Interrupção de Energia Induzida por Ataque Cibernético na Ucrânia: Análise e Estratégias Práticas de Mitigação

David E. Whitehead, Kevin Owens, Dennis Gammel e Jess Smith
Schweitzer Engineering Laboratories, Inc.

A edição revisada anterior foi lançada em outubro de 2016

Originalmente apresentado na
43rd Annual Western Protective Relay Conference, outubro de 2016

Traduzido para o português em fevereiro de 2017

Interrupção de Energia Induzida por Ataque Cibernético na Ucrânia: Análise e Estratégias Práticas de Mitigação

David E. Whitehead, Kevin Owens, Dennis Gammel e Jess Smith
Schweitzer Engineering Laboratories, Inc.

***Sumário*—Em 23 de dezembro de 2015, um "mau funcionamento temporário do sistema elétrico" em três províncias da Ucrânia resultou em interrupções de energia que duraram até seis horas e afetaram 225000 consumidores. Após o evento, uma investigação identificou evidências de que vários sistemas de controle de energia regionais da Ucrânia tinham sido comprometidos por ataques cibernéticos. Este foi o primeiro ataque cibernético efetuado com sucesso ao sistema de controle de uma concessionária de energia elétrica que foi publicamente documentado. Concessionárias e industrias ao redor do mundo estão agora questionando: "O que aconteceu e é possível acontecer um ataque cibernético similar em nossos sistemas de controle?"**

Este artigo fornece uma análise do ataque cibernético da Ucrânia, incluindo como os *hackers* obtiveram acesso ao sistema de controle, quais métodos usaram para explorar e mapear vulnerabilidades, uma descrição detalhada dos ataques de 23 de dezembro de 2015 e os métodos usados para apagar suas atividades e tornar mais difícil a correção dos problemas.

Em seguida, o trabalho apresenta uma descrição detalhada de abordagens de segurança para sistemas de controle do sistema de potência da concessionária baseados nas melhores práticas, incluindo o projeto de rede do sistema de controle, técnicas baseadas na lista branca ("whitelisting"), monitoramento e registros, além de treinamento das equipes de trabalho.

O artigo conclui apresentando uma discussão sobre os métodos de mitigação e recomendações que teriam protegido o sistema de controle da Ucrânia e alertado as equipes antes do ataque cibernético.

I. Introdução

Tendo início às 15h30 de 23 de dezembro de 2015, as IHMs dos centros de controle elétrico de *Kyiv*, *Prykarpattia* e *Chernivtsi* começaram a abrir e fechar disjuntores sem o comando dos operadores. As operações não autorizadas resultantes provocaram falta de energia para aproximadamente 225000 consumidores em toda a Ucrânia [1] [2]. Os operadores dos três centros de operação foram incapazes de recuperar o controle remoto das mais de 50 subestações afetadas pelo incidente. Depois de seis horas e da perda de mais de 130 MW de carga, os operadores restauraram a energia enviando técnicos para as subestações e controlando manualmente o sistema de potência [3] [4] [5].

Complicando a situação e reduzindo as comunicações dos operadores, os hackers também lançaram um ataque de negação de serviço baseado em telefonia, usando sistemas automáticos para sobrecarregar os serviços.

A análise efetuada após a interrupção de energia descobriu que o firmware foi corrompido nos conversores serial-para-Ethernet das subestações, as fontes de alimentação ininterruptas (UPS: "Uninterruptible Power Supplies") de ambos a sala do servidor e sistema de telefonia foram remotamente desligadas e os discos rígidos dos inúmeros computadores foram corrompidos.

Este evento foi a primeira interrupção de energia induzida por ataque cibernético bem-sucedido que desligou uma rede de energia elétrica. Para atenuar tentativas futuras de interrupção de energia elétrica através de ataques cibernéticos, é fundamental que outras empresas de energia elétrica aprendam com o incidente da Ucrânia.

Começamos na Seção II com uma explanação detalhada do ataque. A Seção III descreve um projeto bem conhecido para um sistema de controle seguro; e a Seção IV analisa um projeto bastante conhecido no contexto do incidente da Ucrânia.

Durante a elaboração deste artigo, usamos vários termos traduzidos do ucraniano. O primeiro é обленерго, "oblenergo", que é uma entidade de distribuição de energia regional. Ele pode ser combinado com uma região, tal como Київобленерго, "Kyivoblenergo", que é a entidade de distribuição para *Kyiv* e sua área adjacente. Um область, ou "oblast", é um condado ou região da Ucrânia. O *Ivano-Frankivsk Oblast*, que foi afetado no incidente, às vezes é também referido pelo seu nome tradicional de *Prykarpattia*. *Prykarpattia* e *Chernivtsi* estão localizados na Ucrânia Ocidental, enquanto *Kyiv* (a capital) está na Ucrânia Central (ver Fig. 1).

Fig. 1. Regiões Afetadas pela Interrupção de Energia Induzida por Ataque Cibernético na Ucrânia.

II. O Ataque Cibernético da Ucrânia

As informações apresentadas sobre as redes da Ucrânia e o ataque são provenientes de nossa pesquisa e relatórios públicos fornecidos pelo ICS-CERT ("Industrial Control Systems Cyber Emergency Response Team") do Departamento de Segurança Interna dos Estados Unidos [5]

[6], E-ISAC (“Electricity Information Sharing and Analysis Center”) [7] e pelo governo da Ucrânia [3].

A. Visão Geral do Ataque Cibernético

O ataque cibernético da Ucrânia foi direcionado a seis *oblenergos*, mas apenas três foram diretamente afetados pelas perdas de energia: *Kyiv*, *Prykarpattia* e *Chernivtsi* [1] [2] [5]. Os outros três *oblenergos* foram invadidos com sucesso, mas não foram submetidos a impactos operacionais [5]. Os ataques bem-sucedidos foram concentrados no nível de distribuição. Baseando-se nas informações disponíveis, concluiu-se que as seguintes etapas ocorreram durante a campanha de ataque.

1. Um ataque inicial via e-mail (“spear phishing”) instiga os destinatários a abrirem um documento Microsoft® anexado com um macro que instala Black Energy 3 (BE3) nas estações de trabalho corporativas.
2. BE3 e outras ferramentas executam o reconhecimento e o mapeamento da rede e fornecem um *backdoor* inicial para os *hackers* dentro da rede corporativa.
3. Como resultado do reconhecimento da rede, os agentes maliciosos descobrem e acessam os servidores Microsoft Active Directory® dos *oblenergos* que contêm as credenciais e contas dos usuários corporativos.
4. Com as credenciais coletadas, os agentes maliciosos usam um túnel criptografado de uma rede externa para entrar na rede do *oblenergo*, estabelecendo presença nas redes do sistema de controle do *oblenergo*.
5. Os agentes mal-intencionados descobrem e acessam os servidores das interfaces homem-máquina (IHMs) do sistema de controle supervisivo e aquisição de dados (SCADA) dos centros de controle e as subestações. Enquanto um roteador separa as redes do SCADA e corporativas, as regras do *firewall* são incorretamente configuradas.
6. Em 23 de dezembro de 2015, às 15h30, os agentes maliciosos iniciaram seus ataques para interrupção de energia, entrando nas redes do SCADA e de operações através de *backdoors* nas estações de trabalho do SCADA comprometidas. Os agentes mal-intencionados tiram o controle dos operadores das IHMs e, em seguida, abrem os disjuntores.
7. Os agentes maliciosos executam diversas outras ações com a intenção de complicar as respostas dos operadores de controle e aumentar o trabalho necessário para retornar o sistema às condições normais de operação. Estas ações incluem:
   a. Lançar um Ataque de Negação de Serviço de Telefonia (TDoS: “Telephony Denial of Service”) coordenado que inunda os *call centers* para impedir que chamadas legítimas sejam completadas.
   b. Desabilitar as UPSs para os centros de controle.
   c. Corromper o firmware dos servidores de portas serial-para-Ethernet de módulos das IHMs das unidades terminais remotas (UTRs).s
8. Os agentes mal-intencionados executam o *malware* KillDisk na tentativa de destruir as IHMs dos centros de controle e as estações de trabalho de pontos-chave.

B. Análise Detalhada do Ataque

Os agentes maliciosos reuniram dados das redes da Ucrânia ao longo de muitos meses. Uma análise completa das atividades que antecederam e levaram ao ataque e durante o ataque é útil para compreender a complexidade do evento. Os números na Fig. 2 correspondem às diferentes etapas do ataque, conforme descrito nesta seção.

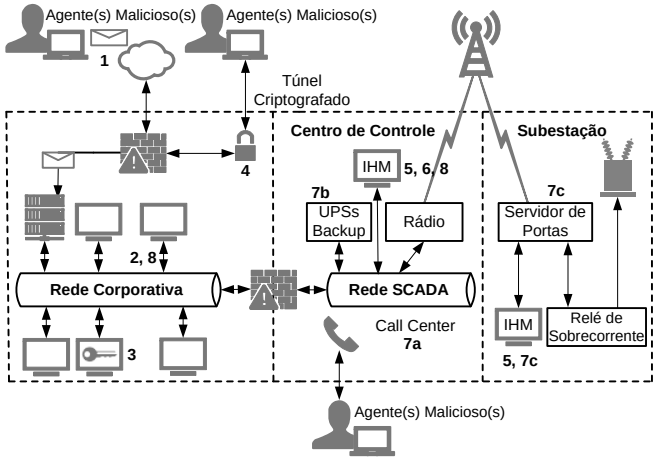

Fig. 2. Modelo Extrapolado da Rede e Ataque.

1) Etapa 1: Spear Phishing

Em março de 2015, agentes maliciosos usaram *spear phishing* para comprometer *hosts* que lhes permitiriam acessar as redes-alvo [4]. Os agentes maliciosos direcionaram o ataque a indivíduos específicos dos *oblenergos* com arquivos de *spear phishing* que pareciam ser correspondência oficial do Ministério de Energia da Ucrânia [8]. Estes e-mails continham uma planilha do Microsoft Excel® ou um documento do Microsoft Word [9]. A abertura do documento e ativação dos macros levaram à instalação de BE3 naquele computador. Muitos usuários foram comprometidos desta forma.

2) Etapa 2: Malware Usado para Explorar e Trafegar na Rede

O reconhecimento e o mapeamento da rede comprometida ocorreram ao longo de muitos meses, com BE3 e outras ferramentas facilitando o movimento lateral através das redes do computador [7]. De acordo com ICS-CERT, BE3 comprometeu um ou mais computadores em cada um dos seis *oblenergos* via *spear phishing*; no entanto, ICS-CERT não pôde confirmar “se o *malware* desempenhou um papel nos ataques cibernéticos reais” [5].

Em abril de 2015, os agentes maliciosos instalaram um *malware* de *backdoor* adicional nas máquinas comprometidas. Este *malware* facilitou aos agentes mal-intencionados o acesso aos computadores comprometidos. O vice-ministro de energia da Ucrânia, Oleksander Svetelyk, declarou que havia “provas de que [os agentes maliciosos] iniciaram a coleta de informações [sobre as redes dos *oblenergos*] nada menos do que seis meses antes do ataque” [10].

3) Etapa 3: Credenciais Obtidas

Em *Prykarpattiaoblenergo*, o servidor Active Directory foi um dos computadores comprometidos, possivelmente levando a um ataque de força bruta contra as senhas ali armazenadas. No *Kyivoblenergo*, os agentes maliciosos

interceptaram senhas usando um método desconhecido. Embora BE3 tenha um plug-in de roubo de senhas, não houve qualquer indicação de encontrar este plug-in específico dentro das redes comprometidas [5].

4) Etapa 4: Túnel Criado Via Rede Privada Virtual

Com as credenciais comprometidas, os agentes maliciosos usaram um túnel criptografado, designado pelo ICS-CERT como rede virtual privada (VPN: "Virtual Private Network"), para estabelecer presença nas redes dos *oblenergos*. Os agentes maliciosos usaram ferramentas de acesso remoto padrão para obter acesso às IHMs das redes do sistema de controle: RDP ("Remote Desktop Protocol"), Radmin ("Remote Administrator") e SSH ("Secure Shell"). Os agentes mal-intencionados criaram este túnel criptografado apenas com credenciais de nome do usuário/senha; as redes dos *oblenergos* não exigiam uma autenticação de dois fatores [5].

5) Etapa 5: Reconhecimento e Comprometimento dos Computadores das IHMs

O acesso a um dos computadores nos *oblenergos* forneceu credenciais para acesso remoto à aplicação das IHMs, que por sua vez permitiu aos agentes maliciosos interagirem remotamente com o sistema de controle. Antes do ataque, os agentes maliciosos executaram o reconhecimento e comprometeram pelo menos 17 IHMs de centros de Operações, as quais são conectadas a mais de 50 subestações [5].

6) Etapa 6: Manipulação de Disjuntores

O ataque ao primeiro *oblenergo* manipulou um disjuntor inicial às 15h:30, conforme Horário do Leste Europeu (EET: "Eastern European Time"). O ataque ao próximo *oblenergo* começou um minuto depois, às 15h31, seguido pelo ataque ao terceiro *oblenergo* às 16h00 aproximadamente. Os operadores eram capazes de ver, mas não de impedir que os agentes mal-intencionados usassem seus computadores e manipulassem a IHM. Os operadores da Ucrânia capturaram e compartilharam um vídeo deste evento com o ICS-CERT [4].

Às 16h10, os operadores da concessionária responderam às interrupções em um *oblenergo* desabilitando uma conta do administrador da IHM. Os agentes maliciosos continuaram a desligar o sistema usando uma segunda conta do administrador da IHM. Mais tarde, os operadores da concessionária desligaram todo o sistema SCADA e, finalmente, a VPN. O tempo total para o ataque cibernético foi de aproximadamente 60 minutos [7]. Finalmente, os operadores colocaram todos os sistemas SCADA off-line e passaram para o modo manual, que era a única maneira que tinham para restabelecer a energia [11]. Um *oblenergo* foi capaz de desativar o acesso remoto, mas apenas em tempo de salvar uma subestação.

O ataque desligou disjuntores em intervalos de minutos um do outro, sugerindo que múltiplos agentes maliciosos manualmente orquestravam o ataque. Não há evidência de ataques automáticos; os movimentos dos cursores do mouse através das telas das IHMs eram similares aos de uma pessoa executando a ação [4]. O ataque, através de pelo menos 17 centros de despacho local, ocorreu em um espaço de tempo muito curto, e pelo menos alguns aspectos do ataque precisariam de uma equipe de agentes maliciosos.

O ICS-CERT concluiu que "O ataque cibernético foi sincronizado e coordenado, conforme reportado, provavelmente após extenso reconhecimento das redes vítimas" [5].

7) Etapa 7: Ações de Ataques Adicionais

a) Negação de Serviço de Telefonia

Os agentes maliciosos lançaram um ataque TDoS para interromper as operações e o restabelecimento em *Prykarpattiaoblenergo* e *Kyivoblenergo*. Os *call centers* ficaram sobrecarregados com falsas chamadas automáticas provenientes de números de telefone estrangeiros. O *Kyivoblenergo* classificou como sendo uma falha técnica ocorrendo no *call center* [7]. Posteriormente, o *Kyivoblenergo* declarou publicamente que o ataque TDoS afetou sua capacidade de responder rapidamente porque não tinha percepção situacional sem a IHM operando e estava incapacitado para receber chamadas sobre onde as interrupções tinham ocorrido [4].

b) Acesso Remoto e Desligamento das UPSs

Pouco antes das 15h30, os agentes maliciosos usaram as interfaces de gerenciamento remoto das UPSs para programar um desligamento das UPSs dos servidores de computadores no *Kyivoblenergo* para mais tarde, ao anoitecer [4] [5]. Em *Prykarpattiaoblenergo*, a UPS para troca de ramais privados (PBX: "Private Branch Exchange") também foi desligada da mesma forma [4]. Isso foi provavelmente efetuado para interferir nos esforços de resposta aos incidentes e restabelecimento [5].

c) Atualização Maliciosa de Firmware

Os agentes maliciosos tornaram um número desconhecido de dispositivos serial-para-Ethernet da subestação inoperáveis ao corromper seu firmware [7]. O fabricante não pôde corrigir os dispositivos que tiveram o firmware comprometido [6].

8) Etapa 8: Execução de KillDisk nos Computadores-Alvo

Todos os três *oblenergos* alegaram que os agentes destruíram alguns sistemas usando o *malware* KillDisk na conclusão do ataque cibernético. KillDisk apaga arquivos selecionados nos sistemas-alvo e corrompe o registro mestre de inicialização, tornando os sistemas inoperáveis [5].

O ICS-CERT também verificou que em, pelo menos, um caso, uma placa-filha de uma UTR executando o sistema operacional Windows Embedded Compact (CE) para acionar uma IHM local foi sobrescrita pelo *malware* KillDisk. O fabricante da UTR foi incapaz de restaurar ou corrigir a UTR [7].

III. Criando uma Arquitetura de um Sistema de Controle Robusto

Para criar uma arquitetura de um sistema de controle robusto com uma defesa sólida, uma organização deve considerar três conceitos.

- Identificar riscos e desenvolver um plano para gerenciamento destes riscos.
- Implementar controles eficazes para gerenciar o risco.
- Criar um modelo de defesa em profundidade que permita controles de segurança eficazes e eficientes.

A. Avaliação e Gestão de Riscos

A avaliação e a gestão de riscos permitem que as organizações efetuem a identificação, medição e controle dos riscos organizacionais. Estes dois fatores garantem que controles de segurança sejam implementados em equilíbrio com as operações da organização. Os *oblenergos* não executaram suficientemente essas funções antes do incidente cibernético.

Avaliação de risco é uma função para identificar vulnerabilidades e ameaças, entender seu impacto e determinar quais controles melhor atenuarão essas ameaças. A avaliação de risco tem os seguintes objetivos:

- Identificar ativos e seu valor
- Identificar vulnerabilidades e ameaças
- Calcular a probabilidade das ameaças e o impacto comercial
- Balancear o impacto das ameaças com o custo dos controles de segurança

Um ativo pode ser tangível ou intangível. Ativos tangíveis incluem equipamentos, software, instalações, sistemas e equipes de trabalho que uma organização depende para funcionar e efetuar negócios. Ativos intangíveis incluem dados, reputação e propriedade intelectual valiosos para a organização.

Os *oblenergos* possuem muitos ativos tangíveis para serem considerados e acompanhados completamente desde os *gateways* de *firewall* do perímetro até as UTRs e IHMs do sistema de controle. Ativos intangíveis para os *oblenergos* incluem as credenciais dos funcionários e topologias da rede. O valor do ativo inclui:

- Valor da substituição
- Custo de manutenção
- Custo dos danos se houver perda
- Penalidades ou multas se houver perda

Vulnerabilidade é uma ausência ou deficiência de um controle de segurança ou medida defensiva dentro do sistema. A falta de proteção contra *malware* ou uma proteção contra *malware* desatualizada nos dispositivos de rede e a falta de filtros de e-mail apropriados para evitar ataques de *phishing* são exemplos de vulnerabilidades. Avaliações de vulnerabilidade são parte da função de gestão de risco global e devem ser conduzidas em uma base periódica.

Uma ameaça é percebida quando há uma exploração para uma vulnerabilidade. Um exemplo de ocorrência de uma ameaça foi quando os agentes maliciosos implantaram *malware* para infiltração e proliferação nas redes dos *oblenergos*.

Para identificar ameaças, muitas vezes é útil considerar os agentes de ameaça. Agentes de ameaça são tipicamente agrupados nas seis categorias mostradas a seguir:

- **Humana**: Inclui agentes maliciosos, indivíduos de um determinado grupo ou organização (“insiders”) e indivíduos que não pertencem a um determinado grupo ou organização (“outsiders”) não maliciosos, equipes de trabalho extintas e terroristas.
- **Técnica**: Inclui falhas de equipamentos, falhas de software, *malware* e tecnologias incompatíveis.
- **Física**: Inclui problemas associados à entrada na instalação, problemas com crachás e questões de monitoramento de vídeo.
- **Ambiental**: Inclui problemas associados à empresa de telefonia externa, questões de tráfego da rodovia, construção próxima e derramamentos de materiais perigosos.
- **Natural**: Inclui enchentes, tornados, incêndios, terremotos, furacões e raios.
- **Operacional**: Inclui problemas em processos e procedimentos que afetam a capacidade de a organização proteger seus ativos.

Vulnerabilidades e ameaças são combinadas para determinar a probabilidade de ocorrência de um evento. Um evento com alta probabilidade e alto impacto vai receber a maior prioridade para mitigação. Quantificar os valores em dólar para eventos distintos e, então, identificar quantas vezes por ano tais eventos vão ocorrer permite priorizá-los para implementação de controles de segurança para mitigação.

B. Controles de Segurança

Nos sistemas de potência modernos, há uma ampla gama de controles de segurança disponíveis para auxiliar o defensor do sistema de controle. O Instituto Nacional de Padrões e Tecnologia (NIST: “National Institute of Standards and Technology”) dos Estados Unidos fornece uma estrutura e agrupamento para estes controles de segurança em [12], os quais são denominados “Security Control Identifiers and Family Names” (Nomes de Famílias e Identificadores de Controles de Segurança). Concluímos que isto é extremamente útil quando se considera controles de segurança para todos os sistemas de controle, não apenas para energia elétrica. Incluímos um subconjunto desses controles com o respectivo tipo do grupo do NIST [13].

1) Isolar os Sistemas de Controle

Família de Controle de Segurança: Controle de Acesso

BE3 foi infiltrado nos sistemas corporativos da Ucrânia através da engenharia social e outros métodos similares. Se o sistema de controle for conectado à rede corporativa ou a outras redes, é possível que um *malware* como BE3 possa afetar o sistema de controle. Técnicas como a criação de redes segmentadas usando *firewalls* e protegendo dados através de criptografia das comunicações são fundamentais para eliminar, ou pelo menos limitar, o impacto do *malware*. Para minimizar a exposição da rede:

- NUNCA conectar os sistemas de controle à Internet.
- Localizar dispositivos e redes do sistema de controle atrás de *firewalls* e isolá-los da rede corporativa, monitorando cuidadosamente as listas de controle de acesso do *firewall* e apenas permitindo o tráfego que é necessário para uma operação segura do sistema.
- Se o acesso remoto for necessário, utilizar métodos seguros como VPNs, reconhecendo que uma VPN é apenas tão segura quanto os *proxies* e dispositivos conectados e autenticação de dois fatores.

Um sistema de controle deve incluir pontos de demarcação que permitam que o sistema seja isolado em diferentes níveis. A Seção C apresenta a discussão de uma técnica para definição e criação destes pontos de demarcação.

2) Estabelecer Padrões de Referência, Registrar e Monitorar Continuamente os Sistemas de Controle

Família de Controle de Segurança: Integridade das Informações e Sistema, bem como Resposta ao Incidente

O monitoramento contínuo da rede é essencial para detectar intrusos ou contaminações, e uma organização deve monitorar todos os segmentos da rede. Diferentes segmentos de rede mostrarão diferentes resultados de monitoramento. Algumas vezes, combinando os dados dos segmentos da rede, podemos ver problemas que não são óbvios em um segmento único da rede. Adicionalmente, é necessário usar monitoramento e análise dos registros automatizados, uma vez que a quantidade de dados a serem processados e considerados torna-se muito grande para ser analisada manualmente [14].

Diversos analisadores de fluxos de rede ("netflow"), sistemas de detecção de intrusão (IDS: "Intrusion Detection Systems"), sistemas de prevenção de intrusão (IPS: "Intrusion Prevention Systems") e aplicativos de controle de acesso à rede (NAC: "Network Access Control") estão disponíveis atualmente. Embora estes indicadores sejam um pouco lentos, eles fornecem aos operadores do sistema uma percepção do estado da rede, padrões de referência ("baselines") do tráfego da rede, estado das portas da rede e recursos de análise. A natureza estática do tráfego da rede de um sistema de controle devidamente isolado torna mais fácil o monitoramento e reconhecimento de segurança do estado do sistema de controle para o propósito de manutenção e análise do que nas redes corporativas.

Os sistemas de controle são sistemas de função fixa. Quando os sistemas de controle estão em operação, não deve haver nenhuma razão para adicionar aplicativos desconhecidos ou executar processos desconhecidos. Os sistemas baseados na lista branca bloqueiam a execução de todos os aplicativos indesejados e desconhecidos, incluindo *malware*.

A adoção de padrões de referência ("baselines") é uma parte crítica do monitoramento; como saber o que é errado, a não ser que tenhamos um padrão de referência para nos dizer o que é certo? Estes padrões de referência devem incluir o maior número possível de pontos de dados do maior número possível de dispositivos diferentes (dispositivos, sensores e todos os controladores de rede), e devem se estender por tempo suficiente para determinação de padrões de regular/normal. A automatização do estabelecimento de padrões de referência e pesquisas para verificação de alterações de ajustes e firmware em muitos dispositivos podem ser realizadas através de um controlador lógico programável (CLP).

Alarmes representam a forma mais direta e imediata que um sistema de controle tem para interagir com os operadores humanos. Os alarmes devem ser pré-programados para disparar sempre que a operação normal do sistema de controle for desviada para além de limites pré-programados e aceitáveis. Os alarmes podem ser definidos para uma gama de disparos, incluindo ação do disjuntor, alterações de senha e outros eventos críticos.

Registros consistem em uma ferramenta valiosa para alertar e coordenar a resposta aos incidentes, bem como determinar o que ocorreu depois que algo deu errado. Após lidar com o problema imediato, é fundamental descobrir a causa do problema ocorrido e evitar que aconteça novamente. O mesmo se aplica a um ataque cibernético. Registros configurados adequadamente vão ajudar a descobrir até que ponto da rede os *hackers* chegaram, o que eles modificaram e como obtiveram acesso em primeiro lugar.

3) Executar Patches, Atualização e Manutenção

Família de Controle de Segurança: Gerenciamento da Configuração e Manutenção

Novas ameaças surgem todos os dias. A criação de processos que garantam a atualização dos sistemas de controle é fundamental para manter um sistema seguro. Os processos incluem o monitoramento de notícias, blogs, listas de contato e outras fontes. Adicionalmente, a NERC exige que *patches* sejam avaliados pelo menos uma vez a cada 35 dias [15]; sugerimos configurar uma programação mensal para executar *patches* e atualizações. Ao efetuar a atualização do firmware ou software, as atualizações devem ser realizadas usando firmware assinado digitalmente pelo fabricante.

4) Ter Planos de Contingência

Família de Controle de Segurança: Planejamento de Contingências e Resposta ao Incidente

No caso de um incidente cibernético ou falha de equipamentos, é fundamental restaurar a funcionalidade do sistema de controle rapidamente. Tenha um plano de recuperação no local que inclua imagens dos dispositivos, esquemas/projetos do sistema de controle e procedimentos de restauração [16]. Pratique estes planos para garantir uma resposta adequada.

5) Relatórios e Lições Aprendidas Após a Ação

Família de Controle de Segurança: Avaliação de Riscos, Conscientização e Treinamento

Se ocorrer um evento em seu sistema de controle, aproveite a oportunidade para analisar por que ocorreu a situação e aprender com a mesma. Use dados disponíveis como *syslogs*, relatórios de evento, relatórios da sequência de eventos e outros registros para efetuar uma análise completa do evento.

6) Garantir a Segurança Física

Família de Controle de Segurança: Proteção Física e Ambiental

Grande parte da segurança cibernética foca na penetração de dispositivos eletrônicos a partir de uma rede interna ou da Internet. No entanto, precisamos também garantir os aspectos físicos do sistema de controle. Muitas vezes, a porta frontal de um dispositivo é deixada com senhas padrão, e se um intruso puder cortar a cerca ao redor da instalação do sistema de controle, ele pode acessar eletronicamente com facilidade os dispositivos através desta porta desprotegida.

7) Assegurar Senhas Complexas

Família de Controle de Segurança: Identificação, Autenticação e Controle de Acesso

Senhas padrão são definidas na fábrica e permitem que os usuários configurem rapidamente os sistemas *out-of-the-box*. Contudo, para proteger seu sistema contra ataques, os usuários devem alterar a senha padrão para algo exclusivo e criptograficamente forte como parte do processo de comissionamento.

É também necessário garantir que as senhas criadas pelo usuário sejam suficientemente complexas e aleatórias. Senhas simples ou fáceis de adivinhar podem fornecer acesso fácil ao sistema de controle. O processo de rotatividade frequente de senhas, através do qual as senhas são alteradas periodicamente, também é um requisito de segurança necessário.

C. Estratégia de Defesa em Profundidade

Nem todas as partes do sistema de controle requerem o mesmo nível ou tipo de segurança. O conjunto abrangente de controles de segurança do NIST 800-53 fornece diretrizes para determinar e desenvolver uma abordagem de defesa em profundidade com ICS-CERT. Este método de defesa em profundidade foi proposto pelo Departamento de Segurança Interna dos Estados Unidos [17], Oman, Schweitzer e Frincke [18], e muitos outros pesquisadores.

Modificamos e expandimos o sistema de controle do modelo de defesa em profundidade no trabalho relacionado [19] e apresentamos um resumo deste método na Fig. 3.

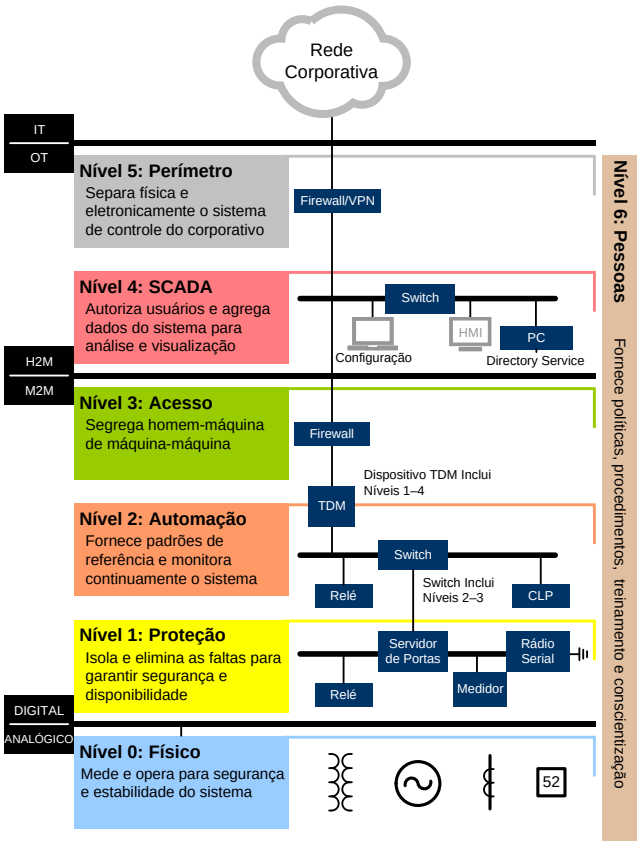

Fig. 3. Modelo de Defesa em Profundidade

Muitas concessionárias dos Estados Unidos estão adotando um modelo de segurança baseado em camadas, onde cada nível introduz mais segurança na rede para proteção dos aplicativos e recursos críticos. Os controles de segurança em níveis adequados permitem que o usuário eficientemente monitore, detecte e impeça tentativas de burlar a segurança. Pontos de demarcação definem a interação homem-máquina (H2M: "Human-to-Machine") com o sistema (laptop ou estação de trabalho), aplicação dos produtos no sistema (IHM, UTR, relé), e protocolos de comunicação (SCADA ou protocolos de proteção). Sob este modelo de segurança, os usuários desenvolvem ajustes da proteção de tal forma que os dispositivos possam continuar a operar corretamente se precisarem ser isolados da rede como uma etapa de mitigação logo que um ataque tenha sido detectado.

1) Nível 0: Físico

A segurança de Nível 0 envolve controles físicos. Para garantir a disponibilidade do sistema, a segurança física da subestação foca em manter afastados os intrusos através de intimidação: obstáculos, fronteiras, sinais visíveis, câmeras visíveis, etc. Medidas de detecção e defesa sob a forma de alertas e alarmes propiciam detectar a intrusão. Exemplos incluem alarmes de porta, sensores de ocupação, sensores de luz e indicadores piscando. Bloqueios físicos com autenticação de crachás estão se tornando um padrão nas subestações críticas dos EUA. Controles de segurança de Nível 0 também são desenvolvidos juntos, em camadas, fornecendo mais informações sobre o acesso e movimentação de intrusos.

2) Nível 1: Proteção

Os dispositivos de Nível 1 são sistemas incorporados em tempo real, configurados para segurança, controle e acionamento específicos dos equipamentos de Nível 0, tais como válvulas, sensores ou disjuntores. Os dispositivos de Nível 1 têm padrões de referência ("baselines") das configurações de revisões de firmware e ajustes. As atualizações de firmware são assinadas digitalmente para efeito de verificação antes de ser instalado.

As comunicações são essencialmente ponto-a-ponto, ponto-a-multiponto, isoladas ou seriais. Estas comunicações não-roteadas ajudam a garantir a integridade dos dados e impedir a injeção de dados, ataques ("spoofing") ou escuta clandestina remota. As informações dos equipamentos de proteção dos relés, incluindo ajustes, devem ser armazenadas em bancos de dados seguros e redundantes com acesso limitado aos engenheiros de sistemas de potência. Isolar os canais de comunicação e rede máquina-a-máquina (M2M: "Machine-to-Machine") de Nível 1 da interação humana garante o processamento em tempo real e comunicações necessárias para um controle rápido do sistema.

Embora a tecnologia de controle de acesso e protocolos como LDAP e RADIUS possam fazer sentido nos sistemas corporativos, excluí-los deste nível nos sistemas de controle reduz a superfície de ataque e a complexidade dos dispositivos de Nível 1. Limitar a interação direta do usuário com os equipamentos neste nível e restringir o acesso através de pontos de acesso dedicados reduz os requisitos de monitoramento e manutenção do sistema. A complexidade extra de LDAP e RADIUS resulta em maior probabilidade de configuração incorreta pelo usuário final e implementação inadequada pelo fabricante. Procedimentos de Autenticação, Autorização e Responsabilidade (AAA:

"Authentication, Authorization, Accountability") e registros apropriados podem ainda ser obtidos sem complexidade adicional. Conforme observado no incidente da Ucrânia, as pessoas representam tipicamente o ativo mais direcionado e comprometido em uma organização. Não é prudente vincular diretamente o acesso 24/7 do usuário final aos dispositivos de Nível 1. Os dispositivos de Nível 1 restringem as tentativas de log-in, capturam as tentativas de log-in sem sucesso e geram alertas.

Os diagnósticos internos e as varreduras de memória contínuas não apenas garantem a operação adequada dos equipamentos de Nível 1, mas também atuam como proteção de *malware* baseada na lista branca. A proteção contra *malware* com lista branca é superior à proteção *antimalware* baseada em assinatura da lista negra para dispositivos incorporados porque os dispositivos executam uma função específica e nada mais.

3) Nível 2: Automação

As comunicações efetuadas a partir dos níveis mais altos para o Nível 1 passam através dos dispositivos de Nível 2. Os dispositivos de Nível 2 filtram e processam essas comunicações e impedem que determinadas atividades, tais como ataques de negação de serviço, atualizações de firmware não assinadas, controles SCADA injetados e acesso remoto da engenharia não autorizado alcancem dispositivos de Nível 1. O Nível 2 fornece uma quebra de protocolo entre as comunicações de entrada e os equipamentos de Nível 1.

O monitoramento contínuo e a adoção de padrões de referência estão concentrados no Nível 2. Os equipamentos de automação (como um CLP) adotam padrões de referência e monitoram as mudanças nas configurações de revisões de firmware e ajustes do sistema de controle. Os dispositivos de Nível 2 coletam e agregam os alarmes do sistema para o sistema de controle via *Syslog* para análise.

Os dispositivos de Nível 2 criam e gerenciam senhas fortes que os dispositivos de Nível 1 precisam para executar determinadas funções, tais como alteração de ajustes ou coleta de dados. Os dispositivos de Nível 2 também mantêm um ponto de isolamento rápido se um ataque comprometer os equipamentos de Nível 1.

4) Nível 3: Acesso

Os dispositivos deste nível separam, restringem e filtram os níveis humano-para-máquina dos níveis máquina-para-máquina. Uma função específica deste nível consiste em executar um *proxy* apenas para o acesso autenticado a partir dos dispositivos SCADA aprovados para aqueles usuários com privilégios de acesso às máquinas nos níveis inferiores. Um *firewall* de estado ("stateful firewall") neste nível de acesso cria uma zona desmilitarizada (DMZ: "Demilitarized Zone") de Nível 4 para o sistema de controle.

O Nível 3 também mantém um mecanismo de isolamento rápido do Nível 2, caso este seja comprometido. Como o Nível 2 contém a lógica do sistema de controle para maior desempenho e eficiência do sistema de controle, é importante estar apto para isolá-lo rapidamente do sistema de controle no caso de um ataque.

5) Nível 4: SCADA

Nível 4 é o nível onde os usuários vão interfacear diretamente com o sistema de controle quando for necessário. Os dispositivos de Nível 4 lidam com tarefas como autorização do usuário. A análise e visualização dos dados do sistema de controle ocorrem neste nível. Os usuários devem manter qualquer IHM necessária para o sistema de controle isolada no Nível 4 juntamente com outro software necessário nos computadores do sistema operacional geral. A proibição de dispositivos do sistema operacional geral de níveis abaixo do Nível 4 reduz a complexidade e a superfície de ataque global do sistema.

A localização dos serviços do Active Directory para o sistema de controle neste nível separa e isola as contas de usuários dos sistemas corporativos. Dispositivos, estações de trabalho ou laptops temporários necessários para manutenção e acesso da engenharia ao sistema de controle usam a rede de Nível 4. O acesso do usuário na rede de Nível 4 força estes dispositivos a terem os mais recentes *patches* e proteção de *malware* atualizada.

Software como o Splunk, representando o estado do sistema e postura de segurança, é necessário neste nível. Outros Sistemas Eletrônicos de Monitoramento ou Controle de Acesso (EACMS: "Electronic Access Control or Monitoring Systems") monitoram e analisam continuamente o tráfego para verificar intrusões no sistema de controle.

6) Nível 5: Perímetro

Nível 5 é o ponto de acesso para o sistema de controle ou subestação. Ele incorpora equipamentos de comunicação de área ampla juntamente com *firewalls* para as redes de negócios ou corporativas. Entre os sistemas de controle (tais como subestações), os equipamentos de comunicações baseadas na Multiplexação por Divisão de Tempo (TDM: "Time Division Multiplexing") fornecem comunicações máquina-a-máquina determinísticas necessárias para o controle efetivo em tempo real do sistema. TDM segrega e criptografa o tráfego, protegendo-o contra *spoofing* e injeção de dados.

Todos os dados relacionados ao negócio que precisam ser reportados ao sistema de controle são baseados em canais e protocolos unidirecionais via *firewalls* de Nível 5. O acesso à VPN nos sistemas corporativos não pode ser efetuado sem passar pelo Nível 5.

Uma Rede Definida por Software de Tecnologia Operacional (OTSDN™: "Operational Technology Software-Defined Network") possibilita a engenharia de tráfego, lista branca e uma arquitetura de negação por padrão para a rede do sistema de controle. Além de fornecer prevenção e detecção de intrusão inerente, OTSDN otimiza o desempenho de recuperação de falhas, necessário para sistemas de controle.

7) Nível 6: Pessoas

Uma cultura de segurança é tão vital para uma organização de infraestrutura crítica quanto a segurança. As políticas, procedimentos, treinamento, conscientização de segurança, análise de risco e outras técnicas baseadas em humanos que garantem a segurança do sistema estão neste nível. O Nível 6 abrange todos os outros níveis devido ao impacto de coisas como políticas e procedimentos em todos os níveis do sistema de controle.

IV. Avaliação da Segurança no Incidente da Ucrânia

Uma das principais dificuldades na análise da interrupção de energia da Ucrânia é o fato de não haver relatórios detalhados suficientes (*syslog*, relatórios de eventos, relatórios IDS) que possam apontar para o que realmente aconteceu no sistema sob uma perspectiva cibernética. O estabelecimento de controles para implementar padrões de referência, registros e monitoramento do sistema global visando efetuar uma análise pós-evento e determinação da causa-raiz teria fornecido estas informações. Se estas ferramentas estivessem implementadas, os investigadores poderiam ter analisado os sistemas conforme construído ("as-built") versus sistemas em serviço. Os investigadores poderiam ter analisado os registros do sistema para determinar quando os sistemas começaram a operar incorretamente. Os indicadores em tempo real teriam fornecido aos operadores os indicadores de desempenho.

Na Ucrânia, limitar o controle a alguns poucos servidores e computadores de estações de trabalho selecionados teria limitado a superfície de ataque e agilizado os tempos de resposta. Um *antimalware* com lista branca nos laptops ou estações de trabalho baseadas em Windows dedicadas aos sistemas de controle, juntamente com ferramentas de comparação de padrões de referência, teriam impedido a propagação de BE3 nos dispositivos e sistemas das concessionárias da Ucrânia. Os aplicativos IDS, IPS e NAC devem detectar alguns dos meios de propagação de BE3, bem como as chamadas na rede causadas por BE3. VPNs e *firewalls* configurados e mantidos adequadamente teriam isolado todos os dispositivos, exceto alguns poucos dispositivos selecionados de redes selecionadas, impedindo que fossem pontos-chave para BE3. O registro de alterações nos ajustes e atualizações de firmware, o estabelecimento de padrões de referência dessas modificações e o posterior monitoramento contínuo destes padrões teriam sido medidas de segurança muito eficazes contra BE3, mesmo se a concessionária não tivesse meios para definir, alterar ou gerenciar senhas ou suas credenciais nos relés ou IEDs.

A Tabela I resume as ameaças que foram observadas no incidente da Ucrânia e relaciona os controles que podem impedir que estes tipos de ameaças sejam bem-sucedidos no futuro.

TABELA I
CONTROLES DE SEGURANÇA PARA EVITAR AMEAÇAS COMO O INCIDENTE DA UCRÂNIA

Etapa	Ameaça	Controles de Segurança
Geral	Falta de conhecimento/percepção situacional dos ativos e sistemas	Monitoramento (sistemas de detecção de intrusão, análise do fluxo de rede, padrões de referência, registros)
1. Acesso Inicial à Rede Corporativa	*Spear phishing*	- Treinamento - Controles de segurança de e-mails (remover anexos, efetuar a varredura automática de anexos)
2. Ponto-Chave na Rede Corporativa	Malware (BE3)	- Antivírus - IDS - *Firewalls* baseados em *hosts*
3. Aumentar Privilégios	Credenciais comprometidas: - Software *keylogger* - Força bruta	- Garantir ao usuário o mínimo de privilégios - Rotatividade de senhas - Antivírus - Credenciais fortes - IDS - Syslogs
4. Acesso à Manutenção	Acesso via túnel	- Regras adequadas de *firewall* - Autenticação multifator - Controles de VPN - Monitoramento
5. Obter Acesso ao Sistema de Controle	Acesso remoto às IHMs/SCADA	- Segmentação da rede - Garantir ao usuário o mínimo de privilégios
6. Ataque	Acesso remoto ao sistema de controle/disjuntores	- Autenticação robusta - Acesso remoto criptografado - Isolação rápida - Canais de comunicação dedicados ou não-públicos - Planejamento do incidente
7. Complicação do Ataque		
a)	DoS de Telefonia	- Comunicações de backup - Bloqueio de chamadas - Conhecimento dos ativos
b)	Acesso remoto às UPSs	- Segmentação da rede - Acesso remoto não interativo - Autenticação robusta
c)	Atualização maliciosa de firmware	- Validação de firmware (*hashing*, assinaturas) - Backups de hardware (sistemas *on-line* ["hot"] e *off-line* ["cold"]) - Procedimentos de restabelecimento
8. Destruir os HDs (Hard Drives)	Malware (KillDisk)	- Backups de dados automáticos - Antivírus

V. Conclusão

Os sistemas de controle industriais fornecem muitos benefícios para a automação e controle remoto dos sistemas de potência, incluindo a percepção situacional e a configuração automática da rede. A interrupção de energia induzida por ataque cibernético na Ucrânia demonstrou que hackers podem explorar um sistema de controle que não seja baseado em princípios de projeto com defesa em profundidade. A interrupção de energia da Ucrânia não foi resultado de uma única vulnerabilidade. Mais propriamente, um conjunto de pequenas deficiências de controle e projeto de rede permitiu que os hackers conseguissem consequentemente desligar a energia.

Este artigo descreveu uma abordagem de segurança em camadas que é apropriada para cada tipo de dispositivo do sistema de controle. Uma segurança cibernética adequada inclui pessoas, hardware, software, políticas e procedimentos, independentemente de estar considerando uma rede corporativa ou um sistema de controle. O incidente cibernético na Ucrânia foi um evento infeliz que desligou a energia de milhares de residências. Como resultado positivo do evento, ele fez com que as empresas de energia elétrica avaliassem suas posturas de segurança e considerassem a implementação das ideias discutidas neste artigo.

VI. Referências

[1] Molbuk News Agency, “Chernivtsioblenergo also suffered cyber attacks from Russia,” viewed August 21, 2016. Available: http://molbuk.ua/ chernovtsy_news/104328-chernivcioblenergo-takozh-zaznalo-kiberataky-z-rosiyi.html.

[2] Prykarpattiaoblenergo Corporate Web Page, “Energy liquidate the consequences of a major accident in the Carpathian region,” viewed August 26, 2016. Available: http://www.oe.if.ua/showarticle.php?id=3413.

[3] Ukrainian Ministry of Energy and Coal, “The Work Group to Study the Causes of the Temporary Malfunction of Power Supply Companies, Which Took Place December 23, 2015,” January 2016. Available: http://mpe.kmu.gov.ua/minugol/control/publish/article?art_id=245082298.

[4] K. Zetter, “Inside the Cunning, Unprecedented Hack of Ukraine’s Power Grid,” WIRED, March 2016. Available: http://www.wired.com/2016/03/inside-cunning-unprecedented-hack-ukraines-power-grid/.

[5] ICS-CERT, “Alert (IR-ALERT-H-16-056-01AP): Cyber-Attack Against Ukrainian Critical Infrastructure,” Department of Homeland Security, March 2016. Available: http://www.eenews.net/assets/2016/07/19/ document_ew_02.pdf.

[6] ICS-CERT, “Advisory (ICSA-16-152-01): Moxa UC-7408-LX-Plus Firmware Overwrite Vulnerability,” Department of Homeland Security, May 2016. Available: https://ics-cert.us-cert.gov/advisories/ICSA-16-152-01.

[7] E-ISAC, SANS, “Analysis of the Cyber Attack on the Ukrainian Power Grid,” March 18, 2016. Available: https://ics.sans.org/media/E-ISAC_SANS_Ukraine_DUC_5.pdf.

[8] P. Polityuk, “Exclusive: Hackers May Have Wider Access to Ukrainian Industrial Facilities,” Reuters, January 2016. Available: http://www.reuters.com/article/us-ukraine-cybersecurity-exclusive-idUSKCN0V51H1.

[9] V. Kremez, “APT Malware Analysis: BlackEnergy Додатокı Excel VBA Dropper,” viewed August 23, 2016. Available: http://www.vkremez.com/cyber-security/apt-malware-analysis-blackenergy1-excel-vba-dropper.

[10] P. Polityuk, “Ukraine Sees Russian Hand in Cyber Attacks on Power Grid,” Reuters, February 2016. Available: http://www.reuters.com/article/us-ukraine-cybersecurity-idUSKCN0VL18E.

[11] iSIGHT Partners, “Cyber Attacks on the Ukrainian Grid: What You Should Know.” Available: https://www.fireeye.com/content/dam/fireeye-www/global/en/solutions/pdfs/fe-cyber-attacks-ukrainian-grid.pdf.

[12] National Institute of Standards and Technology. Special Publication 800-53, “Security and Privacy Controls for Federal Information Systems and Organizations,” Rev. 4, April 2013. Available: http://nvlpubs.nist. gov/nistpubs/SpecialPublications/NIST.SP.800-53r4.pdf.

[13] J. Smith, J. Pereyda, D. Gammel, “Cybersecurity Best Practices for Creating Resilient Control Systems,” proceedings of the International Symposium on Resilient Control Systems, Philadelphia, PA, 2016.

[14] P. Oman, E. O. Schweitzer, III, and J. Roberts, “Safeguarding IEDs, Substations, and SCADA Systems Against Electronic Intrusions,” proceedings of the 3rd Annual Western Power Delivery Automation Conference, Spokane, WA, April 2001.

[15] NERC, “Critical Infrastructure Protection, V5,” 2015. Available: http://www.nerc.com/pa/Stand/Pages/CIPStandards.aspx.

[16] E. O. Schweitzer III, D. Whitehead, A. Risley, and R. Smith, “How Would We Know?” proceedings of the 37th Annual Western Protective Relay Conference, Spokane, WA, October 2010.

[17] K. Barnes and B. Johnson, “Introduction to SCADA Protection and Vulnerabilities,” Idaho National Engineering and Environmental Laboratory, January 2004. Available: http://www.inl.gov/technical publications/Documents/3310860.pdf.

[18] P. Oman, E. O. Schweitzer, III, and D. Frincke, “Concerns About Intrusions Into Remotely Accessible Substation Controllers and SCADA Systems,” proceedings of the 27th Annual Western Protective Relay Conference, Spokane, WA, October 2000.

[19] J. Smith, N. Kipp, D. Gammel, “Defense in Depth Security for Industrial Control Systems,” Proceedings of the Electricity Engineers’ Association Conference & Exhibition, Wellington, NZ, 2016.

VII. Biografias

Dave Whitehead ingressou na Schweitzer Engineering Laboratories, Inc. (SEL) em 1994. Atualmente, é vice-presidente de Pesquisa e Desenvolvimento e também supervisiona a Divisão de Serviços Governamentais da SEL. Ele é membro do Conselho de Diretores da SEL. O Sr. Whitehead recebeu seu BSEE da Washington State University e seu MSEE do Rensselaer Polytechnic Institute. Ele é um membro sênior do IEEE e preside o grupo C6 de Subestações da *Power and Energy Society* que aborda protocolos criptográficos seriais. O Sr. Whitehead atualmente detém 51 patentes em todo o mundo com várias outras pendentes e é um engenheiro profissional registrado em Washington, Nova York, Michigan e Carolina do Norte.

Kevin Owens recebeu um diploma da University of Illinois em Chicago com um BS em Engenharia Elétrica e tem trabalhado ativamente em indústrias de energia elétrica e controle desde 1994. Sua experiência na carreira inclui projetos de conjuntos de manobra em paralelo, projetos de segurança de rede, desenvolvimento de software/produto e segurança cibernética para sistemas de controle industriais (ICS). Mr. Owens é atualmente um engenheiro de pesquisa sênior na Schweitzer Engineering Laboratories, Inc. (SEL). Ele trabalha na SEL desde fevereiro de 2014 e tem mais de 30 anos de experiência em segurança cibernética e projetos ICS.

Dennis Gammel recebeu um diploma da University of Idaho com um BS em Matemática Aplicada e tem trabalhado ativamente nas indústrias de computação e comunicações desde 1996. Sua experiência na carreira inclui projeto de segurança de rede, arquitetura de rede CS, desenvolvimento de produtos incorporados, simulação ASIC e projeto de firmware com desenvolvimento de aplicativos RTOS. O Sr. Gammel é atualmente um diretor de pesquisa e desenvolvimento na Schweitzer Engineering Laboratories, Inc. (SEL), responsável pela tecnologia de segurança desenvolvida e implementada nas linhas de produtos da SEL. Ele trabalha na SEL desde março de 2005 e tem mais de 20 anos de experiência em segurança de engenharia de rede e firmware.

Jess Smith é uma Engenheira de Pesquisa na Schweitzer Engineering Laboratories com um PhD em Ciência da Computação e um MS em Engenharia de Computação. Ela tem experiência trabalhando tanto para o governo quanto para a indústria no setor da segurança cibernética. Na indústria, Dra. Smith tem focado em ambos os métodos de integração segura de sistemas de controle com a internet moderna e nos esforços para melhor educar as empresas de controle de energia elétrica sobre a segurança de seus sistemas de controle. As áreas de pesquisa da Dra. Smith incluem segurança de sistemas de controle e segurança da cadeia de suprimento.

© 2016 por Schweitzer Engineering Laboratories, Inc.
Todos os direitos reservados.
20161014 • TP6774-01