



**XXIV SNPTEE
SEMINÁRIO NACIONAL DE PRODUÇÃO E
TRANSMISSÃO DE ENERGIA ELÉTRICA**

CB/GTL/22

22 a 25 de outubro de 2017
Curitiba - PR

GRUPO - XV

**GRUPO DE ESTUDO DE SISTEMAS DE INFORMAÇÃO E TELECOMUNICAÇÃO PARA SISTEMAS
ELÉTRICOS - GTL**

**DEFENDENDO A REDE
PROTEGENDO AS SOLUÇÕES PARA A PRÓXIMA GERAÇÃO DE REDES INTELIGENTES**

Diego Humberto Kalegari (*)
Omnetric Group

Jon Longstaff
Omnetric Group

RESUMO

A digitalização das redes e dos sistemas de geração, transmissão e distribuição com a introdução de novas tecnologias é irreversível, trazendo inúmeros benefícios para as concessionárias e seus consumidores. Mas com a digitalização vem uma maior exposição dos dispositivos e sistemas interligados à rede, pois esses não mais residem e são acessíveis apenas dos perímetros das concessionárias. Contudo, podem estar e serem acessados de qualquer lugar, expondo assim possíveis vulnerabilidades que podem ser exploradas por pessoas ou invasores. No passado não havia uma preocupação explícita com *cybersecurity*, pois os sistemas e dispositivos estavam em um ambiente mais controlado. Porém, com a evolução, hoje se sabe que o tema *cybersecurity* deve ser prioridade para as concessionárias, já que elas precisam garantir a proteção de suas redes visando minimizar os problemas. Apesar de não estar em foco, sempre existiu um conceito tradicional de como se deveria proteger a rede. No entanto, questiona-se: será que o conceito tradicional se adequa à nova realidade das empresas concessionárias de energia com digitalização? O que precisa ser adequado e repensado para definir um novo modelo de proteção para as redes? Essas não são perguntas simples de se responder e esse será o foco principal do artigo.

PALAVRAS-CHAVE

Cybersecurity, Segurança, Redes Inteligentes, Interoperabilidade, Vulnerabilidade

1.0 - INTRODUÇÃO

As soluções das áreas de tecnologia de informação (TI) têm ajudado as concessionárias de energia elétrica do Brasil e do mundo a criar redes inteligentes para atender seus consumidores, uma vez que a demanda por energia cresce na medida em que novos dispositivos são conectados à rede elétrica. Com a finalidade de garantir a qualidade de seus serviços, as concessionárias de energia têm instalado uma série de sistemas e plataformas de comunicação visando a uma melhora na interoperabilidade. Com um conceito denominado de Digitalização da Rede, as áreas de TI e tecnologia operacional (OT – *Operational Technology*) estão convergindo por meio da unificação de ativos (equipamentos, dispositivos) e do aumento da utilização de controles inteligentes com a utilização de sistemas e aplicações complexas com mecanismos para otimizar e melhorar a gestão da rede.

As novas tecnologias e seus fundamentos trazem consigo benefícios enormes para as concessionárias, mas, por outro lado, acabam expondo a rede a novos riscos como potenciais vulnerabilidades até então não previstas ou pensadas nos moldes tradicionais. Muitos desses riscos estão associados à segurança cibernética, do termo em inglês *cybersecurity*, ou a um conceito ainda mais amplo que é a segurança da informação. Com os riscos eminentes vem a pressão para melhorar e repensar que as políticas de segurança na nova realidade das redes de energia elétrica.

As concessionárias de energia elétrica têm enfrentado grandes desafios na operação de suas redes e isso se deve à uma mudança fundamental no modelo tradicional de negócio com a inclusão de conceitos como microgeração (PCHs, Solar, Eólica), descentralização da geração e a integração de veículos elétricos à rede.

O presente artigo tem como finalidade demonstrar como as concessionárias devem repensar a proteção da sua rede e melhorar a segurança dela e de todos os sistemas que estão à sua volta. Para entender e visualizar essa nova realidade é necessário entender e examinar o modelo tradicional de controle da rede e como ele muda quando se migra para a Digitalização. Como resultado pretendemos mostrar como esses novos conceitos podem estender e melhorar os conceitos tradicionais com a adição de conceitos e controles de segurança.

2.0 - CYBERSECURITY

2.1 - O QUE É CYBERSECURITY?

Quando falamos em segurança é como se estivéssemos falando em gerenciamento de riscos. Um risco pode ser considerado quando alguém por qualquer que seja a razão tenha o desejo de danificar ou até mesmo destruir dispositivos, ativos ou sistemas que estão sobre a responsabilidade de alguém ou de alguma empresa. Nosso papel como defensores é tentar identificar como podemos limitar ou prevenir os potenciais danos e prejuízos aos ativos sob nossa gestão.

O conceito de *cybersecurity* pode ser definido como uma coletânea de ferramentas, políticas, conceitos, mecanismos de proteção, diretrizes, ações, treinamentos, conjunto de melhores práticas, seguros, apólices e tecnologias que podem ser usadas para proteger um eco sistema computacional (cibernético), organizações e usuários de ativos de potenciais ameaças. No mundo atual existem diferentes tipos de ameaça, tais como: ataques terroristas, espionagem, atividades criminais, dentro outros. Sendo assim, quando pensamos em uma organização e seus ativos logo pensamos em dispositivos computacionais, pessoais, infraestrutura, aplicações e serviços sistemas de comunicação, todos conectados e habilitados a enviar, receber e armazenar informações dentro do eco sistema computacional.

O principal objetivo do *cybersecurity* é garantir a confidencialidade, integridade ou disponibilidade dos ativos de uma organização ou de uma pessoa. Quanto se fala em *cybersecurity* muitos pensam que o conceito engloba apenas sistemas e controles computacionais como *firewall* e criptografia, mas, na prática, o conceito é bem mais abrangente, englobando pessoas e processo de uma organização. Desse modo, para garantir os níveis de segurança dentro de uma organização é necessário estabelecer uma cultura e praticar.

3.0 - DEFININDO A REDE

Quando começamos a discutir sobre *cybersecurity* nas concessionárias de energia elétrica a primeira pergunta que devemos fazer é: o que vocês estão tentando proteger? Essa é uma pergunta crítica, pois para haver uma resposta assertiva é necessário conhecer a rede. Sem uma definição clara dos componentes da rede é fácil deixar os elementos chave de lado e, com isso, aumentar os riscos de sofrer ataques.

Abaixo segue uma lista com exemplos de componentes digitais que estão associados a uma rede digital:

- **SIC (Sistemas de Informação dos consumidores):** sistemas que contem informações pessoais dos consumidores.
- **SCADA (Supervisory Control And Data Acquisition):** Sistemas Supervisórios e de Aquisição de Dados / Sistemas de Gerenciamento de Energia que monitoram e controlam a rede da concessionária.
- **PLC (Programmable logic controller):** é um computador digital e considerado um subsistema do SCADA. São usados constantemente para automação de processos industriais como controle de redes de proteção, registradores de falta, etc.
- **EMS (Energy Management Systems) ou DMS(Distribution Management systems):** são sistemas utilizados por operadores de transmissão (EMS) e distribuição (DMS) para monitorar, controlar e otimizar a performance da geração e das redes de transmissão e distribuição das concessionárias de energia elétrica.
- **CPS (Cyber Physical System):** mecanismo controlado por algoritmos utilizados para monitorar e controlar sistemas e equipamentos.
- **PLC (Power Line Communication) and the Public Cellular Network:** são dispositivos comumente utilizados para a comunicação de medidores inteligentes, mas podem ser aplicados em outros equipamentos das redes da concessionárias.
- **Concentradores de Dados:** são dispositivos eletrônicos que fazem a interface com sensores e outros equipamentos, com o intuito de transmitir dados coletados de equipamentos de campo para centrais ou sistemas.
- **Historiadores:** são sistemas computacionais complexos desenvolvidos para coletar e armazenar informações e *logs* gerados por diversos tipos de equipamentos como sensores, alarmes e eventos gerados por dispositivos de campo que são parte da rede.

- **HMI (Human-Machine Interface):** componente/dispositivo responsável pela apresentação dos dados.
- **Infraestrutura de comunicação:** pode fazer uso de equipamentos tradicionais ou específicos para garantir a intercomunicação dos diferentes equipamentos e sistemas conectados à rede.

O presente artigo foca nos dispositivos e ativos digitais das redes inteligentes, e não nos dispositivos físicos como cabos, transformadores etc. Com isso, conseguimos identificar quais e quantos são os dispositivos conectados a uma rede moderna e inteligente. Caso fossemos tratar desses dispositivos físicos para gerenciar os seus riscos, precisaríamos nos atentar não só aos tipos, mas sim às suas características. Porém, este é o desafio das concessionárias: não só mapear os dispositivos digitais, mas, também, os físicos. E para entender suas vulnerabilidades será necessário entender os *softwares* e mecanismos, assim como os componentes dos dispositivos físicos.

4.0 - A VISÃO TRADICIONAL PARA PROTEÇÃO DA REDE

O conceito de proteger a rede se tornou uma preocupação das concessionárias há um bom tempo. E dentro dessa linha existem várias visões de proteção que estão resumidas abaixo:

- 1) **Controles de Acesso Físicos:** dispositivos e equipamentos críticos em lugares fechados, com controle de acesso rígido, como em subestações protegidas por cercas com arame farpado e portões, e centros de controle localizados em prédios, como salas com acesso restrito e protegidas por câmeras e controladores de acesso.
- 2) **Redes Isoladas:** redes nas quais os sistemas conectados utilizam uma rede dedicada com acesso restrito e conectividade extremamente limitada com outros sistemas.
- 3) **Tecnologia Proprietária:** onde se utiliza de tecnologias restritas e proprietárias não usuais, as quais poucas pessoas conhecem (geralmente apenas fabricantes). Exemplos: conexões seriais e protocolos únicos.
- 4) **Equipe Confiável:** historicamente existiam pequenos grupos de pessoas conhecidas e qualificadas que eram responsáveis por operar e gerenciar a rede e os dispositivos conectados a ela, assim como controlar o acesso e manutenção dos dispositivos físicos.
- 5) **Pessoas no Controle:** nos moldes atuais, os sistemas de controle da rede reportam informações para um centro de controle no qual há pessoas aptas a interpretar a informação e tomar decisões caso necessário, ou seja, um operador tem a oportunidade de tomar uma decisão racional em relação à rede utilizando seu conhecimento e experiência, baseando-se em informações conhecidas. Caso os operadores sejam expostos a situações de recebimento de não são de conhecimento e que não estão habituados em muitas vezes não são verificadas, questionadas ou interpretadas.
- 6) **Ameaça Limitada ou Controlada:** no passado, as ameaças às redes eram tangíveis e em muitos casos apenas teóricas. Não existiam muitos exemplos reais de ataques, o que limitava a percepção de até onde os riscos poderiam ir e que controles poderiam ser afetados. Na prática, todos tinham a visão de que ataques não aconteceriam.

Todos os controles de segurança serviram bem e estão bem sedimentados. Muitos estão também associados a procedimentos de segurança, o que é extremamente importante e deve ser levado em consideração quando movemos de uma rede tradicional para uma rede digital.

4.1 - ACESSANDO OS CONTROLES DE PROTEÇÃO TRADICIONAIS DE UMA REDE DIGITAL

Agora que conhecemos os controles de proteção tradicionais de uma rede devemos entender como esses controles podem ser aplicados às ameaças que circundam as redes digitais.

Existem muitas diferenças em como os riscos podem ser mapeados nesse novo conceito. A principal é uma das mais importantes é a separação entre o dispositivo e o invasor. Em uma rede não digital o invasor precisa se aproximar fisicamente do dispositivo para causar danos, já em uma rede digital o invasor precisa apenas estar próximo a algum mecanismo que possa acessar a rede remotamente ou causar algum dano a ela e para tal existe diversas maneiras de como atacar a rede.

Além disso, uma vez que a rede seja invadida, o invasor pode ter acesso a outras áreas, sistemas e equipamentos muitas vezes não localizados na mesma região, mas geograficamente esparsos, o que, fisicamente, no passado, não era acessível, ou seja, o poder de dano aumenta consideravelmente na medida em que o invasor vai quebrando acesso e entrando cada vez mais no centro da rede.

A detecção de um invasor físico a um dispositivo muitas vezes está baseada em processos e sistemas de proteção bem difundidos no mercado, como alarmes e sistema de CFTV. A detecção de um invasor dentro das redes digitais é algo mais difícil e complexo, uma vez que, em muitos casos, os invasores podem demorar meses sem serem detectados.

Nas próximas sessões vamos reexaminar os controles descritos na sessão 4.0, mas com um olhar cauteloso dentro dos conceitos das redes digitais inteligentes.

4.1.1 Controles de Acesso Físicos

O princípio do controle de acesso físico é colocar todos os componentes e dispositivos conectados e interligados em uma localidade com controle de acesso restrito. Tradicionalmente, isso significa utilizar cercas, portões, circuitos de CFTV, dentre outros.

Porém, com a introdução de dispositivos e equipamentos digitais na rede, em especial nas redes de transmissão de média e baixa tensão, essa visão se torna obsoleta, pois em muitos casos os equipamentos são localizados fora dos perímetros das concessionárias nas quais controle de acesso não é uma opção. Um exemplo é a vertente da introdução de medidores inteligentes nas redes, sejam elas residenciais, industriais, de fronteira, de transformadores ou de alimentadores. Esses medidores exigem a existência uma rede de comunicação que possibilite a sua conexão com as concessionárias para a realização de coleta de dados, análises ou envio de comandos. Essa conectividade de um medidor que, apesar de estar a quilômetros de distância das concessionárias, está conectado digitalmente à sua rede, pode representar uma possível rota de invasão.

Outros exemplos que podemos citar incluem equipamentos como os chamados *fuse-safer*, religadores, sensores de transformadores e linhas de transmissão que estão conectados diretamente à rede e não residem nos perímetros da concessionária, mas estão conectados a ela por meio de redes 3G, *Wimax* e, muitas vezes, por rádio e até mesmo por dispositivos USB. Todas as conexões externas com equipamentos são pontos de atenção, pois podem servir de rota de entrada para invasores.

4.1.2 Redes Isoladas

Enquanto o conceito de redes isoladas é bem conhecido e difundido dentro dos departamentos de TI das concessionárias, a sua efetividade vem sendo questionada há algum tempo. Na prática, a ideia de isolar fisicamente uma rede nos moldes atuais é impossível, pois, inevitavelmente, de algum modo a comunicação digital pode acontecer nem que se seja por meio de um dispositivo USB, já que em algum momento será necessário realizar atualizações de *software* e antivírus, alterar arquivos de configuração ou instalar novos *softwares*, os quais serão transferidos de fora da rede isolada.

A digitalização das redes tem em um de seus pilares a troca de informação entre os diversos sistemas que realizam a sua gestão e o seu controle. Além disso, existem necessidades técnicas de integração com sistemas de georeferenciamento, previsão do tempo, equipes de campo, sistemas comerciais e de faturamento, sistema de resposta à demanda, entre outros, aumentando a necessidade das redes de dados de estarem cada vez mais interligadas. Hoje existem sistemas que nem sempre são operados pelas concessionárias e sim por parceiros e outros que precisam enviar dados para os sistemas da concessionárias que residem fora do seu perímetro como: sistemas de fronteira e distribuição.

Todas essas conexões com diversos sistemas requerem mecanismos sofisticados de proteção para os sistemas críticos que controlam e gerenciam a rede, pois simples ataques como *SQL injection* não serão bloqueados por um simples *firewall*. Além disso, cuidados devem ser levados em conta para proteger a rede para um dos tipos mais tradicionais de ataque: *denial-of-service DDOS*.

4.1.3 Tecnologia Proprietária

Com o crescimento e digitalização das redes não devemos ficar surpresos com o crescimento da utilização de aplicações e sistemas de diferentes provedores de soluções de TI. Essas soluções podem utilizar redes IPs, sistemas operacionais comerciais e soluções de *software open source*. Todas essas soluções trazem benefícios de anos de desenvolvimento e testes, resultando em *softwares* maduros e confiáveis. Porém, o ponto fraco é que invasores podem facilmente obter acesso a essas tecnologias e entender como elas funcionam. E esse é o ponto crítico e geralmente inicial quando se planeja um ataque: entender que tecnologias e soluções uma determinada concessionária utiliza para ser assertivo na hora de atacar.

A utilização dessas tecnologias significa que as vulnerabilidades são muito mais fáceis de serem identificadas e de se espalharem rapidamente pela internet e redes sociais, e geralmente os invasores vão utilizar essas informações e explorá-las para invadir e atacar os sistemas. Exemplos claros podem incluir sistemas operacionais como Linux e aplicações escritas em Java que são conhecidos por serem vulneráveis. Para solucionar os problemas conhecidos, muitas vezes *patches* são disponibilizados rapidamente. Porém, a sua aplicação nos sistemas muitas vezes pode demorar meses ou até anos devido à complexidade e criticidade dos sistemas.

Além disso, vemos o grande aumento na utilização de tecnologias *open source*. Esse tipo de tecnologia pode trazer benefícios importantes para as empresas que a utilizam, como rapidez no desenvolvimento de produtos, oportunidades de criar soluções sobre essas aplicações, soluções e *softwares* com baixo custo de desenvolvimento e suporte global das comunidades responsáveis pelo seu desenvolvimento. Porém, existem diversos desafios relacionados a soluções *open source* que não podem ser descartados. Muitos invasores focam seus esforços em aplicações que utilizam essas tecnologias em larga escala, podendo explorar as vulnerabilidades dessas soluções

para atacar e comprometer um ou diversos sistemas com o mínimo esforço, uma vez que mais de uma solução utiliza o mesmo código aberto. Existem alguns estudos como o do relatório do *State of Software Security (SoSS)*, publicado pela Veracode, que demonstra que mais de 97% das aplicações Java contêm componentes inseguros e vulneráveis. Ainda, afirma que 60% das aplicações em geral não se preocupam com as diretrizes de segurança.

Outro fato que devemos considerar e que tem aparecido com o crescimento da rede é a utilização de protocolos que se comunicam com IPv6. Em geral, os administradores de sistemas não se preocupam com esses protocolos e deixam de criar regras que possam bloquear ou desabilitar esse tipo de comunicação dentro da rede da concessionária de energia elétrica, podendo, assim, deixar brechas para possíveis ataques.

4.1.3.1 Equipe Confiável

Com a crescente integração das organizações além do aumento do escopo das redes e da infraestrutura de comunicação também existe um aumento no número de pessoas que tem acesso direto aos equipamentos e dispositivos da rede. Isso significa que mais indivíduos tem acesso a dispositivos críticos a rede inteligente. Com o aumento das relações comerciais e a terceirização de serviços, existem mais organizações operando e gerenciando os ativos da rede, o que significa que nem sempre terceirizados terão a mesma exposição aos treinamentos e às práticas de segurança da organização. Sendo assim, será necessário desenvolver treinamentos e capacitar essas pessoas.

Um fato notável é que muitos dos ataques e tentativas de invasão são atribuídos a erros humanos ou à utilização de mecanismos como *sperr phising*, uma vez que todos nós podemos ser facilmente manipulados e induzidos a erros. Esse é mais um exemplo do porquê o treinamento e a preparação das equipes são importantes.

4.1.4 Pessoas no Controle

A digitalização trouxe uma quantidade massiva de dados aos quais os funcionários das concessionárias são expostos durante a operação do dia a dia. Ainda, trouxe os desafios de gerenciamento e interpretação das informações, sinais e controles para que possam ser utilizados no processo de tomada de decisão dos operadores. Muitas das análises e decisões, que antes eram tomadas exclusivamente por operadores devido à quantidade de dados, têm sido passadas para os sistemas e equipamentos “inteligentes” conectados à rede que processam informações em tempo e analisam uma quantidade enorme de dados e toma decisões em segundos, ou até mesmo milissegundos, decisões essas que operadores não poderiam sequer pensar em fazer.

O risco por trás de terceirizar a tomada de decisão em sistemas críticos pode dificultar a identificação em caso de tentativas de invasão nos sistemas responsáveis pelo processo de tomada de decisão. Em casos como esse: Será que os operadores seriam capazes de identificar se o sistema e a rede estão se comportando e respondendo de maneira correta? Será que o sistema seria capaz de recusar e detectar entradas incorretas causadas por um invasor? Essas não são perguntas com respostas prontas e fáceis mas são coisas que devemos levar em consideração quanto pensamos em segurança.

4.1.5 Ameaça Limitada ou Controlada

Até hoje trabalhamos sempre com uma rede que entendíamos estar protegida de riscos e pouco exposta, e nossos esforços sempre foram focados nos procedimentos de segurança. Proteger a rede e seus dispositivos de ataques diretos era algo pensado, mas com pouco impacto e preocupação dentro das concessionárias.

Porém, com a digitalização, ativos ficaram expostos a invasores e ataques; um risco conhecido, mas com um impacto até então considerado pequeno. Contudo, com o ataque cibernético ocorrido em 23 de dezembro de 2016 em uma concessionária da Ucrânia, no qual pelo menos oito concessionárias de distribuição foram atacadas, o que resultou em falhas no fornecimento de energia que afetaram 230.000 instalações e mais de 30 subestações, foram necessárias seis horas para realizar o reestabelecimento completo da rede, uma vez que os invasores substituíram *firmwares* de equipamentos e atacaram os sistemas SCADA das concessionárias, deixando-as no escuro sem poder operar seus dispositivos e equipamentos em campo. Foi necessário realizar a recomposição manual em cada uma das subestações, uma após a outra.

Apesar dos ataques não terem sido tecnicamente sofisticados, o seu planejamento levou meses. Isso demonstra o alto nível de conhecimento que os invasores (*hackers*) tinham e têm sobre a rede de dados, equipamentos e sistemas. A mensagem que fica é que a rede das concessionárias está exposta a possíveis ataques que podem ser sérios e causar muitos danos. Quando analisamos a fundo o ataque na Ucrânia percebemos que os problemas causados poderiam ter sido ainda maiores caso equipamentos fossem sobrecarregados e danificados.

5.0 - REDEFININDO OS CONTROLES PARA A REDE

As análises realizadas na sessão 4.1 demonstram que devemos considerar métodos adicionais para aumentar a segurança e o nível de proteção das redes de energia elétrica na era da digitalização. Muitas soluções que vêm sendo entregues para a concessionária de energia incluem controles básicos de segurança e esses ajudam a formar uma parcela importante da solução de segurança que aquela determinada concessionária irá utilizar. Contudo, devemos considerar uma gama de controles maior que inclui novos processos e melhorias organizacionais.

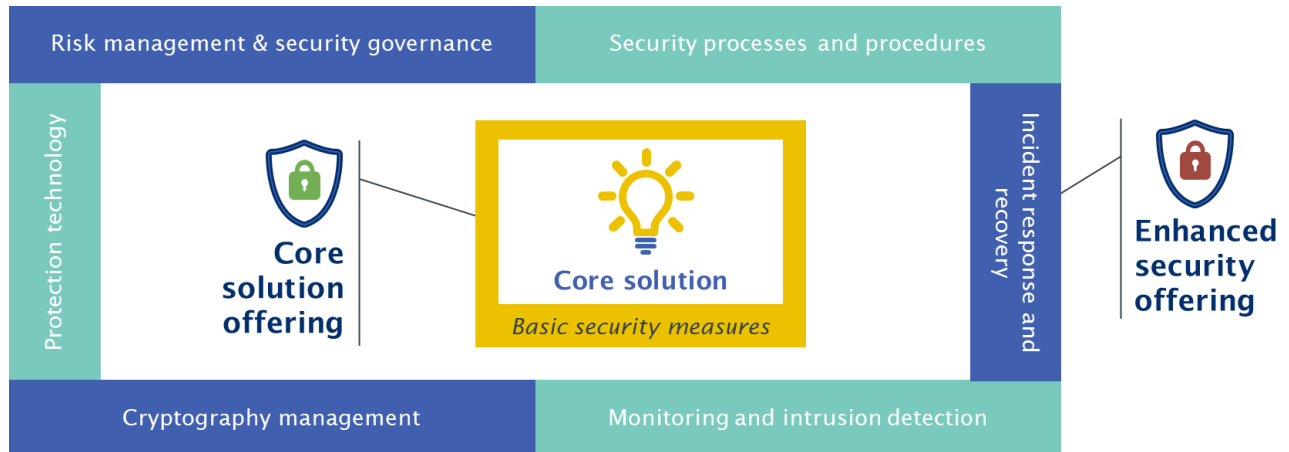


Figura 1 – Melhorias na segurança

Existem muitas maneiras de quebrar os conceitos e domínios, e escolhemos seguir na seguinte linha:

Gerenciamento de Risco e Governança de Segurança (*Risk Management and Security Governance*)

- Esse item se refere a como a segurança deve ser gerenciada dentro das concessionárias e como essas devem definir os requisitos de segurança. Em alguns padrões, como no norma ISO27001, o passo mais importante no gerenciamento de segurança é engajar os gerentes
- Risco é o ponto central na nossa visão de segurança. Os riscos devem ser identificados, analisados e gerenciados. Porém, é importante ter os níveis gerenciais mais altos das concessionárias engajados para as soluções de segurança.

Processos e procedimentos de Segurança (*Security Processes and Procedures*)

- Entender como operar uma solução segura é crítico. Muitas falhas são resultados de decisões operacionais incorretas. Então, é essencial que os processos e procedimentos sejam desenhados, acordados e documentados.
- Treinamento é vital para que as equipes da concessionária e funcionários terceirizados possam seguir os processos e procedimentos. Relatórios e lista de presença, assim como avaliações, são um ponto importante de evidência em caso de falhas e invasões

Tecnologia de Proteção (*Protection Technology*)

- Muitos controles e metodologias de proteção podem ser implementados. Contudo, é nesse momento que as decisões devem ser assertivas e justificadas por uma série de requisitos. Não basta colocar a melhor tecnologia do mercado e gastar milhões se não souber se ela será útil para a estrutura e necessidades da concessionária.

Gerenciamento de Criptografia (*Cryptography management*)

- Nos dias de hoje essa é uma área muito importante e com que os operadores da rede devem estar familiarizados.
- É esperado que a utilização do sistema com criptografia seja estendida a diversas áreas da rede visando dificultar acesso aos dispositivos, equipamentos e sistemas.
- Criptografia é um mecanismo poderoso de tecnologia que merece uma atenção especial. Existem organizações que implementaram mecanismos robustos de criptográfica para se sentir seguras, mas o resultado foi que elas mesmas ficaram sem acesso ao seus próprios sistemas e equipamentos. Processos bem definidos são críticos para o sucesso da utilização de criptografia.

Monitoramento e Detecção de Invasão (*Monitoring and Intrusion Detection*)

- Toda rede ou sistema pode ser invadido, especialmente quando estão espalhados por uma grande área geográfica e apresentam tecnologias obsoletas e sem mecanismos de segurança

- Outro ponto importante é que se não estamos buscando invasores na rede é muito pouco provável que consigamos identificá-lo.
- Devido à natureza operacional das redes, recomendamos que exista um monitoramento que envolva não só a tecnologia, mas, também, os processos e, o mais importante: as pessoas.

Resposta a Incidentes e Recomposição

- Concessionárias estão preparadas para incidentes como falta de energia devido a falhas naturais nos equipamentos.
- Incidentes relacionados a *cybersecurity* são diferentes tanto na identificação quanto na resposta, exigindo, assim, novos processos e habilidades.
- Precisamos garantir que os operadores da rede no centro de controle e os engenheiros de campo estejam familiarizados com os sintomas dos ataques e saibam como responder a eles.

6.0 - FRAMEWORKS PARA DEFENDER A REDE

Existe uma vertente que afirma que devem ser criados padrões para defender a rede com a finalidade de termos uma resposta mais efetiva e, nesse sentido, alguns países e seus institutos têm tomado ações para criar metodologias e processos que ajudem as concessionárias de energia a entender os riscos e criar soluções para a segurança.

Um exemplo desse processo está sendo proposto pelo *US National Institute of Standards and Technology's* (NIST) com a criação de um *Framework* para melhorar a infraestrutura crítica. O *framework* é conhecido como *NIST Framework* e deve ajudar as concessionárias com a seguinte postura:

- Entender o conceito de *cybersecurity*: e como ele pode ser utilizado para atingir os objetivos das empresas.
- Identificar – auditar sistemas, processos ativos para identificar potenciais problemas e priorizá-los para que as informações possam ser adicionadas à metodologia de gerenciamento de risco e suporte na decisão das operações.
- Proteger – implementar um controle de acesso, treinamento, metodologias de segurança dos dados, procedimentos e normas de segurança, manutenção de equipamentos-chave e implementar soluções inteligentes de segurança.
- Detectar – utilizando dados, processos e ferramentas avançadas para que engenheiros e operadores possam detectar ameaças e falhas.
- Responder – utilizar mecanismos que possam responder com rapidez e eficiência a ameaças nos diferentes níveis da concessionária.
- Recuperar – criar um plano de priorização e restabelecimento de fases de acordo com as prioridades e os objetivos da concessionária.

Outro exemplo é o NIS (*Network and Information Security Directive*), que vem sido discutido na Europa. As diretivas do NIS são focadas no setor de energia, uma vez que esse setor é visto como setor chave por englobar operadores de um serviço essencial. As concessionárias devem garantir a segurança de suas redes, dispositivos, equipamentos e sistemas.

A ideia por trás do NIS é definir medidas para aumentar o nível de segurança das concessionárias, seja pela definição de padrões ou pela regulamentação. Os objetivos principais do NIS são:

- Aumentar as capacidades de *cybersecurity* das concessionárias por meio da criação ou extensão de poderes de órgãos reguladores.
- Aumentar a cooperação entre as concessionárias espalhadas pelos países e também por empresas do setor de TI, visando coordenar a troca de informações e melhorar a forma de detecção de falhas e invasões, assim como a resposta quando esses incidentes acontecem.
- Garantir que as empresas pratiquem o gerenciamento de risco na área de *cybersecurity* no maior nível possível. Isso inclui a troca de informação entre os diversos, público ou privado, reportando incidentes que afetaram de alguma maneira seus sistemas e dispositivos críticos.

7.0 - CONCLUSÃO

Está claro que as redes de energia elétrica estão expostas a riscos e devem ser protegidas utilizando diferentes técnicas e estratégias. A base desse artigo foi analisar as soluções tradicionais e identificar que elas, apesar de ainda serem importantes, não são suficientes para defender a rede quando elas entram na era digital.

Uma concessionária não pode simplesmente desativar ou isolar os seus sistemas durante ou após uma invasão assim como acontece com outras organizações. Em um evento de ataque, a preocupação principal das concessionárias deve ser sempre se “o sistema continua funcionando” e se é possível gerenciar a falha e a invasão sem parar o sistema e interromper a distribuição de energia.

Novas tecnologias, processos e replanejamento são necessários caso se deseje continuar a busca pela defesa da rede e chegar a níveis de proteção que nos deem certa segurança. Mas a indústria ainda precisa mudar o seu pensamento e o modo como defendem a rede. Os invasores são ágeis e os defensores também precisam ser. As concessionárias e órgãos reguladores devem pensar em iniciativas conjuntas para a definição das melhores práticas de gerenciarmos os riscos se sabermos como devemos atacá-los.

8.0 - REFERÊNCIAS BIBLIOGRÁFICAS

- (1) Smart Grid Cyber Security Report, A EURELETRIC report, Dezembro 2016
- (2) Communication network dependencies for ICS/SCADA Systems, Dezembro 2016
- (3) Centre for the Protection of National Infrastructure CPNI, “Good Practice Guide. Process control and SCADA security,” 2008
- (4) Digital Bond, “Digital Bond,” [Online]. Available: <http://www.digitalbond.com/tools/basecamp/metasploit-modules/>. [Acessado em 10 02 2017]
- (5) Centre for the Protection of National Infrastructure CPNI, “Securing the move to IP-Based SCADA/PLC networks,” Novembro 2011.
- (6) Organization for Security and Co-operation in Europe (OSCE), “Good Practices Guide on Non-Nuclear Critical Energy Infrastructure Protection (NNCEIP) from Terrorist Attacks Focusing on Threats Emanating from Cyberspace,” 2013.
- (6) Strategic Principals for Securing the Internet of Things, US Homeland Security, Novembro 2016

9.0 - DADOS BIBLIOGRÁFICOS

Nome: Diego Humberto Kalegari

Local e ano de nascimento: Curitiba 1983

Local e Ano de Graduação: PUC-PR, 2005. Engenharia de Computação

Experiência profissional: Mestre em Informática Industrial pela UTFPR

Trabalhos Técnicos:

KALEGARI, DIEGO H.; LOPES, HEITOR S. . An improved parallel differential evolution approach for protein structure prediction using both 2D and 3D off-lattice models. An improved parallel differential evolution approach for protein structure prediction using both 2D and 3D off-lattice models, v. 1, p. 143-150, 2013.

KALEGARI, D. H.. A differential evolution approach for protein structure optimisation using a 2D off-lattice model. International Journal of Bio-Inspired Computation (Print) **JCR**, v. 2, p. 242, 2010.

Fabio Alessandro Guerra ; COELHO, L. S. ; KALEGARI, D. H. ; COELHO, M. C. ; PEREIRA, T. E. V. . Abordagem de enxame de partículas cooperativo paralelo aplicado na otimização da predição da estrutura de proteínas utilizando o modelo AB em 2D. In: X Congresso Brasileiro de Inteligência Computacional (CBIC 2011), 2011, Fortaleza, CE. X Congresso Brasileiro de Inteligência Computacional (CBIC 2011), 2011. v. 1. p. 1-8.

KALEGARI, D. H, KIEFER ANDREAS. Virtualização de Sistemas Supervisórios (SCADA) visando confiabilidade e Alta Disponibilidade. In: XXIII SNPTEE – Seminário Nacional de Produção Transmissão de Energia Elétrica, 2015, Foz Do Iguaçu.

Nome: Jon Longstaff

Local e ano de nascimento: Nottingham 1972

Local e Ano de Graduação: Cranfield University, 1992. Engenharia de Sistemas Aero mecânicos

Experiência profissional: Experiência nas áreas de segurança da informação, medição eletrônica, e *cybersecurity*.
Certificação: CISSP – Certified Information System Security Professional e TOGAF 9 Foundation

Trabalhos Técnicos

LONGSTAFF, Jon: Cyber Security Myths in the Energy Grid, In Linked In, 2016