CRITÉRIOS DE SEGURANÇA PARA SISTEMAS SCADA EM REDE CORPORATIVA

Alexandre Acácio de Andrade*, Lucas Becker†, Luis Fernando Quintino*, José eduardo da costa dias†

* *Rua São Paulo, s/n*
Jardim Antares
São Bernardo do Campo, São Paulo, Brasil

† *Avenida dos Estados, 5001*
Bairro Santa Terezinha
Santo André, São Paulo, Brasil

Emails: aacacio@ufabc.edu.br, lcs.becker@hotmail.com, luis.quintino@outlook.com, jecdias@yahoo.com.br

Abstract— The growing demand for high connectivity among all enterprise levels imposed by the new Connected Enterprise Environment, brings new concern about the supervisory control data and acquisition systems - SCADA security. Originally isolated, SCADA systems are being connected to enterprise networks and to the internet. They differ from the typical IT casual systems on its dedicated architecture, communication protocols, and security priorities. Trough the text it will be identified the main characteristics of the SCADA systems and its safety requirements in a interconnected environment.

Keywords— Information Security, SCADA Security, SCADA, Industrial Ethernet.

Resumo— A demanda crescente por alta conectividade entre todos os níveis corporativos impulsionada pelo novo panorama da industria conectada ou 4.0, trouxe além dos benefícios, diversas preocupações quanto a segurança de sistemas supervisórios de controle e aquisição de dados - SCADA. Antes isolados, os sistemas SCADA passam a ser interligados com as redes corporativas e a internet. Diferente dos sistemas convencionais de TI (Técnologia da Informação), os sistemas SCADA possuem uma arquitetura particular, protocolos de rede dedicado e distintas prioridades de segurança. Nesse trabalho será alavancado as principais características dos sistemas SCADA e os critérios para sua proteção em um ambiente de interconectividade.

Palavras-chave— Segurança da Informação, Segurança SCADA, SCADA, Ethernet Industrial

1 Introdução

Ataques a sistemas SCADA trazem impactos devastadores. Com o devido acesso um sabotador pode facilmente roubar segredos industriais, destruir parques fabris e até causar perigo de vida a diversas pessoas. Por sua facilidade o ataque a esse tipo de sistema tornou-se de grande atratividade para serviços de espionagem, terroristas, ex empregados frustrados, criminosos, hacker ativistas entre outros. (Falliere et al., 2011)

Os ataques podem ser de característicafísica, quando se sabota o sistema por alguma configuração do hardware, ou via software. Tradicionalmente o sistemas SCADA eram isolados, não trocando dados com a rede corporativa, tal situação "blindava" o sistema a ataques externos, ficando relegados apenas a sabotadores internos. No entanto, dado ao paradigma colocado pela industria 4.0 de alta conexão entre todas as camadas da piramide de automação, os sistemas SCADA vem sendo conectados as redes corporativas muitas vezes sem o devido cuidado, deixando sistemas de automação inteiro vuneráveis a ataques via web. (Igure et al., 2006)

As ferramentas de mitigação de ataques a sistemas SCADA são muito semelhantes as utilizadas em TI, no entanto a abordagem e o foco do tipo de defesa são distintos. Existem diversas caracteristicas fatais para automação e toleráveis para TI e vice versa, deste modo se faz necessário o apontamento dos critérios de funcionamento exigido por uma rede SCADA segura antes de abordar a natureza da solução. As diferenças fundamentais entre as exigências de segurança para automação e TI estão colocadas na Tab. 1 .

Tabela 1: SCADA x TI Particularidades nos Critérios de Segurança

Critério	Sistema Scada	TI - Redes e Computadores
Perda de dados e interrupções	Não podem ser tolerados, risco de dano sério ao sistema	Podem ser tolerados e solucionados por rotinas de restauração do sistema

(contínuação)

Critério	Sistema Scada	TI - Redes e Computadores
Atrasos *"Delays"*	Determinismo é prioritário! atrasos são intoleráveis	"delays"são toleráveis
Antivírus	Difícil aplicação, seu processamento pode causar *delays* impactando no determinismo.	São via de regra implementados
Criptografia	Pouco difundida	Largamente utilizada
Teste de Penetração (Simulação de Ataque)	Falta de procedimento padrão,pode impactar em danos permanentes ao sistema	Usualmente utilizado como política de TI para melhoria contínua dos padrões de segurança.
Atualização de Sofware	Atualizações de Firmware e versões de software devem ser feitas com critério, podem afetar permanentemente o funcionamento do sistema	Atualização constante e facilmente reversível
Auditoria de Segurança da informação	Pouco frequente	Frequente.
Frequência na troca de equipamentos	Equipamentos utilizados por longos períodos sem substituição (em média mais de 10 anos)	Equipamentos substituídos em média em cada três anos.
treinamento de políticas de Segurança da Informação	Poucos treinamentos	Treinamentos constantes

Fonte: (Krutz, 2005) & (Igure et al., 2006)

1.1 Protocolos Fieldbus e Conceito de Ethernet Industrial

Os protocolos para redes de TI e TA (tecnologia de automação), começaram a ser desenvolvidos praticamente no mesmo momento, em meados da década de 70, com abordagens distintas. As necessidades de transmissão de dados para TI impunham uma larga banda de transmissão de dados, mas não impunham o determinismo, ou seja, não era imperativo estabelecer o tempo de envio e recebimento de um pacote de informação. As redes de automação por sua vez deveriam atender exatamente o contrário, a característica determinística é fundamental, em especial para sistemas com sincronismo de movimento, enquanto a banda não precisava ser alta dado a natureza padronizada dos pacotes de instrução transmitidos. (Felser and Sauter, 2002)

Desta forma os protocolos para redes de TI padronizados pela IEEE 802.3, ou "protocolo Ethernet", possui uma larga banda de transmissão de dados e baixo determinismo (Tanenbaum et al., 2003), enquanto os protocolos para redes de automação definidos pela norma IEC 61158 ou "protocolo fieldbus", possui alto determinismo e bandas de transmissão mínimas suficientes para atenderem suas necessidades determinísticas (Thomesse, 1998). Caso necessário, ambos as redes de TI no modelo Ethernet, e TA no modelo fieldbus, podem ser interconectados via um dispositivo de interface ou "gateway".

Com a interligação cada vez mais constante de ambas as redes e a maior necessidade de extração de dados da rede de automação, surge uma maior necessidade de banda para redes fieldbus, de modo que fabricantes e associações de automação industrial vem encapsulando, ao logo dos últimos 17 anos, os diferentes tipos de protocolos fieldbus na estrutura de transmissão de dados do protocolo Ethernet. Esse modelo "híbrido" é chamado de "Ethernet Industrial", possui alta banda de transmissão de dados e garante o determinismo de maneiras distintas de acordo com o tipo de protocolo Fieldbus encapsulado. (Winkel, 2006)

Em termos de segurança, é importante em primeiro lugar a observância das especificidades dos protocolos fieldbus e ethernet industrial apontados pelos fabricantes. A título de exemplo o protocolo Ethernet/IP da ODVA, e promovido pela Rockwell Automation atinge o determinismo pela segregação de rede e alta banda disponível, o que implica na utilização de switches gerenciáveis, já o protocolo Profinet da Profibus International e promovido pela Siemens garante o determinismo pelo emprego de switches especiais voltados a Profinet. (Felser and Sauter, 2004) Dessa maneira abordar redes de automação como redes de TI convencionais podem levar a falhas e acidentes.

2 AUTORES DE ATAQUES A SISTEMAS SCADA

2.1 CONCEITO DE GUERRA CIBERNÉTICA "Cyber Warfare"

Com a quantidade cada vez maior de sistemas e infraestruturas críticas conectadas a internet, o ataque cibernético torna-se uma nova ferramenta de guerra, e um tema crítico para segurança nacional. De acordo com o relatório *"In the crossfire: crítical infrastructure in the age of cyber war"* publicado pela companhia de segurança da informação McAfee, cerca de 120 países estão desenvolvendo expertise em guerra cibernética, com destaque para cinco países,China, Estados Unidos, Israel, Rússia e França, que possuem agências e elevado grau de conhecimento na área. (Baker et al., 2009).

além de conflitos entre estados, os mecanismos de guerra cibernética possibilitam um novo campo de atuação a terroristas, criminosos e espiões industriais. (Nicholson et al., 2012). O conhecimento dos possíveis atacantes torna-se fundamental para companhias e estados definirem estratégias de segurança a suas infraestruturas críticas.

2.2 HACKERS ESTATAIS

Tratam-se de agentes contratados por departamentos de inteligência ao redor do mundo, com intuito de promover ações de ataque e defesa e estruturas estratégicas das nações.(Nicholson et al., 2012)

Hackers estatais possuem o maior potencial destrutivo a sistemas SCADA e de TI, pois seu financiamento estatal os possibilitam acesso a uma quantidade infindável de recursos, pessoal, e tecnologia. (Nicholson et al., 2012)

Exemplos de ataques realizados por esse tipo de grupo estaria o vírus Stuxnet, desenvolvido para atacar sistemas SCADA em base SIEMENS. O Stuxnet fora propagado em usinas nucleares Iranianas, provocando a sabotagem de seus sistemas de controle. A análise realizada pelo grupo Symantec aponta que foram necessários mais de uma dezena de engenheiros de software em tempo integral, altamente qualificados, por mais de um ano para desenvolvimento do Stuxnet. Tais recursos empregados e a motivação do ataque a estrutura energética de uma nação específica, levam a conclusão que o virús fora encomendado por algum departamento de inteligência. (Falliere et al., 2011)

2.3 HACKERTERRORISMO

Terroristas são grupos extremistas de uma dada orientação política, religiosa, ou ideológica, que buscam por meio de ações de sabotagem a promover suas ideias. (Baker et al., 2009)

Ainda não há um registro considerável de ataques terroristas cibernético a redes SCADAS, mas considerando os poucos custos e a facilidade envolvida nesses ataques, tais alvos se enquadram como ideais. (Nicholson et al., 2012)

2.4 HACKERS CRIMINOSOS

A modalidade de crime cibernético vem ganhando popularidade nos últimos anos. Em termos gerais, os criminosos sequestram via acesso remoto os sistemas e a infraestrutura de TI de companhias, criptografam o acesso ao sistema, e solicitam uma recompensa em dinheiro para sua liberação. (Nicholson et al., 2012)

Por se tratar de um alvo fácil e estratégico, sistemas SCADA encaixam-se como alvos adequados ao crime cibernético, mesmo que no momento não haja muitos registros de ataques classificados nessa modalidade. (Nicholson et al., 2012)

2.5 EMPREGADOS DESCONTENTES / ATAQUE INTERNO

São os autores mais comuns de ataques internos a sistemas SCADA. A razão para o ataque pode variar de uma vingança a um desligamento indesejado da companhia , conflitos humanos, falta de motivação e reconhecimento, etc.

Um estudo da Internet Security Systems, concluiu que a maior parte das contas de acesso a sistemas SCADA não são nominais, mas sim genéricas, como "administrador", "engenheiro", de forma que a identidade do atacante fica camuflada, facilitante esse tipo de ataque. (Nicholson et al., 2012)

Um exemplo de ataque fora o realizado na estação de tratamento de água de Maroochy na Austrália, onde Vitek Boten, um engenheiro recém demitido da empresa, utilizou acessos conhecidos ao sistema de controle da companhia para transmitir milhares de metros cúbicos de água não tratada ao sistema pluvial da região. (Slay and Miller, 2007)

2.6 "HOBBISTAS"

"Hobbistas" no ambiente de guerra cibernética, são indivíduos cuja motivação de ataques não está em motivos criminosos, ou terroristas, mas sim na superação de desafios pessoais.

Históricamente cita-se o caso do hacker britânico Gary McKinnon, que extraiu informações sigilosas de 90 sistemas militares dos Estados Unidos alegando estar procurando pela evidência da existência de alienígenas. Ou o caso de um garoto polonês de 14 anos que em 2008 hackeou via um sistema de controle remoto o sistema de direção dos bondes elétricos da cidade de Lodz. (Nicholson et al., 2012)

2.7 SCRIPT KIDDIES

"Script Kiddies" , são indivíduos com pouco ou nenhum conhecimento de programação, e que utilizam ferramentas disponibilizadas na internet para executar invasões a sistemas. As motivações dos *"Script Kiddies"* são parecidas com a dos hobbistas, sendo muitas vezes de cunho pessoal. (Nicholson et al., 2012)

2.8 HACKATIVISTAS

Hackativismo corresponde a uma modalidade de ativismo político no ambiente da guerra cibernética. Os Hackativistas tem como motivação sabotar sistemas de corporações, bancos e governos que consideram contrários a sua ideologia política. (Nicholson et al., 2012)

3 FERRAMENTAS DE SEGURANÇA PARA SISTEMAS SCADA

A maioria das redes de comunicação possuem um conjunto de métodos e técnicas comuns de segurança, como por exemplo"firewalls".

A particularidade das redes em ambiente SCADA é que os métodos de segurança não podem :

- interferir no determinismo do tráfego de informações.
- bloquear o acesso do sistema a operadores, mesmo que este tenha errado sua senha de acesso diversas vezes.
- requerer muita memória e longos tempos de processamento.

Mesmo com as restrições citadas, há um conjunto de medidas e melhores práticas normalmente aplicavéis a redes de arquitetura TCP/IP que devem ser considerados na implementação de redes em sistemas SCADA, sendo essas abordadas a seguir.

3.1 FIREWALLS

Trata-se de um elemento de proteção que monitora o fluxo de dados de uma rede confiável para uma rede não confiável tal como a internet . Um firewall fornece proteção contra vírus, códigos maliciosos, e invasões de rede. (Tanenbaum et al., 2003).

3.2 ZONA DESMILITARIZADA (DMZ)

A zona desmilitarizada (DMZ) trata-se de uma "área franca", uma camada que define o limite entre duas redes, no geral uma rede confiável interna e uma rede externa. (Tanenbaum et al., 2003)

A abordagem da implementação de zonas desmilitarizadas possibilita a conexão segura de redes com distintas políticas de seguranças . De modo que o firewall, que está no limite entre a zona corporativa e a desmilitarizada , não permite o tráfego de informações impróprias a rede corporativa, e o firewall no limite da zona de automação impede o fluxo de dados não desejados ao ambiente SCADA.

O monitoramento na transmissão de dados também poderia ser feito apenas com o uso de um único firewall modificado a atender diversas políticas de segurança. No entanto certas políticas de segurança podem não ser completamente conciliatórias de modo que o firewall modificado torna-se como um ponto vulnerável da rede, impactando no conceito de defesa em profundidade *defense-in-deph* (Didier et al., 2011).

3.3 REDE PRIVADA VIRTUAL - VPN

A VPN é caracterizada pela configuração de firewalls nas redes corporativas locais, que criam um "túnel" na internet, permitindo o acesso seguro a rede corporativa por usuários remotos, desde que estes sejam devidamente cadastrados na VPN e obedeçam as normas de tráfego observadas pelo firewall. (Tanenbaum et al., 2003)

3.4 SISTEMAS DETECÇÃO DE INTRUSÃO (IDS) EM AMBIENTE SCADA

Sistemas detecção de intrusão definem-se por soluções de software e hardware desenvolvidos para monitorar as atividades de um computador hospedeiro *host* ou a rede, com intuito de detectar a ocorrência de eventos maliciosos que buscam comprometer a confidenciabilidade, integridade e disponibilidade da rede. (Krutz, 2005)

3.5 PROPOSTA DE ARQUITETURA DE REDE INDUSTRIAL

Em termos gerais, a segurança de redes SCADA e corporativas pode ser resumida em dois termos, segmentação e monitoramento. Todas as ferramentas de segurança abordadas até aqui buscam

auxiliar em uma dessas funções. Em uma rede insegura, toda sua infraestrutura está conectada sem nenhuma definição de permissões, de forma que qualquer um que tenha acesso a rede pode atacá-la.

A segmentação define camadas e níveis de prioridade, onde a jurisdição de um usuário começa e termina. O monitoramento por sua vez identifica quem está fazendo o que e quando, possibilitando a de detecção da fonte de ataques.

Acima de possuir as melhores ferramentas de segurança, é importante definir como implementá-las de forma conjunta, afim de fato complementarem suas funções na garantia da totalidade da segurança do sistema. As propostas de junção dos elementos de segurança com a infraestrutura da define-se como "arquitetura".

O manual *Converged Plantwide Ethernet (CPwE) Deseign and Implementation*, desenvolvido pela Rockwell Automation e a Cisco, aborda os passos e ponderações para uma adequada implementação de uma rede industrial. O documento fornece uma proposta de arquitetura de rede padrão, onde as áreas de controle e manufatura, rede corporativa interna, e rede externa (internet), são segregadas por zonas de desmilitarização e firewalls em seus extremos.

A implementação da arquitetura proposta pelo CPwE deve, assim como comentado, sempre considerar as realidades práticas de aplicação a aplicação. O emprego de outras ferramentas de segurança como softwares IDS, antivírus, etc, também devem ser realizados, desde que devidamente implementados nas camadas de segmentação da arquitetura, afim de otimizar as funções de segurança e não comprometer o funcionamento adequado da rede.

4 APLICAÇÃO DE TÉCNICAS DE SEGURANÇA PARA SISTEMAS SCADA

Nessa seção será abordado em detalhes os princípios, diretrizes e normas mais comumente referenciados na implementação da linha de defesa de sistemas SCADA.

4.1 ISA-99

A ISA (sociedade internacional de automação), buscando padronizar os procedimentos de segurança de sistemas SCADA, estabeleceu uma linha normativa específica para esse tema denominada ISA-99. (Knapp, 2014)

As normas ISA-99 vem sendo atualizadas de acordo com o estabelecimento de novas técnicas de mitigação de risco, sendo as ultimas atualizações lançadas nos ano de 2007.

5 DEFESA EM PROFUNDIDADE

O principio de defesa em profundidade *"Defense in Depth"* trata-se de uma abordagem adotada pelo departamento de defesa dos EUA, e muito comumente utilizado no meio corporativo, para definição de medidas de segurança de redes.

A abordagem de defesa em profundidade parte de três elementos críticos "pessoas, tecnologias, e operações", sendo esses abordados pelos seguintes passos:

- Defesa da rede e da infraestrutura
- Defesa das delimitações da rede
- Defesa do ambiente computacional
- Defesa das infraestruturas de suporte

5.1 ESTRATÉGIA DE IMPLEMENTAÇÃO DA DEFESA EM PROFUNDIDADE

Existem diversas estratégias para a aplicação de uma estratégia de defesa em profundidade, no entanto o documento *"Information Assurance Technical Framework (IATF). Realease 3.1"* publicado pela Agência Nacional de Segurança dos Estados Unidos NSA, adota uma estratégia comumente adotada como padrão, sendo seus passos tratados a seguir.

- Adquirir produtos de fabricação dedicada para sistemas de detecção de intrusão e sistemas de segurança e redes, e os instalar com um time interno de desenvolvimento não terceirizando essa tarefa
- Conduzir avaliações de vulnerabilidade.
- Conduzir treinamentos de segurança e de conscientização da necessidade das políticas de segurança.
- Criar um planejamento para caso de eventos maliciosos.
- Crie controle de segurança com redundância.
- Certifique que apenas pessoas autorizadas possam ter acesso físico as instalações da companhia.
- Instalar sistema de detecção de intrusão e criar plano de relatório de intrusão.

O documento também salienta os tipos mais comuns de ataque a sistemas SCADA e a estratégia para mitigá-los, sendo esses ataques listados na sequência.

- **Passivo** : Interceptação de senha, monitoramento de redes de comunicação abertas.
- **Ativo** : Vírus, roubo de informação, quebra de criptografia

- **Próximo**: Ataques realizados por agentes próximos fisicamente da rede e os usuários.
- **"Insiders"**: Ataques realizados por agentes dentro da própria companhia.
- **Distribuição** : Modificação maliciosa de software durante sua estadia na fábrica ou durante a distribuição do software

6 21 PASSOS PARA AUMENTAR A SEGURANÇA CIBERNÉTICA DE REDES SCADA

Visando criar um guia orientativo de boas práticas de seguraça para sistemas SCADA, o comitê de proteção presidencial as infraestruturas críticas dos EUA, juntamente com o departamento de energia Estadunidense, lançaram o documento intitulado *Os 21 passos para aumentar a segurança cibernética de redes SCADA* em setembro de 2002. (DoE, 2002). O documento é proposto como um material auxiliar para complementar as políticas e medidas de segurança de sistemas SCADA já existentes.

1. Identificar todas as conexões ao sistema SCADA
2. Desconectar qualquer conexão desnecessária ao sistema SCADA
3. Avaliar e fortalecer os níveis de segurança das conexões necessárias ao sistema SCADA
4. Blinde as redes SCADA de acessos não desejáveis desabilitando ou removendo serviços não utilizados.
5. Não confie na falsa "impenetrabilidade" de protocolos proprietários para proteção do sistema
6. Implemente as medidas de segurança do equipamento orientadas pelo fabricante
7. Estabeleça uma forte relação de controle sobre qualquer meio de acesso ao sistema SCADA (roteadores, modens , gatways, etc)
8. Implemente sistemas de monitoramento de intrusão e estabeleça monitoramento uma rotina de 24 horas de monitoramento de incidentes
9. Realize auditorias técnicas nos dispositivos do sistema SCADA e suas redes implementadas, assim como qualquer rede conectada ao sistema, afim de identificar ameaças a segurança.
10. Realize levantamento físico da segurança de acesso ao sistema SCADA e suas conexões.
11. Estabeleça "Equipes de Segurança SCADA" responsáveis por identificar e avaliar possíveis cenários de ataque .
12. Defina os níveis de prioridade dos usuários desde o administrador ao usuário final, definindo responsabilidade e o papel de cada usuário na manutenção da segurança cibernética.
13. Documente a arquitetura de Rede e identifique sistemas que fornecem funções críticas ou contem informações sensíveis que necessitem de níveis adicionais de proteção.
14. Estabeleça um processo rigoroso de gerenciamento de riscos.
15. Crie uma estratégia de proteção de rede baseada no principio da "defesa em profundidade" *Defense-in-depth*
16. Identifique de forma clara os requisitos de segurança cibernética.
17. Estabeleça processos efetivos de gerenciamento da rede.
18. Conduza rotinas de auto-acesso, afim de detectar vulnerabilidades no acesso do sistema.
19. Crie backups do sistema e planos de recuperação em caso de desastres.
20. O grupo diretor da companhia deve fomentar um constante clima de seriedade na implementação das medidas de segurança cibernética
21. Estabelecer políticas, e conduzir treinamentos afim de conscientizar as pessoas dos riscos relacionados a segurança cibernética, e fazê-las cooperar com o sigilo das informações do sistema.

7 EXEMPLO DE GRAU DE VUNERABILIDADE DE SISTEMAS SCADA INSEGUROS CONECTADOS A INTERNET

Buscando demonstrar a grande vulnerabilidade e a falha de aplicações de políticas adequadas de segurança, será documentado nesta seção, passos simples para se estabelecer uma conexão com qualquer sistema SCADA inseguro conectado a internet.

Dispositivos conectados a internet deixam "marcas" ou "foot printing" na rede, próprias de seus fabricantes, ou pelo padrão dos protocolos e portas de comunicação utilizados. Desta forma, com o auxílio de alguma ferramenta de scanner

de rede, é possível encontrar todos os dispositivos conectados a internet de determinado fabricante assim como seus endereços de IP públicos. (Knapp, 2014)

Uma vez identificando o endereço de IP público de alguma CPU de controlador, ou cartão de Ethernet contacto a rede, pode-se estabelecer comunicação com o sistema SCADA a distância, e com as ferramentas de softwares do fabricante sabotar , espionar ou copiar programações e rotinas de manufatura de sistemas de automação.

Dentre as ferramentas de scanner de rede, destaca-se o portal SHODAN (www.shodan.io). O portal SHODAN permite a busca de dispositivos na rede por fabricante, endereço físico, portas, protocolos de comunicação utilizados etc. O objetivo dos desenvolvedores do portal é possibilitar uma ferramenta poderosa que auxilie companhias a verificar o nível de segurança de suas aplicações online, assim como providenciar estatísticas de utilização da rede, por exemplo numero de TVs inteligentes por fabricante num dado país etc. Da mesma forma que o SHODAN traz seus benefícios, torna-se também uma ferramenta muito útil para invasão e sequestro de sistemas inseguros conectados a internet. (Knapp, 2014)

Em sua versão gratuita o SHODAN possibilita realizar uma busca com até 10 resultados, tal limitação é eliminada com a compra de uma licença paga no portal.

A título de exemplo, a fig. 1 retrata a busca de cartões Ethernet 1756-ENBT da Rockwell Automation / Allen-Brandley, conectados de maneira insegura na internet. Nos resultados é possível observar os endereços de IP público dos dispositivos, seus países de origem, numeros de série, fabricantes e endereços de IP local.

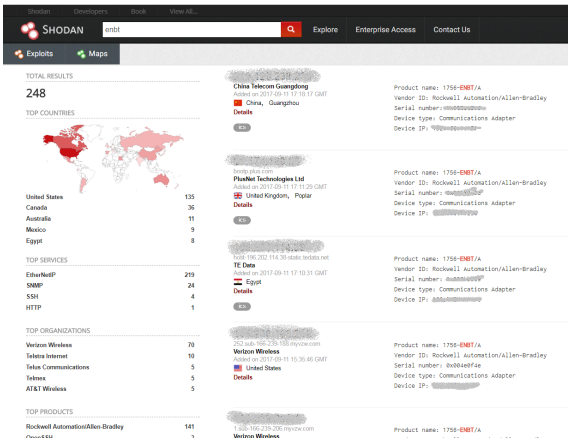

Figura 1: Exemplo de Busca do Cartões Ethernet 1756-ENBT da Rockwell Automation Conectados de Maneira Insegura a Internet

8 ESTABELECENDO COMUNICAÇÃO COM SISTEMA SCADA INSEGURO

A busca no portal SHODAN proporcionou diversos endereços de IP públicos atribuídos a cartões ethernet 1756-ENBT da Rockwell Automation/ Allen Brandley ao redor do mudo. A titulo de seguir com a demonstração, selecionou-se o cartão 1756-ENBT de endereço“196.202.114.38” provindo de uma aplicação de sistema SCADA no Egito.

Através do comando “ping” testou-se no “prompt” de comando do windows a comunicação com cartão, sendo essa estabelecida com sucesso conforme observado na fig. 2.

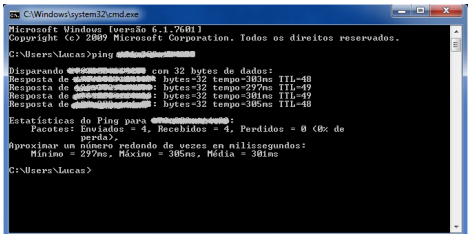

Figura 2: Teste de Comunicação com Cartão 1756-ENBT de Aplicação Remota Insegura

Possuindo os softwares de interface do fabricante, agora é possível estabelecer comunicação com o sistema SCADA remoto, isso possibilita reprogramar controladores, realizar “download” e “upload” de programas, mudar versões de firmware dos cartões do controlador, desligar periféricos etc. Nesta demonstração apenas se estabeleceu a comunicação com o sistema SCADA remoto via o software de interface de comunicação da Rockwell Automation “RSLinx Classic”, cuja versão gratuita pode ser baixada diretamente pelo site da Rockwell Automation.

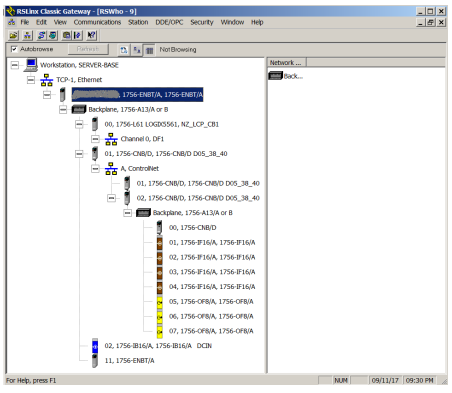

Figura 3: Estabelecimento de Comunicação com Sistema SCADA inseguro via software “RSLinx Classic”

Em resumo essa demonstração deixou claro, que apenas com ferramentas gratuitas e em poucos minutos é possível estabelecer comunicação e realizar ataques a sistemas SCADA inseguros, caindo

por terra a teoria da "invunerabilidade de sistemas SCADA.

9 CONCLUSÕES

A problemática posta neste trabalho enaltece a importância da mudança de mentalidade quanto a redes de automação conectadas a sistemas corporativos e a internet.

Como sistemas de automação foram por anos tratados como "ilhas" e não classificadas como parte da infraestrutura de TI, falta esclarecimento na hora de conectar o mundo da automação a redes externas, levando grandes empresas e departamentos públicos a simplesmente "conectarem" a rede de automação a redes externas sem nenhuma clara política de segurança. Pontos falhos como este levam a grandes ameaças como a exposta neste trabalho, onde em apenas 15 minutos com uma busca na internet e um software gratuito fora possível estabelecer uma conexão com um sistema supervisório de tratamento de água e esgoto.

A implementação dos métodos de mitigação de ameaças apresentados exigem um trabalho específico cenário a cenário conforme a arquitetura de rede da planta industrial. Isso não exige necessariamente uma parada nas operações da planta, mas sim um planejamento minucioso tanto de infraestrutura como de treinamento humano para possibilitar conectar as antigas "ilhas de automação" a redes externas de forma a mitigar ao máximo os riscos de um ataque.

Por fim, na era do cybernético, o cyberterrorismo e a guerra cibernética, ambientes SCADA tornam-se os alvos de maior impacto físico e econômico, além de serem atualmente mais vulneráveis as redes de TI dado a pouco importância que se dá a segurança de suas redes. É importante salientar que este é um tema de segurança nacional e que sua importância deve ser enfatizado para toda a comunidade industrial.

Referências

Baker, S. A., Waterman, S. and Ivanov, G. (2009). *In the crossfire: Critical infrastructure in the age of cyber war*, McAfee, Incorporated.

Didier, P., Macias, F., Harstad, J., Antholine, R., Johnston, S. A., Piyevsky, S., Schillace, M., Wilcox, G., Zaniewski, D. and Zuponcic, S. (2011). Converged plantwide ethernet (cpwe) design and implementation guide, *Cisco Systems and Rockwell Automation* .

DoE, U. (2002). 21 steps to improve cyber security of scada networks.

Falliere, N., Murchu, L. O. and Chien, E. (2011). W32. stuxnet dossier, *White paper, Symantec Corp., Security Response* **5**(6): 29.

Felser, M. and Sauter, T. (2002). The fieldbus war: history or short break between battles?, *Factory Communication Systems, 2002. 4th IEEE International Workshop on*, IEEE, pp. 73–80.

Felser, M. and Sauter, T. (2004). Standardization of industrial ethernet-the next battlefield?, *Factory Communication Systems, 2004. Proceedings. 2004 IEEE International Workshop on*, IEEE, pp. 413–420.

Igure, V. M., Laughter, S. A. and Williams, R. D. (2006). Security issues in scada networks, *Computers & Security* **25**(7): 498–506.

Knapp, E. D. (2014). *Industrial Network Security: Securing critical infrastructure networks for smart grid, SCADA, and other Industrial Control Systems*, Syngress.

Krutz, R. L. (2005). *Securing SCADA systems*, John Wiley & Sons.

Nicholson, A., Webber, S., Dyer, S., Patel, T. and Janicke, H. (2012). Scada security in the light of cyber-warfare, *Computers & Security* **31**(4): 418–436.

Slay, J. and Miller, M. (2007). Lessons learned from the maroochy water breach, *Critical infrastructure protection* pp. 73–82.

Tanenbaum, A. S. et al. (2003). *Computer networks, 4-th edition*, ed: Prentice Hall.

Thomesse, J. P. (1998). A review of the fieldbuses, *Annual reviews in Control* **22**: 35–45.

Winkel, L. (2006). Real-time ethernet in iec 61784-2 and iec 61158 series, *Industrial Informatics, 2006 IEEE International Conference on*, IEEE, pp. 246–250.