8º SENOP
Seminário Nacional de Operadores de Sistemas e de Instalações Elétricas

De 4 a 6 de outubro de 2017
Foz do Iguaçu | Paraná

Teleassistência no SIN

Fábio S. Eloy

Realização: ONS Operador Nacional do Sistema Elétrico

Organização: ITAIPU BINACIONAL

PREMISSA DO PROCEDIMENTO DE REDE

Estabelecer critérios técnicos e operacionais para que a **Teleassistência de Instalações de Geração e Transmissão** seja viabilizada, sem provocar perda para a **segurança do SIN**.

Interferência da Teleassistência Observada na Operação

- Interferência **POSITIVA**
  - Pode automatizar manobras;
  - Pode acelerar o processo de recomposição.

- Interferência **NEGATIVA**
  - Pode causar tempo adicional no processo de recomposição, nas solicitações de manobras para controle de tensão e complementação de vãos;
  - Pode não cobrir todas as condições de operação;
  - Maior dependência dos meios de telecomunicações.

- Ameaça Real
  - Ataques cibernéticos.
    - Estudo de “honeypots”.
    - Caso real da Ucrânia.

Tempo Médio Adicional em Manobras

Desde 2007 tem sido verificado (RO e RAP) ocorrências de falha em telecomando de instalações teleassistidas, implicando em tempo adicional ou na realização de manobras de recomposição após desligamento ou em manobras para controle de tensão ou manobras que envolvem geradores.

O tempo médio adicional tem sido de:

- 2007: 34 minutos;
- 2009: 41 minutos;
- 2011: 57 minutos;
- 2012: 62 minutos.
- 2013: 37 minutos;
- 2014: 58 minutos;
- 2015: 78 minutos;
- 2016: 54 minutos.

honeyTARG

Distributed Honeypots Project (http://honeytarg.cert.br/honeypots/index-po.html)

Search

English

Home
Statistics
Members
Timeline

honeyTARG
SpamPots

Sobre o Projeto Honeypots Distribuídos

Este projeto, mantido pelo CERT.br e parte do honeyTARG Honeynet Project, tem o objetivo de aumentar a capacidade de detecção de incidentes, correlação de eventos e determinação de tendências de ataques no espaço Internet brasileiro. Para atingir estes objetivos as seguintes atividades são desenvolvidas:

- É mantida uma rede distribuída de honeypots de baixa interatividade (utilizando Honeyd), cobrindo uma quantidade razoável do espaço de endereços IPv4 da Internet no Brasil;
- Foi desenvolvido um sistema que notifica, diariamente, os grupos de tratamento de incidentes (CSIRTs) das redes responsáveis por originar ataques aos honeypots;
- São mantidas estatísticas públicas:
  - gráficos diários dos fluxos de rede do tráfego direcionado a todos os honeypots;
  - gráficos gerados a cada hora com o sumário do tráfego TCP e UDP direcionado aos honeypots, incluindo as tendências observadas.

Localização dos Honeypots

#	Cidade	Instituições
01	São José dos Campos	INPE, CTA
02	Rio de Janeiro	CBPF, Eletrobras, Eletronuclear, Embratel, Fiocruz, Furnas, PUC-RIO, RedeRio, UFRJ, VIVO
03	São Paulo	ANSP, CERT.br, Durand, LOCAWEB, PRODESP, TIVIT, UNESP, UOL, USP
04	Campinas	ITAL, UNICAMP
05	São José do Rio Preto	UNESP
06	Piracicaba	USP
07	Petrópolis	---
08	Brasília	CTIR Gov, Eletronorte, UnB
09	Porto Alegre	CERT-RS, Commcorp, PROCERGS, TRI
10	Ribeirão Preto	USP
11	São Carlos	USP
12	Florianópolis	POP-SC, UFSC DAS
13	Uberlândia	Algar Telecom

Membros

Algar Telecom
ANSP
CBPF
CELEPAR
CEMIG
CERT.br
CERT-RS
Chesf
Commcorp
CSIRT PoP-MG
CTA
CTIR Gov
Durand
Eletrobras
Eletronorte
Eletronuclear
Embratel
EMPREL
Fiocruz
Furnas
INPE
ITAL
LOCAWEB
MD Brasil
MORPHUS
Nlink
Onda
PoP-ES
PoP-PR
PoP-RO
PoP-SC
PROCERGS
PRODESP
PUC-RIO
RedeRio
TALKLINK
TELETALK
TIVIT
TRI
UFBA
UFRJ
UFSC DAS
UnB
UNESP
UNICAMP
UOL
UPF
USP
Unisinos
VIVO

Cyberattacks Surge on Energy Companies, Electric Grid

Companies and utilities reported a raft of 'successful' attacks – and worry worse is yet to come.

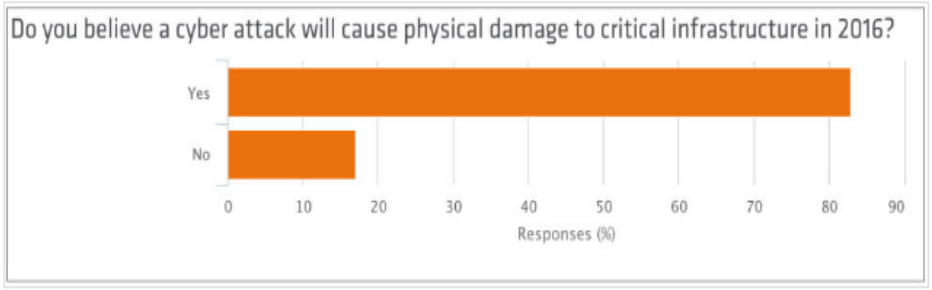
By Alan Neuhauser | Staff Writer April 8, 2016, at 4:00 p.m.

Energy companies and electric utilities have experienced a spike in cyberattacks in the past year, according to a new survey by Tripwire, a digital security firm.

Of 150 information technology workers that were surveyed, more than 75 percent reported that their companies in the oil, natural gas and electricity sectors had experienced at least one "successful" cyberattack in the past 12 months, meaning intruders were able to breach one or more firewalls, antivirus programs or other protections.

Close to half said the number of attacks have increased in the past year. More than 80 percent believe an attack will harm physical infrastructure this year.

"It's a wake-up call," says Travis Smith, a senior analyst with Tripwire. "We can start doing things to protect these networks before anything happens."



Most breaches seem to have been aimed at learning systems' vulnerabilities, but that may soon change. COURTESY TRIPWIRE

http://www.usnews.com/news/blogs/data-mine/2016/04/08/cyberattacks-surge-on-energy-companies-electric-grid

Vírus WannaCry assusta o mundo digital e levanta uma questão: Sua subestação está protegida contra ataques cibernéticos?

17 de maio de 201717 de maio de 2017SEL SchweitzerSegurança Cibernética

Nossas subestações estão seguras? Em termos de segurança cibernética, talvez não estejam. Um ataque cibernético ocorrido na Ucrânia e analisado pela SEL em conjunto com outras instituições e empresas elétricas mostrou que o inimigo já pode estar dentro de casa e passar despercebido. O ataque, recém divulgado, culminou na paralisação do sistema de operação e controle de mais de 50 subestações de energia, em 23 de dezembro de 2015, deixando 225 mil consumidores sem eletricidade por mais de seis horas.

Foi o primeiro ataque conhecido capaz de derrubar uma rede de energia elétrica e, em plena guerra civil ucraniana, levantaram-se suspeitas de que fosse ligado a rebeldes apoiados pela Rússia. Deixando a questão política de lado, o ataque mostrou a importância de realizar um monitoramento constante do sistema de operação e controle das concessionárias, tanto para evitar e barrar um possível ataque, quanto para fazer análises pós-eventos, descobrindo causas e formas de mitigação.

http://www3.selinc.com.br/news/?p=2011&utm_source=SEL+Mailing+Completo&utm_campaign=feebed6166-EMAIL_CAMPAIGN_2017_05_17&utm_medium=email&utm_term=0_effb76c828-feebed6166-35888221

Conceitos vigentes do SM 10.14

- Assistência pode se dar localmente ou a partir de um Centro de Controle remoto ou por outra instalação.
- Teleassistência = a monitoração + telecomando à distância (recursos similares ao de uma operação local).
- Instalação teleassistida pode contar com pessoas habilitadas localmente para operação em retaguarda.

INSTALAÇÕES
(usinas e subestações)

ASSISTIDA
Monitorada e comandada ininterruptamente

- Localmente
- Remotamente

DESASSISTIDA
Interrupção de monitoração e/ou comandos

- A desassistência (inexistência de supervisão e comando permanente, local ou remoto) é vetada pelos procedimentos.

Teleassistência = Telessupervisão + Telecomando.

Conceitos vigentes do SM 10.14

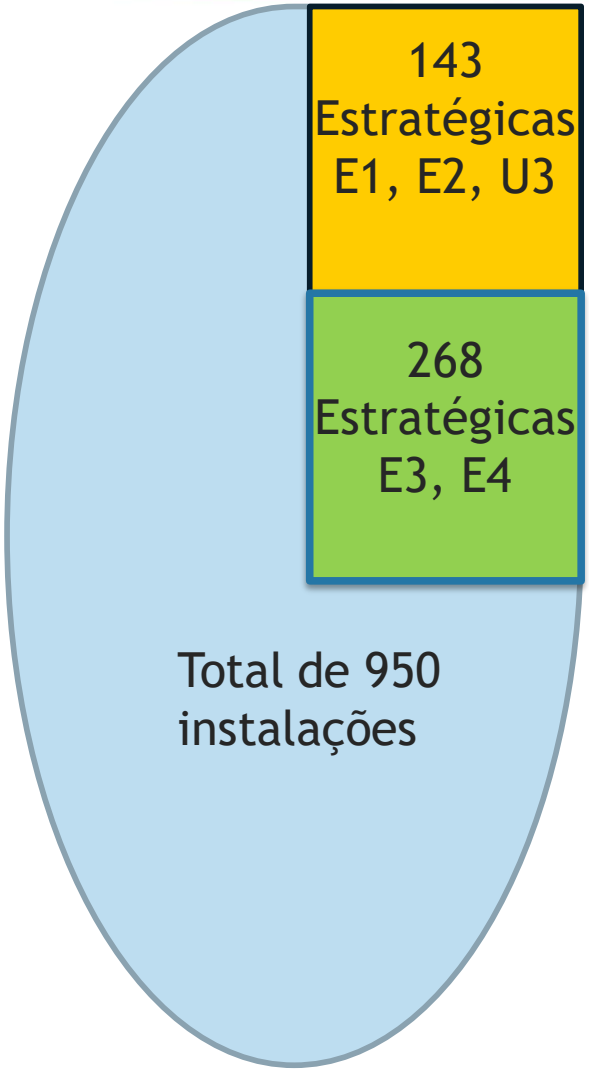
- Instalações estratégicas tipo E1, E2 e U3 devem manter operadores locais em turnos ininterruptos.

- **Objetivo:**
  - Eliminar a interferência negativa da teleassistência.

- **A presença no local de um operador permite:**
  - Atuação sobre os equipamentos;
  - Detecção de problemas;
  - Cobertura de modos não telecomandados;
  - Atuação em situações imprevistas.

- **Porque instalações estratégicas?**
  - Resultado de avaliação da matriz de risco (Probabilidade x Consequências)

Conceitos vigentes do SM 10.14



- Instalações estratégicas E1, E2 e U3 devem dispor de operador local 24h à despeito da teleassistência.
- Instalações estratégicas E3 e E4 devem ter redundância nos equipamentos e sistemas que se interponham entre as unidades concentradoras de supervisão e controle e o Centro de Operação remoto.
- Instalações estratégicas do tipo E1, E2, E3, E4 ou U3 têm prazo de 18 (dezoito) meses para as devidas adequações.

O que motivou a revisão?

- A evolução tecnológica, fundamentada através de discussões técnicas entre ANEEL, ONS, Agentes e Associações, permitiu a opção de operar instalações através de teleassistência (sem operador local).
- Teleassistência em 2017 (80%) x 2012 (56%).
- Padrão tecnológico IEC 61850 integra supervisão, controle e proteção.
- Redundância permite grau de confiabilidade elevado.
- Ofício 036 SRT/ANEEL de 04.04.2017.
- Workshop com os Agentes realizado no dia 09.06.2017.
- As alterações impactadas por esta revisão, serão submetidas a aprovação da ANEEL.

Proposta WORKSHOP

- Todas as instalações teleassistidas devem ter redundância nos equipamentos e sistemas que se interponham entre as unidades de aquisição de dados de supervisão e controle e o Centro de Operação remoto.

- **Para mitigar os possíveis efeitos negativos da operação teleassistida, os seguintes requisitos deverão ser atendidos:**

- Confiabilidade: As instalações teleassistidas devem ser dotadas de **redundância** nos equipamentos associados ao sistema de supervisão, telecomando e comunicação e o próprio Centro de Controle.

- Recursos: Equivalente a operação local

Alterações no SM 10.14

Total de 950 instalações
Mais de 80% possuem recursos de teleassistência

- **Definição de prazo para adequação dos requisitos de Centros de Operação, referente ao item 4 do SM 10.14.**
  - Centro de relacionamento com ONS, em território nacional;
  - Centro backup ou assunção de centros regionais (plano de contingenciamento);
  - Proteção contra ataques cibernéticos.

- **Prazo para adequações aos requisitos será definido pela ANEEL, após sua aprovação.**

Rebatimentos e Outras Alterações

- Sem rebatimento no SM 2.3 (requisitos de serviços auxiliares em subestações). Já exige redundância das fontes de alimentação DC e AC;
- Alteração no texto do SM 2.7 (requisitos de supervisão);
- Alteração no texto do SM 13.2 (requisitos de telecomunicações).

Obrigado pela atenção!

Fábio S. Eloy
(21) 3444-9024 – eloy@ons.org.br