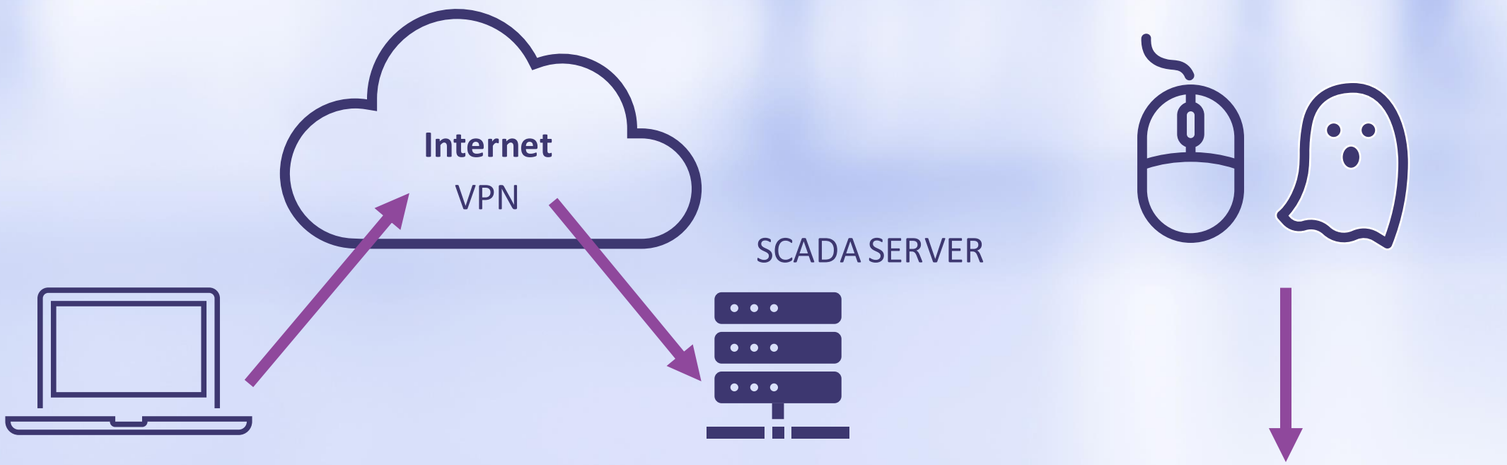
Fontes: ifri, Symantec, ICS-CER, NERC

Ano	Alvo	Nome do Ataque	Consequências	Objetivo	Origem
2013	**Represa Bowman Avenue (EUA)**		Atacantes tomaram controle da remoto da usina, com poucas consequências	Reconhecimento	Externa
2014	**Empresas do setor elétrico (EUA e Europa)**	Energetic Bear	250 empresas nos EUA e Europa ocidental foram infectadas	Espionagem	Externa
2014	**Estações de petróleo**	Operation Petrol	O grupo de hackativistas anonymous anunciou ataques de negação de serviço (DoS) e roubo de dados à companhias e estações de petróleo.Existe pouca informação a respeito da extensão e da profundidade do ataque.	Sabotagem e roubo de dados	Anonymous
2014	**Korea Hydro & Nuclear Power**		Roubo de projetos e manuais de dois reatores, diagramas dos circuitos, medidas de exposição à radiação na área e dados de mais de 10.000 funcionários.	Blackmail	Externa
2015	**Empresas do setor elétrico da Ucrânia**	Black Energy 3	30 subestações desconectadas da rede, 8 províncias sem eletricidade por várias horas, Mais de 200.000 pessoas afetadas, Infraestrutura fisicamente danificada, Subestações operadas manualmente por várias semanas após o evento	Sabotagem	Externa
2016	**Empresas do setor elétrico da Ucrânia**	Black Energy 3	Nova tentativa de ataque com o mesmo método do ataque anterior. Uma subestação foi desligada por algumas horas.	Sabotagem	Externa
2017	**Aramco (Petrolífera Saudita)**		Sem consequências maiores, o ataque visava comprometer o sistema de supervisão de acidentes de uma refinaria.	Sabotagem	Externa
2020	**EDP (Portugal)**		Roubo de dados financeiros, de funcionários e de gestão	Roubo de dados	Externa
2020	**Grupo Energisa**		Indisponibilidade de sistemas de suporte a clientes	Sabotagem	Externa

Sistema Elétrico da **Ucrânia - 2015**

Os hackers utilizaram **duas abordagens de ataque,** uma customizada e outra agnóstica, e obtiveram sucesso em acessar os sistemas SCADA/DMS de três diferentes empresas.

SCADA HIJACKING TECHNIQUES



ROGUE CLIENT
Remote SCADA Client Software

PHANTOM MOUSE
Remote Amin Tools at OS-level

Sistema Elétrico da **Ucrânia - 2015**

Os atacantes demostraram **grande perícia**, pois não só ganharam acesso às infraestruturas ligadas na rede interna, mas também na operação dos sistemas de controles de supervisão, além das interfaces homem-máquina (IHM) e sistemas de call center.

30 subestações desconectadas da Rede	**8 províncias sem** eletricidade por várias horas
Mais **de 200.000** pessoas afetadas	Infraestrutura fisicamente **danificada**
Subestações operadas manualmente por várias **semanas após o evento**	

Ataque a Israel Electric - 2016

“

Yesterday we identified one of the largest cyberattacks that we have experienced. The virus was already identified and the right software was already prepared to neutralize it. We had to paralyze many of the computers of the Israeli electricity authorities. We are handling the situation and I hope that soon, this very serious event will be over... But as of now, computer systems are still not working as They should,” said Steinitz, according to the Times of Israel.

Israel: Electricity board crippled by ransomware cyberattack causing widespread panic

By Mary-Ann Russon
January 28, 2016 13:42 GMT

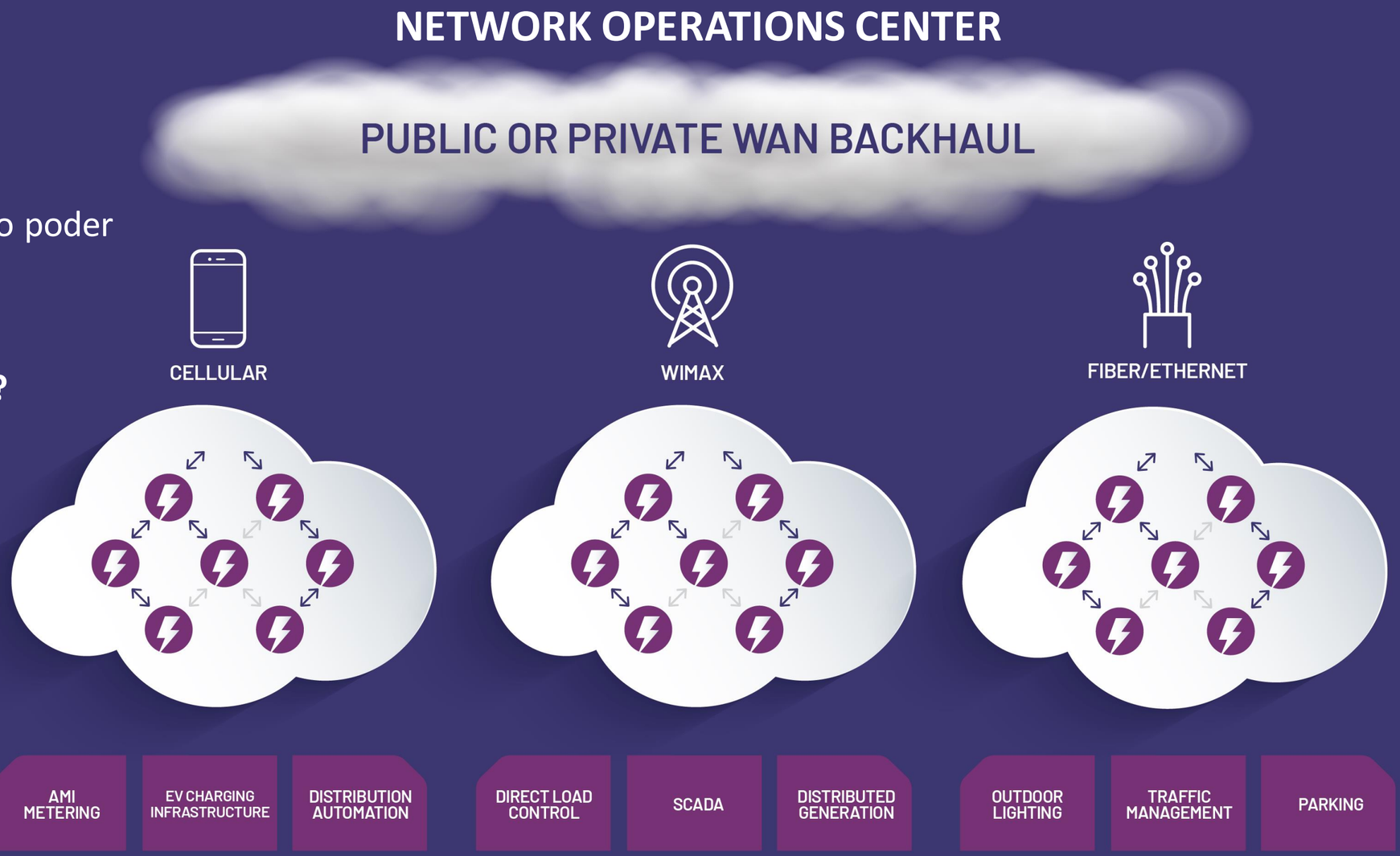
Israel's electricity regulator hit by ransomware, sparking fears the country's electricity grid had been hacked (Reuters)

Israel's Electricity Authority has been hit by a ransomware attack that paralysed some computers for more than two days, leading to fears that Israel's electrical grid had been hacked and taken down.

On 26 January, Yuval Steinitz, Israel's minister of infrastructure, energy and water, told attendees to the CyberTech 2016 security conference in Tel Aviv that Israel's electricity authority had been hit by a severe cyberattack on 25 January.

DESAFIO: Garantia de confiabilidade e privacidade em Smart Grids

- Dados sensíveis dos consumidores
- Sistemas críticos
- Equipamentos com baixo poder de processamento
- Redes de banda estreita
- **Operação em nuvem???**



Quem são os atacantes?

“

Yesterday we identified one of the largest cyberattacks that we have experienced. The virus was already identified and the right software was already prepared to neutralize it. We had to paralyze many of the computers of the Israeli electricity authorities. We are handling the situation and I hope that soon, this very serious event will be over... But as of now, computer systems are still not working as They should,” said Steinitz, according to the Times of Israel.

Israel: Electricity board crippled by ransomware cyberattack causing widespread panic

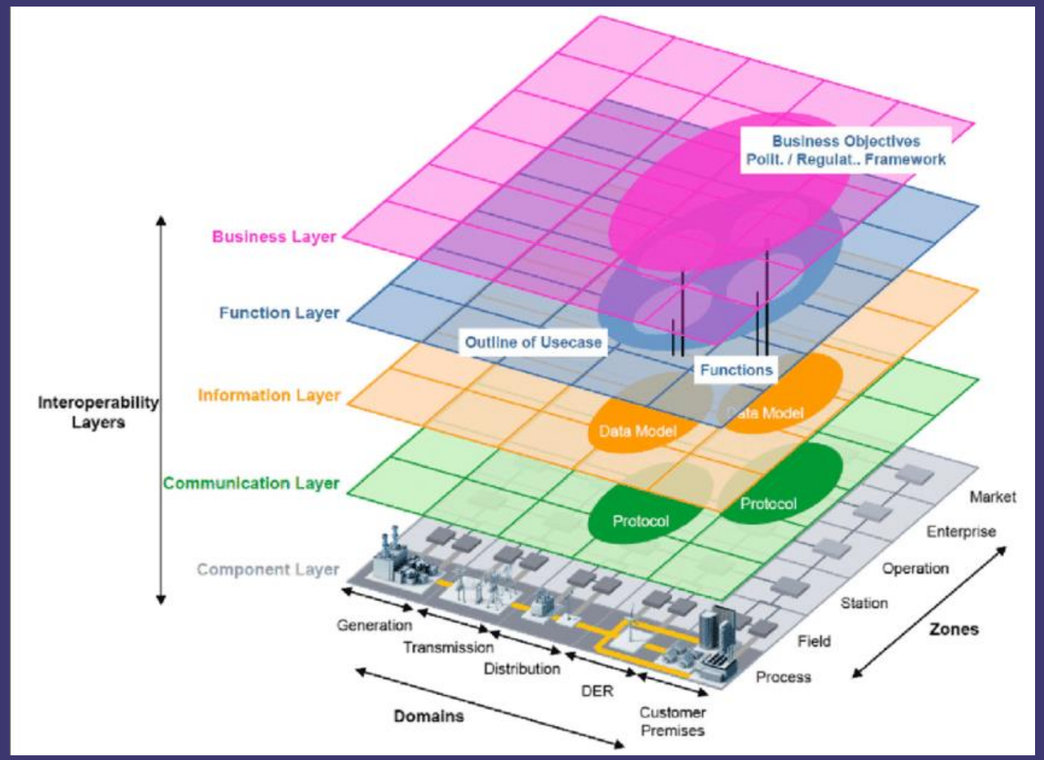
By Mary-Ann Russon
January 28, 2016 13:42 GMT

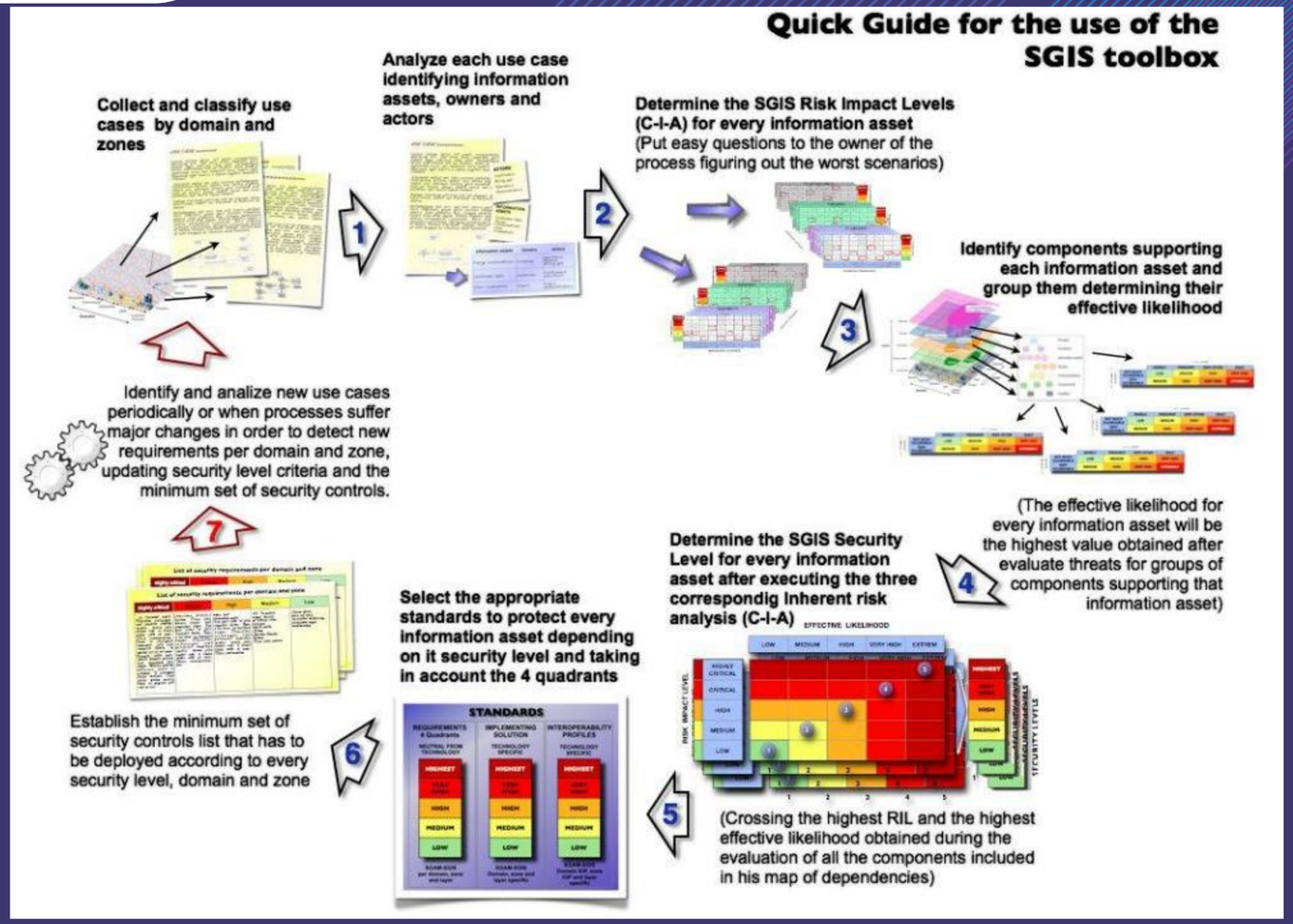
Israel's electricity regulator hit by ransomware, sparking fears the country's electricity grid had been hacked (Reuters)

Israel's Electricity Authority has been hit by a ransomware attack that paralysed some computers for more than two days, leading to fears that Israel's electrical grid had been hacked and taken down.

On 26 January, Yuval Steinitz, Israel's minister of infrastructure, energy and water, told attendees to the CyberTech 2016 security conference in Tel Aviv that Israel's electricity authority had been hit by a severe cyberattack on 25 January.

Framework CENELEC





Framework NIST

- Focos em segurança, confiabilidade do sistema de energia, resiliência e Modernização da rede de suporte
- Divisão em funções e categorias de ação
- Detalhamento de ação em cada categoria
- Atribuição de times responsáveis em todos os domínios.
- Visão global dos níveis de ação para cada função, categoria e sub categoria.

NIST Technical Note 2051 - Cybersecurity Framework Smart Grid - 2019

Function Unique Identifier	Function	Category Unique Identifier	Category
ID	Identify	ID.AM	Asset Management
		ID.BE	Business Environment
		ID.GV	Governance
		ID.RA	Risk Assessment
		ID.RM	Risk Management Strategy
		ID.SC	Supply Chain Risk Management
PR	Protect	PR.AC	Access Control
		PR.AT	Awareness and Training
		PR.DS	Data Security
		PR.IP	Information Protection Processes and Procedures
		PR.MA	Maintenance
		PR.PT	Protective Technology
DE	Detect	DE.AE	Anomalies and Events
		DE.CM	Security Continuous Monitoring
		DE.DP	Detection Processes
RS	Respond	RS.RP	Response Planning
		RS.CO	Communications
		RS.AN	Analysis
		RS.MI	Mitigation
		RS.IM	Improvements
RC	Recover	RC.RP	Recovery Planning
		RC.IM	Improvements
		RC.CO	Communications

Tecnologia, pessoas, **processos e ambiente**

- Previsão
- Identificação
- Proteção
- Detecção
- Resposta

1. Anti-vírus, Firewalls, AntiSpam, Filtros de Conteúdo
2. Detecção e controle de Vulnerabilidades
3. Managed Security Services
4. Ambientes de monitoramento contínuo
5. Sandbox
6. Treinamento intensivo para equipes de TI e TO
7. Treinamento regular para toda a empresa (phishing prevention)

Considerações finais

- Regulação atualizada e direcionadora – Alternativas 3 e 4 da nota técnica 20/2021 Aneel.
- Considerações quanto aos custos de implantação em todos os domínios propostos pela ONS.
- Levantamento do grau de maturidade e roadmap para adequação da infraestrutura e preparação dos times.
- Plano para abrangência do legado.
- Proteção ativa (MSS) – Times internos ou externos?

Rodrigo Jardim Riella

Pesquisador Lactec

riella@lactec.org.br

www.lactec.org.br

Siga-nos em nossas redes sociais