Segurança Cibernética de Microrredes: Protegendo e Construindo a Rede do Futuro

MICROGRID KNOWLEDGE

Por que Precisamos de Segurança Cibernética em Microrredes: A Ameaça é Real

A supertempestade Sandy gerou uma onde de ativismo em favor das microrredes ao revelar como o vento e a água podem arrasar uma grande rede elétrica metropolitana. Cinco anos depois, a América do Norte sofreu uma destruição similar com os furacões Harvey, Irma e Maria. Mesmo sendo eventos muito devastadores, eles não são nada comparáveis com a ameaça de um grande ataque cibernético contra as redes elétricas.

Esta nova ameaça é pior porque, diferente da ação da natureza, muitas vezes chega sem aviso, não deixando muito tempo para preparação. Um ataque cibernético tem o potencial de devastar extensas porções de sistemas elétricos por períodos maiores de tempo, devido ao risco do efeito cascata. Os especialistas em segurança descrevem um ataque cibernético contra um sistema elétrico como uma forma de guerra desigual, o equivalente a destruir uma sociedade pelo colapso no abastecimento de alimentos, água, atendimento médico, no comércio e nas comunicações. A economia moderna é movida a eletricidade. Sem a eletricidade, ela paralisa.

"Eles não podem nos derrotar no ar; eles não podem nos derrotar no mar ou em terra. Então eles irão nos perseguir onde somos vulneráveis, e por isso precisamos proteger nossa infraestrutura", diz William Anderson, ex-secretário assistente da Força Aérea, agora como consultor de defesa especializado em energia, segundo a Microgrid Knowledge.

Como em toda guerra, a prevenção é a primeira estratégia. Além da prevenção, porém, devemos estar preparados para o pior. Isso significa criar sistemas para respostas rápidas, abrigo para a população afetada e proteção para os ativos críticos no caso em que os hackers consigam sabotar os sistemas de energia na geração, distribuição ou transmissão.

As microrredes são uma parte expressiva deste plano de recuperação, porque elas podem garantir um oásis elétrico durante uma interrupção de fornecimento. As microrredes podem alimentar os serviços essenciais de uma comunidade – segurança pública, proteção contra incêndios, assistência médica, comunicações e distribuição de água, alimentos e combustíveis. Algumas incluem um centro comunitário dentro de sua área de abrangência, com um abrigo onde as pessoas afetadas podem se reunir para carregar as baterias dos telefones e entrar em contato com familiares.

Essas ilhas elétricas são criadas usando fontes de energia que podem se desconectar da rede e operar de forma autônoma, usando geradores reserva, geração localizada, energias renováveis e baterias para alimentar as linhas dentro da microrrede. As microrredes assumem a distribuição de energia durante interrupções de fornecimento ou instabilidades de tensão, ou elas podem ser configuradas para distribuição temporária ou móvel de energia em cenários de emergência.

A segurança cibernética de microrredes está chegando, mas rápido o suficiente?

As microrredes começaram a ser implementadas em comunidades, hospitais, concessionárias e instalações militares, entre outras, porém não no ritmo ideal. Se um ataque cibernético em massa abater uma grande seção de rede hoje, provavelmente serão necessários meses ou anos para a recuperação. A Navigant Research identificou 1.842 projetos de microrrede em todo o mundo, muitos deles para proteção de serviços essenciais durante interrupções de fornecimento, representando cerca de 20 gigawatts (GW) energia produzida. Colocando em uma perspectiva, a rede elétrica dos EUA gera 1.000 GW para atendimento às suas necessidades – a cidade de Nova Iorque sozinha consome 10 GW. Claramente, devemos considerar a implementação de microrredes com segurança cibernética com maior rapidez.

Enquanto isso, um incidente após outro coloca em evidência a urgência de riscos de segurança cibernética. Em Dezembro de 2015, um ataque na Ucrânia deixou 225.000 pessoas sem fornecimento de energia por diversas horas, evidenciando a vulnerabilidade das redes, não somente naquele país mas em todo o mundo desenvolvido. Três concessionárias foram invadidas, possivelmente por alguma nação inimiga ou por agências de espionagem governamentais, como a "Sandworm" ou a "Electrum". Os apagões foram causados por invasões cibernéticas remotas coordenadas, "provavelmente após um extenso reconhecimento das redes-vítima", conforme relatório do Departamento de Segurança Doméstica dos EUA. A rede ucraniana foi novamente atacada em Dezembro de 2016. Desta vez somente uma única subestação foi comprometida. O evento, contudo, foi preocupante porque os invasores usaram uma sofisticada arma cibernética denominada "Crash Override", que pode ser facilmente modificada para atacar uma extensa gama de instalações industriais em todo o mundo.

Mais recentemente, constatamos que não são somente os códigos computacionais que tornam uma infraestrutura vulnerável. Na verdade, os hackers contam com um espaço de manobra bem mais amplo. Por exemplo, em Dallas, Texas, as 156 sirenes de alerta de tornados foram acionadas de forma simultânea e não-esperada em Abril, quando os hackers manipularam códigos tonais, não códigos computacionais, em um sistema rádio com 10 anos em operação. Por 90 minutos – até que os operadores as desligassem todas manualmente – as sirenes ecoaram um alarme inconfundível, jogando os holofotes sobre o estado exposto de nossa infraestrutura crítica.

Ficou claro também que os terroristas cibernéticos podem contar com o comportamento humano para, de forma inadvertida, obter apoio e instigar suas intenções destrutivas. O ataque de ransomware "WannaCry", que afetou 200.000 sistemas em 150 países em 12 de Maio de 2017, em grande parte ocorreu porque os usuários de computadores falharam em seguir práticas adequadas de higienização em seus computadores, dizem especialistas em segurança. Ao negligenciar a atualização de softwares Microsoft corriqueiros, que têm patches de segurança regularmente oferecidos, eles deixaram a porta aberta para o malware.

Soluções de segurança cibernética nem sempre são tão simples como a instalação de atualizações de software. As concessionárias de energia e os especialistas em segurança se preocupam com a possibilidade de códigos maliciosos assumirem o controle da rede elétrica da América do Norte. Essa complexa rede elétrica inclui equipamentos de muitas partes do mundo; o temor é que alguns destes componentes possam conter bombas-relógio na forma de vírus ou malwares programados por nações inimigas para sabotar a rede em questão de tempo.

Devido à urgência da situação, a Microgrid Knowledge, em parceria com a S&C Electric Company, preparou este guia, "Segurança cibernética de Microrredes: Protegendo e Construindo a Rede do Futuro". Oferecemos este guia para download gratuito e encorajamos os leitores a compartilhar o link deste guia de forma ampla. Neste guia, nós explicamos como as microrredes em geral, e microrredes com segurança cibernética em particular, oferecem proteção durante um ataque cibernético em uma infraestrutura elétrica.

Três exemplos de segurança cibernética em microrredes

A arquitetura distribuída é o cerne da segurança cibernética de microrredes, oferecendo três formas de proteção.

Primeira forma: os sistemas distribuídos são mais difíceis de sofrer ataques em massa pelos terroristas cibernéticos do que os sistemas centralizados com um único ponto de falha – uma característica da rede dos EUA. As microrredes usam recursos distribuídos de energia – diversos e diferentes pontos de geração – e são inerentemente segmentadas da macrorrede. Elas podem também ser novamente segmentadas em sub-redes que podem operar de forma autônoma ou em conjunto e ser isoladas uma da outra e da macrorrede no caso de um ataque cibernético. Para invadir uma microrrede, os atacantes devem descobrir e comprometer múltiplos pontos não-conectados. Não há um só centro de alvo vulnerável.

Na segunda forma, as microrredes oferecem redundâncias inerentes. Na falha de uma fonte, outra toma seu lugar. Por exemplo, se o software de gerenciamento de um painel solar é atacado, a microrrede pode ainda gerar energia por outras fontes, como armazenamento de energia ou cogeração térmica.

Na terceira forma – ponto central deste relatório – uma nova e avançada estirpe de microrrede, a microrrede com segurança cibernética, eleva a proteção cibernética e a resiliência de energia a um outro nível. Ela faz isso pela incorporação do conceito de ativos distribuídos na inteligência do software que gerencia a microrrede. Em vez de ter um único sistema mestre de controle, ou "cérebro", a microrrede com segurança cibernética possui vários. Se houver invasão da microrrede que desabilite um controlador, outro controlador automaticamente assume o gerenciamento do sistema. Isso dá tempo aos operadores das microrredes com segurança cibernética para isolar a falha sem interromper o fornecimento a instalações críticas e aos equipamentos servidos pela microrrede.

Para uma plena percepção do valor da segurança cibernética de microrredes, é necessário primeiro compreender a arquitetura centralizada com a qual as redes de maior porte foram construídas por um século. Isso torna claro a razão do medo existente de que um ataque cibernético estratégico possa derrubar a rede, especialmente quando estamos entrando na era da "Internet das Coisas", explanada no próximo capítulo.

Capítulo 2: Ataque Cibernéticos na Rede: Até que Ponto Nosso Sistema é Vulnerável?

A rede elétrica dos EUA foi descrita como uma única e enorme máquina, uma das maiores do planeta, com cerca de 1.000 GW de geração e 200.000 milhas de linhas de transmissão.

É uma máquina única no sentido de que todas as suas partes devem trabalhar em conjunto. Se ocorrer uma falta dentro de qualquer de suas redes semiautônomas, as falhas podem se propagar para o restante do sistema. O sistema é construído para ser resiliente e não ser afetado pelas faltas – até um certo ponto.

A vulnerabilidade da rede foi demonstrada em uma larga escala em 2003, quando uma linha de transmissão sobrecarregada tocou uma árvore ao sul de Cleveland, Ohio. Em poucos minutos, uma combinação de falhas em equipamentos e erro humano deixou 50 milhões de pessoas sem fornecimento de energia, com um prejuízo estimado em 6 bilhões de dólares.

Como consequência daquele apagão, as regras de confiabilidade foram reforçadas, e a rede está hoje em melhor posição para evitar ou suportar uma repetição do que ocorreu em 2003. Infelizmente, porém, o escopo das ameaças cresceu desde então. A possibilidade de apagões resultantes de ataques cibernéticos aumentou, com o potencial de causar mais estragos que tormentas ou acidentes.

A preocupação acerca da segurança da rede aumentou com os relatos de intrusões cibernéticas em redes comerciais de computadores em uma larga faixa de empresas. Houve diversos ataques de muita repercussão em anos recentes, incluindo o sequestro de dados sensíveis da Sony Pictures em 2014, a quebra das defesas digitais da J.C. Penney e da Yahoo! e os ataques cibernéticos bem sucedidos a redes da Ucrânia em 2015 e novamente em 2016 e 2017. Até o momento, a rede elétrica dos EUA não foi ainda invadida por hackers, mas não foi por falta de tentativas. Muitos consideram que é apenas uma questão de tempo para que isso ocorra.

Em Dezembro de 2016, o *Wall Street Journal* noticiou que oficiais americanos acreditavam que um ataque cibernético em 2017 contra a indústria de energia dos EUA resultou em pelo menos 17 companhias sendo invadidas, incluindo quatro concessionárias. Um estudo da Cisco revelou que 70 por cento dos profissionais de segurança de empresas elétricas informaram ter experimentado pelo menos uma violação na segurança.

Ataques cibernéticos em redes não são mais uma preocupação teórica

Em um artigo de Abril de 2017, o Conselho de Relações Exteriores afirmou que os ataques cibernéticos a redes não são mais uma questão teórica, e que a rápida digitalização, baixos investimentos em segurança cibernética e uma fraca regulação tornam o país ainda mais vulnerável.

Não bastasse a vulnerabilidade da rede em sua situação atual, ela está se tornando mais susceptível a ataques à medida em que ocorre a expansão de redes usuárias de energia, como cidades e casas inteligentes, que incorporam energia distribuída, veículos elétricos e aparelhos com Internet das Coisas (IoT), que incluem tudo, desde laptops e câmeras a telefones celulares, iluminação pública e pendrives. Um mundo com dispositivos interconectados deixa a vida mais conveniente, porém todos esses dispositivos dependem de um número rapidamente crescente de interfaces digitais de interconexão. Essas interfaces se constituem em pontos potenciais para a entrada de ataques cibernéticos de todas as formas.

Esta ameaça crescente chamou a atenção da indústria fornecedora para as concessionárias. O Edison Electric Institute (EEI), uma entidade mantida por concessionárias de energia, promoveu diversas iniciativas objetivando a salvaguarda da rede contra ameaças cibernéticas e está mantendo parcerias com agências federais para aprimorar a resiliência contra ataques cibernéticos. O EEI também colabora com o NIST – National Institute of Standards and Technology, com o NERC – North American Electric Reliability Corp. e com as agências federais jurídicas e de inteligência para aprimorar as capacidades da rede.

O Departamento de Energia dos EUA (DoE) está também destinando um fundo de 15 milhões de dólares para suporte aos esforços da American Public Power Association e da National Rural Electric Cooperative Association (NRECA), duas entidades que representam concessionárias de energia municipais, cooperativas e outras concessionárias públicas. As associações estão usando os fundos para fortalecer a segurança cibernética de seus membros, muitos deles pequenas concessionárias locais sem recursos adequados para gerenciar ameaças cibernéticas por si só.

Os militares se preparam para ataques cibernéticos a redes com microrredes

Há uma conscientização apurada entre os militares dos EUA em relação a ameaças impostas por ataques cibernéticos. Isso levou os líderes militares a adotar as microrredes como uma forma de reduzir a dependência da rede das concessionárias em missões críticas e sobretudo em combustíveis fósseis.

No entanto, os objetivos de resiliência de energia destas microrredes não podem ser determinados se as microrredes acidentalmente deixarem suas instalações expostas a ataques cibernéticos. Por isso, o Departamento de Defesa (DoD) dos EUA estabeleceu estritos requisitos de segurança para instalações militares, incluindo microrredes; elas devem ser bem menos vulneráveis a ataques cibernéticos que as redes das concessionárias.

Com esses objetivos em mente, em 2008 o DoD lançou o programa Smart Power Infrastructure Demonstration for Energy Reliability and Security (SPIDERS). O programa foi concebido para reforçar a segurança cibernética e a eficiência energética das instalações militares norteamericanas pela implantação de microrredes avançadas, e para transferir este conhecimento a infraestruturas não-militares críticas.

O SPIDERS incluiu três fases de projeto abrangendo garantias de segurança aprimoradas em instalações militares, integrando tecnologias de rede inteligente, geração de energia distribuída e renovável e armazenamento de energia com arquitetura de microrrede com segurança cibernética. Até o momento, o DoD já implantou mais de doze microrredes em locais que incluem Joint Base Pearl Harbor-Hickam no Havaí, Camp Pendleton na Califórnia, Fort Carson no Colorado e Fort Belvoir na Virgínia.

A microrrede em Camp Smith no Havaí, que fornece energia para a totalidade das operações da base durante interrupções de fornecimento mais prolongadas, é um exemplo de uma microrrede com defesas contra ataques cibernéticos inseridas no sistema de controle. Como será visto no próximo capítulo, essas defesas são cruciais para assegurar que a microrrede em si não se torne um portal para ataques cibernéticos.

Então, como exatamente uma microrrede pode assegurar a continuidade de fornecimento durante uma invasão cibernética? O Capítulo 3 explica.

Capítulo 3: A Segurança Cibernética – Valor do Ilhamento de Microrredes

O valor das microrredes como medida defensiva de segurança cibernética começa com sua habilidade única em operar em dois diferentes modos: conectado à rede elétrica ou ilhada, como um sistema autocontido e como um provedor independente de energia.

No geral, uma microrrede opera no modo conectado à rede, com seus recursos contribuindo para o fortalecimento de toda a rede. Porém, se uma falta na rede da concessionária causar uma interrupção de fornecimento, a microrrede pode se desconectar da rede e atender individualmente seus consumidores com seus recursos de geração próprios. Esta capacidade de ilhamento faz com que as microrredes sejam muito convenientes em operações críticas, como equipes de atendimento a emergências, operações militares, hospitais, aeroportos e estações de tratamento de água.

O ilhamento de uma microrrede ocorre se uma invasão de terroristas cibernéticos invade uma rede elétrica e causa uma grande falha de fornecimento. Ao sentir a ruptura, as fontes de geração local e as cargas desta microrrede são isoladas da falha pela tecnologia de

software. Estes recursos de geração locais dentro da área de abrangência da microrrede são ativados e passam a fornecer energia para os consumidores da microrrede. Essas fontes de geração geralmente consistem de uma combinação de energias renováveis, baterias, cogeração termoelétrica e geradores de emergência.

Não há exemplos de ilhamento de microrredes nos EUA durante um ataque cibernético porque – felizmente – a rede nunca sofreu um ataque hacker. Entretanto, as microrredes puderam demonstrar o valor do ilhamento durante outras grandes catástrofes.

Por exemplo, em 2012, quando o Furacão Sandy atingiu o litoral de Nova Jersey e devastou a Costa Leste, deixando 8 milhões de consumidores sem energia, as luzes continuaram acesas na Universidade de Princeton devido ao ilhamento de sua microrrede.

A microrrede operou até o restabelecimento de energia na rede principal – um dia e meio depois – suprindo as necessidades de energia e aquecimento. Devido à sua microrrede, Princeton se tornou um refúgio onde policiais, bombeiros, paramédicos e trabalhadores de outros serviços de emergência puderam carregar seus celulares e equipamentos. A população local foi também convidada a usufruir do aquecimento, recarregar as baterias dos telefones e usar serviços de Internet sem fio disponibilizado pelo centro de hospitalidade da universidade.

Não são somente furacões e ataques cibernéticos que ameaçam a rede elétrica. Muitas interrupções de fornecimento são causadas por causas mais corriqueiras como temporais, tempestades de neve e afundamentos de tensão. Individualmente ou em conjunto, essas perturbações podem afetar o consumidor de forma significativa. Num exemplo, uma microrrede na Califórnia alimentou Borrego Springs por nove horas depois que uma linha de transmissão foi danificada por raios. Mais uma vez, o ilhamento de microrredes provou ser uma forma de assegurar o fornecimento.

Microrredes aninhadas sendo desenvolvidos em Chicago, Nova York e Pittsburgh, entre outros locais

Há alguns exemplos de microrredes exibindo a capacidade de prover alimentação de emergência, resiliência e redundância. Trata-se, nestes casos, de redes autônomas. Oferecendo ainda mais possibilidades estão as microrredes interconectadas, ou “aninhadas” com outras microrredes próximas.

Ainda uma abordagem nascente – porém oferecendo uma oportunidade superior para a resiliência (o objetivo principal da segurança cibernética) – as microrredes aninhadas são eletricamente interconectadas, permitindo intercâmbio de energia. Elas podem compartilhar fontes geradoras e chavear entre elas para assegurar uma eficiência otimizada. Por exemplo, uma microrrede com painéis solares pode suprir a carga em um dia ensolarado, enquanto uma microrrede próxima com cogeração termoelétrica pode assumir o fornecimento em um dia tempestuoso.

Resiliência, um benefício muitas vezes associado com microrredes, descreve a capacidade de evitar perdas de fornecimento ou de recompor o serviço mais rapidamente após um desastre.

Em Chicago, a Commonwealth Edison propôs uma microrrede em Bronzeville. Quando concluída, ela irá proporcionar resiliência e segurança para a população local, bem como para o hospital e para as sedes da polícia e dos bombeiros. A microrrede de Bronzeville poderá também se aninhar com uma microrrede existente no Instituto de Tecnologia de Illinois, em operação desde 2013.

Em Nova Iorque, a cidade de New Paltz propôs uma microrrede modular de 12 milhões de dólares compreendendo 10 zonas ou nós independentes, cada uma contando com seus próprios recursos de geração para atendimento a uma ou mais instalações críticas. No total, a rede aninhada de New Paltz deverá atender a 25 instalações críticas.

É fato que as microrredes oferecem proteção durante um ataque cibernético devido a sua capacidade de ilhamento, em essência criando uma separação entre os sistemas elétricos sob ataque e os recursos inerentes das microrredes. Entretanto, as microrredes também são construídas com base em software e comunicação de dados, e se as microrredes são destinadas a proteção da rede da concessionária contra o risco de ataques cibernéticos, é essencial que a própria microrrede também seja protegida contra esses ataques.

Projetando um microrrede com real segurança cibernética real

Nesse aspecto, é necessário reconhecer que os mesmos elementos que fazem uma microrrede resiliente podem ser os mesmos que a tornam vulnerável. As microrredes geralmente incluem recursos distribuídos de energia, como painéis solares, que requerem inversores para a alimentação

dos consumidores ou para enviar à rede. Uma das funcionalidades-chave de uma microrrede, na verdade, é a comunicação bidirecional de dados entre os participantes da microrrede e destes com a rede à qual são conectados.

Essas funções de controle e comunicação podem criar vulnerabilidades pelo aumento da superfície de ataque – essencialmente apresentando portais aos invasores cibernéticos – e enfraquecendo a resiliência que uma microrrede deve prover.

Uma microrrede invadida por hackers pode até mesmo ser um portal que expõe a própria rede a ataques cibernéticos. No mínimo, construir uma rede sem segurança cibernética é um investimento ruim. No pior dos casos, uma catástrofe pode ser precipitada ou agravada.

É importante salientar, porém, que uma microrrede com segurança cibernética efetiva supera estas vulnerabilidades. Quais seriam as premissas de projeto de uma microrrede para se obter essa condição? Este é o tema do próximo capítulo.

Capítulo 4: Como Criar uma Microrrede com Segurança Cibernética e Também Proteger a Macrorrede

A segurança cibernética deve ser a consideração primordial já no início do projeto de uma microrrede. Se uma microrrede for instalada para ser resiliente, não faz sentido que ela apresente maior vulnerabilidade a seus consumidores ou à macrorrede.

Na comparação com o modo centralizado amplamente usado em redes primárias, as microrredes usam uma arquitetura distribuída em múltiplos sistemas que se comunicam entre si. Intrinsecamente, esta arquitetura distribuída inclui redundância de geradores e resiliência. Os controles da microrrede também proveem um nível básico de segurança porque são distribuídos, sem um único ponto de falha sequer que poderia resultar na perda de todo o sistema. Conforme já citado, as microrredes avançadas são capazes de compensar perdas em um ou mais pontos controlados.

Uma microrrede com um projeto avançado inclui dispositivos de manobra, fontes de geração, armazenamento de energia e outros equipamentos que se comunicam de forma harmoniosa usando um software de supervisão e controle. O controlador é o sistema nervoso e o cérebro de uma microrrede. Seu software coleta um grande número de dados dos participantes da microrrede, toma decisões operacionais e de segurança e comunica essas decisões à microrrede, repassando instruções aos equipamentos conectados. O controlador também coordena e gerencia seus recursos e as relações com a rede central para operar com eficiência máxima o tempo todo.

Enquanto os diferentes recursos de uma microrrede aumentam sua resiliência, os complexos sistemas de controle e comunicação necessários para a coordenação têm também o potencial de aumentar sua vulnerabilidade – se uma segurança cibernética adequada não for implementada. Para uma resiliência efetiva, as proteções de segurança cibernética devem ser implementadas na microrrede já na sua concepção inicial.

Resiliência obtida pela segurança cibernética

"A segurança cibernética efetiva de microrredes requer que não haja um único ponto de falha no sistema, como na arquitetura centralizada", diz Erik Svanholm, CEO da IPERC, uma subsidiária da S&C Electric, que oferece um controlador para microrredes com segurança cibernética, o Sistema de Controle de Microrredes GridMaster®. "A resiliência é obtida pela transferência da "mestra" de um controlador distribuído para outra. A incorporação de inteligência e poder de processamento em pontos extremos possibilita comunicação e controle de forma localizada, o que significa segurança e monitoração em uma área de rede menor".

Svanholm descreve uma abordagem "Defense in Depth" (DiD) (Defesa em Profundidade), que demanda o emprego de um grande número de contramedidas de segurança, todas trabalhando em conjunto de uma forma coerente numa estrutura em camadas, para proteção contra qualquer forma de ataque cibernético imaginável, ao mesmo tempo que possibilita que as comunicações na microrrede e as atividades de manipulação de dados prossigam sem sobressaltos.

A primeira linha de defesa ocorre no perímetro da microrrede, com o objetivo de repelir completamente qualquer ataque. Para isso, um bom começo seria algo simples, como o uso de sensores que registram e emitem alertas se os equipamentos da microrrede sofrerem alguma interferência. Sistemas de detecção de invasão e firewalls também podem ajudar a manter os intrusos de fora e identificar tentativas (e sucessos) de penetrar no perímetro da rede. Ações em nível de hardware, como a remoção de softwares e serviços desnecessários, e desabilitação de comunicações e portas de dados (particularmente portas USB) não-utilizadas, nos computadores com o software de controle, possibilitam uma outra camada de segurança do perímetro.

É aí que a segurança é comprometida na maioria dos sistemas de controle industriais legados e em muitos sistemas de controle de microrredes atuais. Se os atacantes penetram a camada perimetral da rede, eles ganham acesso a fluxos de dados e arquivos expostos e legíveis, podendo desenvolver e implantar códigos maliciosos devastadores.

Os protocolos industriais padrão para o setor de energia não foram escritos pensando na segurança cibernética, e a grande maioria deles transmite dados a descoberto. Muitas outras camadas de defesa devem ser colocadas no sistema, com isso nem tudo se perde se o perímetro da rede é invadido. Se estas medidas de segurança não forem incluídas no DNA original do código de controle, é quase impossível acrescentá-las posteriormente sem uma reengenharia significativa do software e sem testes de interoperabilidade com os participantes da microrrede, incluindo os sistemas da concessionárias. Isso coloca os operadores de grandes e caros sistemas de controle industriais diante de uma escolha desagradável: eles podem aplicar proteções externas modernas nos velhos softwares expostos e esperar que eles nunca sejam invadidos – uma solução barata, porém de alto risco – ou substituir todo o sistema de controle por um produto novo e muito mais seguro.

Em contraste, os atacantes que conseguem êxito na invasão de sofisticados sistemas de controle que usam uma abordagem DiD se deparam com um grande número de defesas integradas que os impede de realizar estragos mesmo quando a invasão já ocorreu. Há um reforço em software, firmware e nos sistemas operacionais, obtido pela desabilitação ou remoção de códigos, protocolos e serviços que não são necessários especificamente para a operação da microrrede. É usada criptografia nos dados armazenados e nas comunicações entre os componentes de microrrede, e com isso os invasores não podem ler, interceptar ou manipular o tráfego de controle, configurações e arquivos. O Whitelisting é um protocolo de segurança em que o acesso ao sistema somente é permitido a dispositivos pré-aprovados. Mesmo que um novo dispositivo apareça em uma microrrede com proteção DiD e passe no teste da lista branca, o software ainda executa diversos exercícios de autenticação para validar se aquele dispositivo tentando comunicação com a microrrede é um participante legítimo.

Uma microrrede com segurança cibernética também monitora as comunicações internas e os processos sistêmicos para identificar eventos anormais durante as operações. Isso inclui alertas em tempo real e a criação de registros de auditoria de segurança, que emitem alertas ao operador sobre a postura de segurança do sistema, seu nível de disponibilidade e anomalias potenciais, tudo sem afetar a operação da microrrede. Esses alertas e registros de auditoria também podem ser incorporados em um sistema de Gerenciamento de Informações de Segurança e de Eventos (SIEM).

As conexões da microrrede com a rede da concessionária requerem gateways de segurança adicionais, ou zonas desmilitarizadas (DMZs), e firewalls dedicados à segurança daquele ponto de conexão. Onde for possível, os gateways unidirecionais (por exemplo, diodos de dados) podem ser usados onde a comunicação bidirecional não for necessária. A conexão direta entre uma microrrede e a concessionária ou com a Internet nunca deve ser usada.

Não há atalhos para a segurança cibernética

Todos esses métodos são apenas exemplos de diversas contramedidas usadas em sistemas de controle baseados na abordagem DiD para estabelecer uma segurança cibernética forte em microrredes avançadas. A maioria das abordagens de defesa usadas são bem conhecidas nos círculos de segurança e são largamente usadas em muitas aplicações. No entanto, implantar um grande número de proteções de forma simultânea e coerente, tornando o sistema praticamente hermético, exceto para os movimentos precisos de dados necessários para o funcionamento da microrrede, é algo extremamente difícil de conseguir e leva anos para o desenvolvimento do software e do hardware. Não existe atalho para uma segurança cibernética efetiva.

"Um desafio significativo para as concessionárias é que muitas não possuem recursos orçamentários específicos para a segurança cibernética. Por isso muitas recorrem à abordagem pragmática 'se não quebrar, não precisa consertar'" diz David Chiesa, diretor geral de desenvolvimento de negócios da S&C Electric Company. "Eles estão gerenciando sistemas previstos para permanecer operando por décadas, não anos. E requerem uma solução cibernética que possa ser integrada em um novo sistema, porém que possa operar também em sistemas legados".

É importante que as concessionárias – e outras entidades – estejam cientes que os casos de negócios, em termos de segurança cibernética, e para as próprias microrredes, diferem da infraestrutura padrão de energia que elas possuem.

"Os custos para assegurar a segurança cibernética devem ser encarados como uma forma de seguro. Da mesma forma que as microrredes protegem contra distúrbios na rede da concessionária, a segurança cibernética atua como um seguro para a operação segura e confiável das microrredes", diz Chiesa.

"A existência de sistemas com uma robusta segurança cibernética pavimenta o caminho para a proliferação de microrredes que aprimoram e reforçam a rede frente a perigos, tanto naturais como originados pelo homem".

As microrredes com segurança cibernética atuais foram fruto de muitos anos de trabalho na esfera militar. No próximo capítulo, nós entrevistamos um dos atores fundamentais por trás deste desenvolvimento.

Capítulo 5: Segurança Cibernética de Microrredes: Uma Guerra Desigual

É comum encontrar sementes de avançadas tecnologias dentro do trabalho dos militares. A segurança cibernética de microrredes não é uma exceção, como veremos nesta entrevista com Darrell Massie, que possui doutorado em engenharia civil e é o fundador e diretor de tecnologia da Intelligent Power & Energy Research Corporation (IPERC), uma subsidiária da S&C Electric Company.

A ameaça de ataques cibernéticos tendo como alvo a rede elétrica dos EUA está crescendo, com os hackers se tornando cada vez mais sofisticados. No início, os hackers faziam invasões de sistemas por esporte, para se tornar conhecidos e para testar suas habilidades. Depois eles passaram cada vez mais a capturar informações pessoais e bancárias visando ganhos financeiros. Mais recentemente, governos estrangeiros tem sido os responsáveis por um crescente número de ataques cibernéticos. O *Wall Street Journal* noticiou recentemente que o software malicioso que derrubou o fornecimento de energia em partes da capital da Ucrânia ano passado poderia ser redirecionado para a rede dos EUA.

"Nas mãos de nossos inimigos, os ataques cibernéticos podem ser uma arma devastadora contra os Estados Unidos. Os ataques cibernéticos estão sendo atualmente utilizados como uma nova forma de terrorismo e de uma guerra desigual", disse Massie. "O ataque cibernético na Ucrânia foi uma amostra espetacular dos danos que os atacantes cibernéticos são capazes de conseguir atualmente. O ataque foi focado não só para chamar a atenção do público sobre a vulnerabilidade da rede elétrica, como também tendo como alvo o alto valor da rede".

Essa ameaça é reconhecida pelos altos executivos das concessionárias, porém muitos relutam em admitir publicamente esses problemas. Essa atitude está mudando, na medida em que as agências reguladoras e as próprias concessionárias começam a demandar níveis maiores de segurança cibernética. A indústria também está percebendo a ruptura em massa e as repercussões econômicas que podem resultar de um ataque cibernético em estilo ucraniano na rede dos EUA. Um relatório de 2015, divulgado pela companhia de seguros Lloyd's de Londres, estimou que, se um ataque cibernético mergulhasse a Costa Leste dos EUA na escuridão, o impacto econômico poderia chegar a 1 trilhão de dólares.

O ataque na Ucrânia deu margem a lições valiosas, conforme Massie. A concessionária invadida tinha publicado uma relação dos fabricantes de seus equipamentos, o que permitiu aos hackers determinar as especificações-chave dos componentes instalados na rede. Os hackers então sequestraram arquivos corriqueiros da Microsoft para obter o controle sobre os sistemas de controle industriais da concessionária. Com os sistemas já invadidos, eles usaram as informações dos fabricantes que tinham sido disponibilizadas ao público para reescrever o software de controle de modo a alterar as configurações dos dispositivos, enquanto as telas de interface dos usuários, visualizadas pelos operadores da concessionária, continuavam mostrando status normal.

A segurança da arquitetura distribuída

O ataque na Ucrânia evidenciou um conceito básico de segurança cibernética. "Um invasor escolhe o alvo mais fácil. Um sistema centralizado pode ser facilmente invadido em uma tempestade", disse Massie.

Uma das soluções é caminhar no sentido de uma arquitetura mais distribuída. Porém muitas microrredes existentes não fizeram isso, portanto elas não tem necessariamente segurança cibernética, de acordo com Massie.

"A maioria dos sistemas de controle em uso atualmente foram projetados bem antes que a segurança cibernética se tornasse uma preocupação, portanto não contendo funcionalidades de segurança. A tática comum usada, numa tentativa de obter segurança em sistemas de controle existentes, é simplesmente instalar firewalls na periferia do sistema. Este é o equivalente eletrônico ao Band-Aid", disse Massie. "Qualquer firewall pode ser violado. No entanto, os sistemas de controle precisam continuar operando, mesmo com o invasor dentro. Nós testamos e operamos nossos sistemas de controle dentro desta premissa".

A microrrede com segurança cibernética é governada não por um único controlador mestre central, mas sim por diversos controladores interconectados. Se um controlador ficar comprometido por uma razão qualquer, ele pode ser sequestrado e outro assume suas tarefas. Há backup do backup.

Em contraste, se uma microrrede depende de um único controlador central, se ele sofrer uma falha todo o sistema é paralisado.

"Quase todo sistema de controle do mercado possui um ponto de controle central. Nosso Controlador GridMaster é diferente por ser distribuído. Se algum hacker derrubar um controlador, outro assume," diz Massie.

A abordagem de controle distribuído remonta às origens do IPERC. Massie serviu no exército dos EUA por 27 anos, e um dos desafios que enfrentou foi providenciar fornecimento de energia elétrica em lugares como Bósnia, Irã e Iraque. Na implantação destes sistemas havia uma exigência adicional: eles deveriam ter condições de ser mudados de local a qualquer hora e até mesmo subdivididos em locais diferentes. Isso levou Massie a imaginar como esses sistemas poderiam ser "dinamicamente reconfigurados", de forma a obter o restabelecimento do serviço numa simplicidade do tipo "plug-and-play".

Após anos trabalhando nestas questões tecnológicas, Massie concluiu que a resposta requeria uma reformulação da arquitetura de software da microrrede. Um único controlador central não seria factível, porém uma estratégia de controle distribuído, uma questão de aumento no número, sim.
Além disso, as funcionalidades de resiliência inerente e a segurança cibernética de um sistema de controle distribuído poderiam ser um atrativo para a instalação de microrredes permanentes, da mesma forma como eram para as unidades móveis de campo.
Massie adotou este conceito e fez dele a base do IPERC. Em 2007, percebendo a ameaça crescente dos ataques cibernéticos, o IPERC iniciou o desenvolvimento e os testes de sistemas de controle distribuídos já com a segurança cibernética agregada.

O IPERC já estava, portanto, preparado quando o Departamento de Defensa solicitou propostas para seu programa de segurança cibernética de microrredes trifásicas em seu programa SPIDERS.
O sistema de controle do IPERC foi selecionado para todas as três fases do projeto, e a empresa liderou o desenvolvimento dos controladores, comunicações e segurança cibernética até o final.

Pelos cinco ou seis anos seguintes do programa, o IPERC aprimorou seu controlador para a microrrede com segurança cibernética com o financiamento específico do Departamento de Defensa, do Departamento de Energia e Departamento de Segurança Interna.

"Nós passamos em todos os testes de segurança que o DoD aplicou no nosso sistema de controle, porque nós embutimos nele nossa arquitetura de segurança cibernética desde o início", diz Massie.

Designação militar exclusiva do controlador GridMaster

O controlador de microrrede GridMaster do IPERC é o único do mercado que recebeu, duas vezes até agora, a respeitada "Autorização para Operar", ou "ATO", emitida pelos militares, que valida a postura de segurança do sistema e autoriza seu uso contínuo de forma geral em instalações militares. As ATOs foram concedidas após demonstração da implementação de segurança usando o Risk Management Framework (RMF) do DoD e mediante testes rigorosos realizados por diversas equipes de segurança cibernética do DoD.

O que há pela frente? Massie prevê futuros controles da microrrede reparando a si próprios de forma autônoma e se adaptando a comunicações inesperadas ou mudanças de configuração. Somente um sistema composto por controladores distribuídos tem a capacidade de atingir esta classe de recuperação automática da microrrede.

À medida que as ameaças à rede aumentam, as microrredes com segurança cibernética apresentam um método que assegura a continuidade do fluxo de fornecimento, iniciando pela infraestrutura crítica, como serviços de primeiros socorros, hospitais, abastecimento de alimentos e água e comunicações. A implantação de microrredes suficientes para atender a essa necessidades em todo o país passará por um longo caminho. É tempo de agir.

Capítulo 6

Estudo de Caso: Primeiro Controlador de Microrrede com Segurança Cibernética Instalado por uma Concessionária do Centro-Oeste dos EUA

Um projeto-teste de 1,475 MW está sendo descrito por uma concessionária do centro-oeste dos EUA e uma parceira-chave como uma das microrredes mais avançadas tecnologicamente em nível de concessionárias na América do Norte. Além dos controles avançados, a microrrede inclui energia eólica, energia solar, geração com gás natural e armazenamento de energia.

A implantação da microrrede ocorre num tempo em que aumenta a preocupação mundial com invasões de sistemas, motivada por um ataque de ransomware em Maio de 2017 que se espalhou por 150 países, infectando centenas de milhares de empresas e instituições, desde hospitais na Inglaterra ao FedEx nos EUA e montadoras de veículos na França.

"Pioneirismos" da Microrrede

Além de contar com o primeiro (e ainda o único) controlador de microrrede a receber um ATO da DoD, esta é a primeira microrrede de uma concessionária a incluir um avançado controlador de microrrede com segurança cibernética, fabricado pela S&C Electric Company através de sua subsidiária IPERC.

A microrrede incorpora duas tecnologias "pioneiras" adicionais, de acordo com a S&C, que foi responsável pela engenharia, aquisições, construção e comissionamento:

1. A instalação marca a primeira vez que uma microrrede atende cargas de consumidores em um alimentador de distribuição de uma concessionária na América do Norte. A geração na microrrede pode operar em modo ilhado para servir somente os consumidores locais, ou pode operar integrada à rede para prover serviços auxiliares a ela.
2. É a única microrrede conhecida de uma concessionária no país capaz de fazer uma transição sem problemas de fontes de geração de um circuito de distribuição completo da microrrede para a rede, de acordo com Chiesa da S&C. Isso evita as interrupções de fornecimento normalmente curtas quando a microrrede realiza a manobra entre a condição integrada à rede e o modo ilhado.

Esta microrrede é também uma das poucas no mundo a operar nas tensões típicas das concessionárias, entre 4 kV e 34,5 kV, com múltiplos níveis de controle, de acordo com a concessionária. A microrrede está sendo usada pela concessionária para testar métodos de monitoramento e controle de agregação de energia limpa com automação avançada e armazenamento com baterias.

Escrito pela Equipe de Editoração da Microgrid Knowledge,

Sobre a S&C Electric Company

A S&C, com sede mundial em Chicago, EUA, aplica sua tradição em inovação para endereçar os desafios encontrados nas redes mundiais de energia, desta forma modelando o futuro do fornecimento confiável de eletricidade. A missão da S&C, uma empresa pertencente a seus funcionários, é o desenvolvimento contínuo de novas soluções para o fornecimento de eletricidade, promovendo melhoras de eficiência e confiabilidade requeridas para a rede inteligente. Mais informações sobre a S&C estão disponíveis em www.sandc.com.

Fale conosco:

S&C Electric Company