SEGURANÇA CIBERNÉTICA

MATEUS M. COELHO, SÉRGIO CORDEIRO, ALAN OLIVEIRA

Introdução

Quem pôde acompanhar o Jornal Nacional exibido no último dia 18 viu como um hacker divulgou que invadiria o sistema de controle de um avião em pleno vôo. A polícia federal dos Estados Unidos, o FBI, só chegou ao hacker Chris Roberts devido ao fato dele ter publicado em redes sociais que acessaria os sistemas de vídeo da aeronave e o sistema que controla as máscaras de despressurização de gás. Chris afirmou que entre 2011 e 2014 invadiu mais de 15 vezes os sistemas de controle de aviões, chegou a mudar a altitude e a rota de um vôo e também fez com que um avião voasse ligeiramente de lado; tudo foi possível devido ao fato de Chris ter roubado os códigos de segurança da aeronave durante a realização de um vôo. O FBI investiga o caso para apurar se as alegações são verdadeiras. Com matérias assim devemos questionar: até onde estamos seguros do ponto de vista cibernético? quais são nossas maiores armas de defesa?
Os artigos lidos ajudam a compreender as práticas de segurança digital pelo mundo e os ataques cibernéticos que já foram realizados, bem como as principais causas destes ataques. Foram analisados os seguintes trabalhos:

- artigo: ***Cybersecurity Essentials for Electric Operators***
- artigo: ***Smart Grid Cyber Security***
  artigo complementar consultado:
  - *Markets for Cybercrime Tools and Stolen Data* - Rand Corporation (`http://www.rand.org/pubs/research_reports/RR610.html`)
- artigo: **NERC CIP e SMART Grid: Como eles se encaixam?**
- artigo: ***Analysis of the Siemens WinCC/PCS7 "Stuxnet" Malware for Industrial Control System Professionals***
  artigos complementares consultados:
  - *To Kill a Centrifuge. A Technical Analysis of What Stuxnet's Creators Tried to Achieve* - R. Langner (`http://www.langner.com/en/wp-content/uploads/2013/11/To-kill-a-centrifuge.pdf`)
  - *A Forensic Dissection of Stuxnet* - Nachenberg (`http://www.ttivanguard.com/ttivanguard_cfmfiles/pdf/sanjose12/sanjose12session7117.pdf`)

Importância do tema

Uma das principais fontes de suprimentos mundial é a energia elétrica. Um ataque ao setor elétrico de uma nação que não possui um sistema consistente de proteção para evitar e/ou reestabelecer o fornecimento após um ataque pode acarretar em grandes transtornos. A Segurança Cibernética tem sido um problema negligenciado por operadores de infra-estrutura crítica por quase duas décadas - mas agora, com a possibilidade de ataque aos avançados sistemas de controle industrial é imperativo para operadores de sistemas elétricos tratar pontos fracos críticos da sua rede e sua segurança operacional.
O setor elétrico está no topo da lista dos ataques a sistemas de controle industriais. Existem 2 vetores de ataques para o hacker industrial: os ICS (Sistemas de Controles Industriais), que controlam os processos físicos de uma planta ou concessionária, e os computadores internos da rede usados para operações não críticas e tarefas administrativas. O pior cenário para um operador de sistema elétrico é uma brecha no ICS, mas um ataque na rede interna pode ser também altamente danoso, particularmente se esta rede se conecta com o ICS.
Montar um plano de negócio para segurança em smart-grids é difícil devido a incertezas quanto ao tipo e gravidade das ameaças, a quem deve pagar o investimento e aos custos reais do esforço. Existem ainda barreiras institucionais e culturais ao trabalho. Os trabalhos examinados permitem analisar todas essas dificuldades e propor respostas a elas.

Conceitos

Tipos de hackers. Um mapeamento realizado já traça o perfil de possíveis ameaças cibernéticas e hoje temos 04 ameaças conhecidas que descrevemos a seguir:

Estado-Nação. Um dos mais temidos hackers, ou qualquer outra organização, é o tipo Estado-Nação. Este tipo possui elevados recursos financeiros e consequentemente maior capacidade para lançar um ataque sofisticado, podendo mantê-lo por um prolongado período se necessário. Há significante diferença na forma de atacar, variando de acordo com o objetivo. Exemplos: a China vem fazendo ataques sofisticados e eficientes há décadas nos Estados Unidos em busca de reunir informações sobre as operações, pesquisas e desenvolvimento, planos de negócios, propriedade intelectual, e não com o objetivo de interromper sistemas ou destruir equipamentos. O Irã é exatamente o oposto, por objetivar a destruição ou interrupção do funcionamento de qualquer atividade.

Hackvitivistas. O mais conhecido e influenciável grupo hacktivista é o Anonymous, que passou por uma série de 3 anos de ataques aleatórios a empresas e organizações governamentais baseado em várias motivações. A motivação principal é a publicidade, ou exposição pública, porém o dano causado pode ser sério, particularmente se dados internos das empresas ou instituições atacadas forem capturados e/ou expostos.

Individuo. Os ataques cibernéticos podem ser conduzidos por um indivíduo sozinho por motivos que variam desde ganho financeiro, por vingança ou simplesmente um desejo de provar que ele pode hackear determinada empresa. Como hoje existem muitos softwares maliciosos de prateleira que qualquer pessoa pode comprar online e modificá-lo para uso particular, o indivíduo é uma ameaça real, não muito para sistemas de controle industriais, mas para redes corporativas internas. A mais séria ameaça via "indivíduo"é o funcionário desonesto que pode ter acesso a sistemas importantes da empresa.

Crime organizado. O crime organizado desempenha um papel substancial no submundo dos hackers, particularmente quando se trata do desenvolvimento de robôs virtuais (redes de PCs infectados), desenvolvimento e venda de softwares maliciosos, venda de dados roubados ou acesso remoto a redes corporativas. A motivação principal, obviamente, é o dinheiro. Os ataques são feitos não para destruir a máquina, mas para obter informações ou acessos a redes que possam ser vendidos posteriormente.

Ameaças de ataques cibernéticos. Um sistema de controle industrial pode ser atacado de 3 maneiras:

1) Ataque ao computador da rede interno do operador que possui uma porta que não seja isolada do sistema de controle industrial;
2) Descoberta de conexão de internet direta com alguma porta do ICS;
3) Obtenção de acesso no local físico do sistema de controle industrial.

O ICS é certamente o prêmio para o hacker, mas a rede interna da instalação elétrica pode ser também uma mina de ouro. Muitas vezes é mais fácil para o hacker manter presença neste tipo de rede do que em nos sistemas de controle industriais. A rede interna pode ser atacada de várias maneiras. A mais comum é o ataque "phishing", no qual um email é enviado aos empregados com um anexo infectado ou link, sendo mais eficientes quando são utilizadas mídias sociais para obter informações pessoais que tornam o contato mais convincente. Outra maneira comum de obter acesso é encontrar uma falha na segurança de rede, que pode ser uma senha fraca, VPN mal gerenciada, segurança de internet insuficiente, etc.
A invasão de um sistema de controle de uma planta industrial pode representar a o acesso aos dados sigilosos da instalação, onde os mesmos podem ser divulgados ou

até mesmo vendidos para concorrentes, ainda há as ameaças de instalação de vírus que deixaram abertas as possibilidades de ataques e acompanhamento em tempo real dos passos deta instalação interferindo diretamente no seu controle diário.

Outros conceitos importantes. Os **objetivos** das práticas de segurança cibernética em smart-grids devem ser os seguintes:

- proteção da infraestrutura crítica envolvida na geração e distribuição de eletricidade
- proteção do sigilo dos dados dos consumidores

Um sistema seguro deve exibir as seguintes **propriedades**:

- Confidencialidade dos dados
- Disponibilidade dos serviços
- Integridade dos dados
- Autenticação
- Imputabilidade

As **ameaças** à segurança podem ser divididas em:

- ataque malicioso
- acidentes (erros humanos, desastres naturais, falhas no equipamento)

As **dificuldades** que identificadas neste momento são:

- Limitação de recursos
- Limitação de conhecimento técnico
- Reduzido relato de incidentes
- Poucas parcerias governo-indústria
- Pequena coordenação entre diversas agências governamentais
- Existência de sistemas legados
- Necessidade de pessoal altamente especializado
- Avanço tecnológico dos atacantes maliciosos

Entre elas, acreditamos que a existência de sistemas legados não vá desaparecer ou diminuir com o tempo. Com relação ao avanço tecnológico dos atacantes maliciosos, o artigo complementar estudado mostra que já existe uma economia subterrânea baseada na exploração de software malicioso.

Estudo de caso com lições para a indústria elétrica: Stuxnet. O Stuxnet é um vírus projetado para a invasão do sistema SCADA que controla a planta de enriquecimento de Urânio de Natanz (Irã). Os sistemas desenvolvidos pela empresa alemã Siemens e pela norte americana Microsoft são suas principais fontes de ataque. Trata-se do mais complexo vírus criado para atacar sistemas: consegue programar e sabotar diversos processos industriais, o primeiro ataque registrado a um sistema SCADA na história. Descoberto em 2010, vem sendo analisado até hoje; posteriormente, descobriu-se uma versão anterior, datada de 2005. O Stuxnet foi provavelmente desenvolvido por um estado nacional.
Foram desenvolvidas, pelos principais fabricantes de antivírus, ferramentas capazes de identificar a infecção e eliminá-la. Para prevenção de novas infecções, recomenda-se:

- Antivírus/Instalação Lista Branca: Aplicável para todos os sistemas operacionais Windows
- Nos computadores mais vulneráveis recomenda-se que sejam instalados um antivírus ou software de lista branca
- Drivers USB devem ser evitados em sistemas operacionais Windows
- Se necessário o uso de drives USB, pré-qualificá-los antes de instalá-los em um computador.
- Autorun deve ser desabilitado para todos os drivers, devido ao fato das primeiras versões do Stuxnet terem sido carregados através desta funcionalidade
- Desabilitar a exibição de ícones de atalhos
- Desativar o serviço WebClient
- Desativar a conta do convidado; o invasor deve ser autenticado para ter acesso à rede

Descrição. Para se instalar num hospedeiro, o Stuxnet explora 4 vulnerabilidades do Windows desconhecidas à época, que lhe permitem se propagar através de portas USB e/ou pela rede Ethernet local. Explora também características específicas da plataforma Siemens para infectar arquivos contendo programas em linguagem STEP 7. Finalmente, explora características específicas da planta alvo para localizar o alvo e atingi-lo, sabotando o processo.
Diversas versões de Windows, incluindo Windows 2000, Windows XP, Windows Server 2003, Windows Vista, Windows Server 2008 e Windows 7 são vulneráveis ao ataque. Todos os sistemas da Siemens utilizando o software de programação STEP 7 são vulneráveis.
O ciclo de vida do software é o seguinte:

- inserido em PCs de empresas de engenharia no Irã por meio de drives USB
- conecta-se a um centro de controle remoto

- infecta novas máquinas pela rede Ethernet ou por meio de drives USB
- quando encontra uma estação de engenharia Siemens, infecta arquivos específicos da plataforma
- quando se encontra na planta alvo, infecta os PLCs
- periodicamente, executa a ação de ataque

Efetivamente, consiste em duas partes:

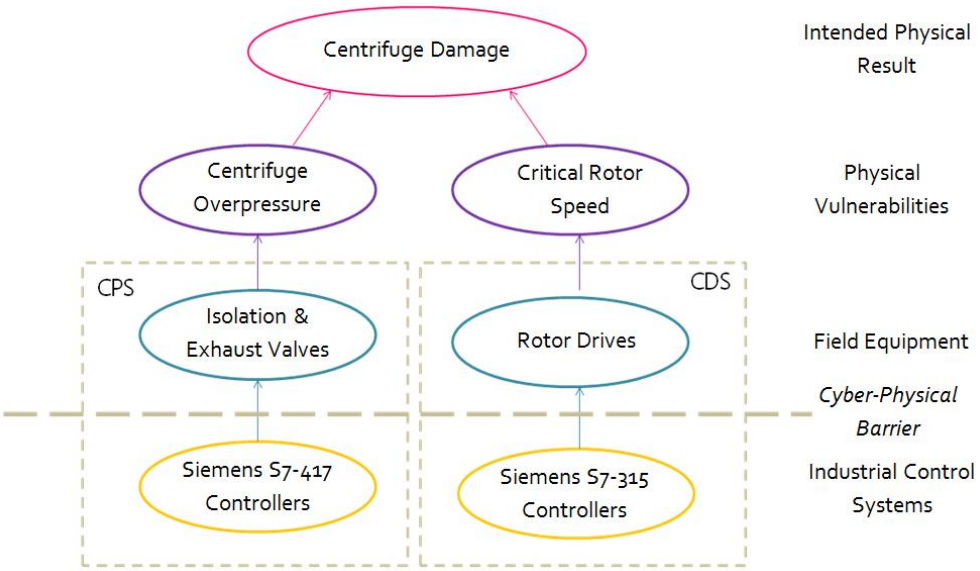
- um verme (*worm*) que propaga a infecção
  - Explora as vulnerabilidades do sistema para se instalar e se propagar
  - Verifica se deve instalar o núcleo
  - Comunica-se com o centro de controle remoto para receber atualizações e instruções e registrar suas ações
- um núcleo, que executa o ataque
  - Infecta DLL da Siemens que faz interface entre o PC e o PLC
  - Infecta arquivos de programa Step 7 quando o programador é executado
  - Programa infectado é eventualmente copiado para o PLC pelo programador
  - Após a infecção, o ataque é executado periodicamente pelo programa infectado

Além de verme, tem características de vírus e de *rootkit*, além de ser polimórfico. O verme se comporta de forma tradicional; a única característica notável é o fato de explorar muitas vulnerabilidades inéditas à época. O núcleo é a parte que apresenta maiores novidades:

- Infecta o PLC, não apenas o PC
- Explora vulnerabilidades da plataforma Siemens:
  - senha fixa entre o WinCC e o SQLServer
  - blocos podem ser criptografados
- Explora características específicas da planta alvo:
  - Endereços de I/O determinados
  - Processo de controle de velocidade das centrífugas
  - Processo de regulação de pressão nas centrífugas (versão antiga)

O ataque existe em duas versões, a mais antiga e a mais nova. Na versão antiga, o Stuxnet fechava determinadas válvulas de forma a fazer aumentar a pressão em algumas centrífugas, impedia a abertura das válvulas de alívio de pressão e apresentava ao operador dados falsos sobre o processo, para evitar intervenção manual. Na versão recente, ele aumentava o setpoint do inversor em 40% ou diminuia para uma velocidade muito baixa; depois de alguns minutos, voltava ao

normal. Em ambas as versões, executava o ataque com pequenas frequência e duração, para evitar ser identificado.



O objetivo do ataque era danificar o equipamento no médio prazo. Não se tem confirmação do sucesso do ataque, mas aparentemente 10% das centrífugas foram danificadas.

Conclusão. O ataque do Stuxnet não poderia ter sido evitado por meios tradicionais. Os danos (e talvez também a infecção) seriam evitados por meio de boas práticas de engenharia. As defesas tradicionais, que consistem em *hardening*/*patching*/atualizações de software/firmware, segregação/segmentação das redes, monitoramento da rede, bloqueio de portas USB, equipe de resposta a incidentes, anti-virus/descobridor de *rootkits*, AAA (*autentication, authorization and auditing*) e certificados digitais, não poderiam ter evitado o ataque. Por outro lado, medidas como:

- Virtualização de desktops (VDI) e de servidores (na reinicialização sempre se lê uma imagem não corrompida)
- Uso de controle de versão centralizado (controle do que foi alterado de uma versão para a outra)
- Uso de relés de segurança, válvulas auto-operadas, sistemas redundantes, maior monitoramento (robustez do projeto de automação)
- Dimensionamento correto dos equipamentos (robustez dos projetos elétrico e mecânico)

- Uso de software de código aberto, que facilita a análise

poderiam ter evitado ou minimizado seus efeitos.

Problemas de longo prazo para operadores do sistema elétrico. Os operadores de sistemas elétricos necessitam considerar 4 problemas crônicos que irão existir por algum tempo:

Falhas zero-day. São falhas ou bugs em um programa ou software que ninguém tem conhecimento. Não há um meio real de se prevenir de um zero-day nos softwares ou sistemas adquiridos de desenvolvedores de software terceirizados.

Sistemas ICS projetados sem segurança cibernética. Sistemas ICS e SCADA são inseguros por natureza. Foram originalmente desenvolvidos quando o acesso via internet a esses sistemas não era considerado um risco. Muitos deles vêem com senhas padronizadas do fabricante ou impossibilitam a troca de senhas de acesso. A substituição destes sistemas não é viável.

Erros de empregados. Um empregado não é um expert em segurança, podendo vir a abrir qualquer email, clicar em qualquer link, visitar qualquer site da internet, comprometendo assim a rede.

Dificuldade de atribuição. É quase impossível atribuir a qual país, organização ou pessoa veio cada ataque cibernético, com 100% de certeza. Muitos crimes não serão investigados ou identificados os responsáveis, podendo os ataques vir a acontecer novamente. O foco do plano de segurança cibernética deveria ser na prevenção.

Conselhos de segurança. Operadores do sistema elétrico necessitam tomar medidas proativas de segurança cibernética para reduzir as ameaças que podem ocorrer.
Um bom plano de segurança cibernética é aquele que busca a prevenção de ameaças antes delas atingirem as máquinas dos empregados, e é capaz de conter o dano e previnir que a infecção se espalhe após um ataque bem sucedido.
Tecnologias de redes inteligentes lidam com o controle do uso da eletricidade pelos consumidores e afetam de forma abrangente a confiabilidade e eficiência do sistema de distribuição de energia visto que a eletricidade está cada vez mais incorporada no cotidiano e nas operações de negócios críticos. Assim, as redes inteligentes necessitam ser desenvolvidas com segurança contra invasões cibernéticas, mau uso e operações sem cuidado.
Apenas o atendimento às normas de segurança não deve ser considerado como

suficiente, pois são a barreira mínima do que deve ser feito para proteger sua organização das avançadas e persistentes ameaças. Considerando a sofisticada natureza dos atuais ataques cibernéticos e as crônicas fraquesas dos sistemas ICS e SCADA, existem nove elementos essenciais para um robusto programa de segurança cibernética para operadores do sistema elétrico:

1) Isolação física (air-gapping) para todos os sistemas de controle industrial
2) Atualização inicial e periódica de todas as senhas e códigos de acesso a ICS e sistemas SCADA
3) Proibição do uso de drives USB de terceiros na rede da companhia
4) Segmentação das redes e das informações
5) Configuração de listas brancas (white lists) para softwares e programas nos computadores de executivos
6) Implementar defesas robustas no perímetro da rede, para proteger tanto a intrusão quanto a evação de informações
7) Verificar se não há redes Wi-Fi conectadas na rede principal
8) Determinar um plano de recuperação ou resposta para situações nas quais a rede for comprometida
9) Treinamento dos empregados

Implementando a segurança. Os três principais grupos de medidas são a regulação, a análise de risco e a defesa em profundidade. Todas já são utilizadsa pela TI corporativa. A regulação ataca a rejeição organizacional, mas é difícil de se executar devido à diversidade das situações encontradas, pode causar problemas colaterais (por exemplo, influenciar na escolha do equipamento usado) e também pode "engessar"demais os agentes. A análise de risco ataca a dificuldade de se elaborar um orçamento realista; nela, o benefício a ser obtido consiste na prevenção de custos provocados por um incidente. Na prática, é difícil de se executar devido ao número de combinações possível dos fatores e pelos fatos de dever ser executada continuamente e de depender de relatos de incidentes acontecidos. A defesa em profundidade constitui um passo adiante da pura regulação. Ela proporciona flexibilidade aos agentes, mas deve ser combinada com boas práticas reconhecidas pela indústria para melhorar a prevenção de incidentes.
O Cigrè propôs um conjunto de medidas preparatórias que o ISGAN também adotou:

- Implementar um processo de gerenciamento de risco
- Estabelecer a política de segurança
- Alocar os recursos necessários
- Educar e involver as pessoas

Semelhanças e potenciais oportunidades compartilhadas. Por que as concessionárias de energia devem coordenar esforços e como fazê-lo? Existem várias respostas positivas:

1) As curvas de aprendizado em cibersegurança são semelhantes;
2) Muitas áreas de ameaça sobrepõem-se onde as melhores práticas de processos e tecnologia são comumente aplicadas;
3) Existem oportunidades no compartilhamento da ampla área de infraestrutura de comunicação, presumindo-se que os problemas de conformidade não interiram;
4) A potencialidade de alinhamento regulatório, evitando a duplicação de normas e estruturas de conformidade.

Conclusão

O conjunto de medidas proposto pelo ISGAN, baseado em suas pesquisas e também no trabalho realizado anteriormente pelo Cigrè, constituem um bom começo para se implantar a segurança cibernética na automação do sistema elétrico. Uma limitação óbvia é que ele só contempla as primeiras etapas da tarefa; uma outra é que elas são bastante genéricas. O trabalho precisa ser continuamente refinado com agregação de informações derivadas pela experiência concreta e propostas de medidas mais avançadas e mais específicas. NERC CIP se concentra principalmente em ativos operados e de propriedade de concessionárias de energia, particularmente sistemas primários e ativos de subestações de energia. Em contraste, sistemas de redes inteligentes incluem dispositivos de propriedade dos clientes e redes de comunicação também de propriedade de clientes. Além disso, podem lidar com questões de privacidade (ex. AMI) que não estão previstas no NERC CIP.
Segurança cibernética é um elemento essencial de todas as iniciativas em redes inteligentes. Concessionárias, fornecedores de tecnologia e formuladores de políticas têm papéis importantes para acelerar a entrega das redes da próxima geração. Muitas empresas adotam uma estratégia de fuga das normas NERC CIP, que consiste na minimização do escopo de conformidade da norma através da minimização do número de subestações críticas e evitando a classificação de ativos críticos como cyberativos por não possuírem conexões roteáveis ou do tipo dial-up. Esta é um nítido contraste em relação ao espírito das redes inteligentes que promovem o uso generalizado de arquiteturas abertas e baseadas em comunicação IP.