A IMPORTÂNCIA DA SEGURANÇA CIBERNÉTICA EM SISTEMAS DE CONTROLE INDUSTRIAL

Davi Marques Lima
Bacharel em Sistemas de Informação pela PUC-RJ e especialista em Gestão Empresarial pela FGV-RJ.
Auditor Interno de Sistemas - Petrobras
Avenida Chile 65, 16º Andar, Sala 1604 - Rio de Janeiro, RJ - Telefone +55 21 32241748
Email: davimlima@gmail.com

Álvaro Vieira Lima
Doutor em Administração. COPPEAD – UFRJ.
Professor Associado da Faculdade de Administração e Finanças – UERJ.
Email: alvarolima@uerj.br

RESUMO

O propósito deste estudo é entender o conceito de Segurança Cibernética aplicado a Sistemas de Controle Industrial, utilizando uma abordagem fenomenológica de pesquisa. Parte-se da elaboração e entendimento dos conceitos de segurança cibernética apresentados em diversos artigos e livros. Em seguida são analisados dois relatórios de organismos especializados no assunto, além de quatro incidentes em empresas de diferentes ramos industriais. A análise desenvolvida conclui pelo expressivo aumento do número de casos de ataques cibernéticos, inclusive quanto à profundidade e gravidade dos ataques, concluindo pela necessidade de maior atenção, mais recursos e investimentos a serem aplicados à área de segurança cibernética, tendo em vista a preservação dos ativos das organizações.

Palavras-chave: Segurança Cibernética, Sistemas de Controle Industrial, Ataques Cibernéticos.

A IMPORTÂNCIA DA SEGURANÇA CIBERNÉTICA EM SISTEMAS DE CONTROLE INDUSTRIAL

RESUMO

O propósito deste estudo é entender o conceito de Segurança Cibernética aplicado a Sistemas de Controle Industrial, utilizando uma abordagem fenomenológica de pesquisa. Parte-se da elaboração e entendimento dos conceitos de segurança cibernética apresentados em diversos artigos e livros. Em seguida são analisados dois relatórios de organismos especializados no assunto, além de quatro incidentes em empresas de diferentes ramos industriais. A análise desenvolvida conclui pelo expressivo aumento do número de casos de ataques cibernéticos, inclusive quanto à profundidade e gravidade dos ataques, concluindo pela necessidade de maior atenção, mais recursos e investimentos a serem aplicados à área de segurança cibernética, tendo em vista a preservação dos ativos das organizações.

Palavras-chave: Segurança Cibernética, Sistemas de Controle Industrial, Ataques Cibernéticos.

1. INTRODUÇÃO

No atual estágio de desenvolvimento industrial, a diferenciação e a possibilidade de um desempenho de destaque, seja qual for o ramo de negócios da empresa, se dão através da utilização de recursos que otimizem a execução das atividades, ao tempo em que reduzem seu custo.

É nesse contexto que as empresas trazem a tecnologia da informação para mais próximo da automação industrial, fazendo com que as duas áreas se integrem. Desta forma, sistemas de controle industrial, antes isolados e de propriedade exclusiva, passam a compartilhar espaço virtual, equipamentos, tecnologias e ferramentas com outros tipos de sistemas e aplicações mais conhecidos e amplamente utilizados.

Através de dispositivos e soluções oriundas da tecnologia da informação, as indústrias podem desfrutar de novas funcionalidades, tais como: o uso de protocolos de comunicações de redes mais baratos; a possibilidade de operações remotas; a análise de dados de produção em tempo real, dentre outras.

Porém, juntamente com as novas funcionalidades, vêm os riscos cibernéticos associados a elas. Apesar de já existirem amplas discussões e diversas soluções de segurança para os sistemas de tecnologia da informação típicos, o mesmo não ocorre no ambiente de sistemas de controle industrial devido às especificidades tecnológicas e operacionais.

Este trabalho pretende mostrar, de maneira clara e objetiva, a importância da segurança cibernética em sistemas de controle industrial. Para tal, serão analisados dois relatórios de organismos especializados no assunto, além de quatro incidentes em empresas de diferentes ramos. Espera-se que as questões que se colocam em face da necessidade da proteção de

ativos industriais contra os riscos cibernéticos a eles relacionados fiquem amplamente demonstradas.

2. REVISÃO DA LITERATURA

2.1 Sistemas de Controle Industrial

2.1.1 Definição

Segundo Hubka e Eder, "sistema é um conjunto finito de elementos reunidos para formar um todo sob certas regras bem definidas, por meio das quais existem determinadas relações precisas definidas entre os elementos e para com seu ambiente. É possível que um sistema possa conter elementos isolados (i. e. elementos com nenhuma relação com outros), ou grupos isolados de elementos (i. e. o grupo não tem relações com outros elementos ou grupos dentro do conjunto). Os termos elemento e sistema são relativos. Um elemento também pode ser considerado como um sistema, e um sistema pode ser considerado como um elemento dentro de um sistema maior. Assim sendo, os sistemas são hierárquicos".

No contexto tecnológico industrial, Groover (2011) define um Sistema de Controle Industrial (SCI) como um componente básico de um sistema automatizado em que o controle industrial "é a regulação automática das operações da unidade e de seus equipamentos associados, bem como a integração e a coordenação dessas operações no sistema de produção maior".

Na visão de Mattioli e Moulinos (2015), membros da *European Union Agency for Network and Information Security* (ENISA), sistemas de controle industrial são "utilizados para controlar processos industriais e possuem um papel crítico não apenas na manutenção da continuidade desses processos, mas também na garantia de sua segurança, prevenindo grandes acidentes e desastres naturais".

Com o intuito de prover um guia para a segurança em sistemas de controle industrial, em 2006, Stouffer et al (2015), membros do *National Institute of Standards and Technology* (NIST), lançaram a primeira versão da publicação especial 800-82, intitulada como o Guia para a Segurança de Sistemas de Controle Industrial, na qual definiam SCI como "um termo genérico que inclui diversos tipos de sistemas de controle, incluindo sistemas supervisórios e de aquisição de dados (SCADA), sistemas de controle distribuído (SCD), e outras configurações de sistemas como os controladores lógicos programáveis (CLP), comumente encontrado nos setores industriais e de infraestruturas críticas".

2.1.2 Arquitetura e componentes

Um Sistema de Controle Industrial típico contém uma diversidade de loops de controle, interfaces humano-máquina (IHM) ferramentas remotas de manutenção e diagnóstico implementadas utilizando um conjunto de protocolos de redes (Stouffer et al: 2015). Tais componentes podem ser analisados mais detalhadamente abaixo:

• *loop de controle* é uma combinação de dispositivos e funções de controle projetadas de tal forma que uma variável de controle é comparada com um valor definido e retorna para o processo uma nova variável manipulada. Geralmente, consiste em uma rede que integra sensores para mensuração, atuadores como válvulas de controle e hardware de controle como controladores lógicos programáveis (CLP). Variáveis controladas são transmitidas pelos sensores para o controlador. O controlador interpreta os sinais e gera as variáveis correspondentes, baseado em valores definidos, que são transmitidas para os atuadores.

Mudanças no processo resultam em novos sinais, identificando o novo estado do processo, para novamente ser transmitido ao controlador (Stouffer et al: 2015).
• *interface humano-máquina* é o hardware ou software através do qual o operador interage com o controlador. Uma IHM pode variar de um painel de controle físico com botões e indicadores de luz até um computador pessoal com uma tela gráfica colorida rodando um software de IHM dedicado (Falco et al: 2003). Operadores e engenheiros utilizam máquinas IHM para monitorar e configurar variáveis, algoritmos de controle e ajustar e estabelecer parâmetros no controlador. As máquinas IHM também exibem informações sobre o histórico e status do processo (Stouffer et al: 2015).
• *ferramentas remotas de manutenção e diagnóstico* são utilitários usados para prevenir, identificar e recuperar o processo de operações anormais ou falhas.

2.1.3 Tipos de Sistemas de Controle Industrial

2.1.3.1 Sistemas de Controle Distribuídos (SCD)

Sistemas de Controle Distribuídos controlam processos industriais dentro da mesma localização geográfica e são integrados como uma arquitetura contendo um nível supervisório de controle monitorando múltiplos subsistemas integrados que são responsáveis por controlar os detalhes de cada processo localizado. SCDs são extensivamente usados em indústrias baseadas em processos e, nos sistemas mais modernos, os SCDs possuem interfaces com a rede corporativa com a finalidade de oferecer às operações de negócio uma visão da produção (Stouffer et al: 2015).

2.1.3.2 Sistema de Supervisão, Controle e Aquisição de Dados (do inglês SCADA)

Sistemas SCADA são altamente distribuídos e utilizados para controlar ativos geograficamente dispersos em que a centralização do controle e da aquisição de dados é crítica para a operação do sistema. Tais sistemas integram sistemas de aquisição de dados com sistemas de transmissão de dados e softwares de IHM com a finalidade de prover um sistema de controle e monitoramento centralizado para inúmeras entradas e saídas de processos. Os sistemas SCADA são projetados para coletar informações do campo e transferi-las para uma instalação central para que um operador possa monitorar ou controlar de forma centralizada um sistema inteiro em tempo real (Stouffer et al: 2015).

2.1.3.3 Controladores Lógicos Programáveis (CLP)

CLPs são utilizados em ambos os sistemas SCD e SCADA como os componentes de controle de um sistema de controle hierárquico maior com a finalidade de prover a gestão local de processos. Eles são também implementados como os componentes primários em configurações de sistemas de controle menores. CLPs possuem uma memória programável para armazenar instruções com o intuito de implementar funções específicas como controle de entrada e saída de dados, execução de lógica, contagem, comunicação e processamento de arquivos e dados. (Stouffer et al: 2015).

2.2 Segurança Cibernética

2.2.1 Definição

A União Internacional de Telecomunicações (do inglês, ITU) define segurança cibernética como (2008):

A coleção de ferramentas, políticas, conceitos de segurança, proteções de segurança, guias, metodologias de gestão de riscos, ações, treinamentos, melhores práticas e tecnologias que podem ser utilizadas para proteger o ambiente cibernético e os ativos da organização e de seus usuários. Tais ativos incluem dispositivos computacionais, pessoas, infraestrutura, aplicações, serviços, sistemas de telecomunicações e a totalidade da informação transmitida e armazenada no ambiente cibernético. A segurança cibernética luta para garantir a manutenção das propriedades de segurança dos ativos da organização e de seus usuários contra riscos de segurança elevados no ambiente cibernético. Os objetivos gerais de segurança são os seguintes: disponibilidade, integridade e confidencialidade. (ITU, 2008)

Para a Associação de Controle e Auditoria de Sistemas de Informação (ISACA, 2013), "o termo cibernético no contexto da segurança da informação necessita de uma explicação, pois é comumente confundido e utilizado de forma muito abrangente". A instituição define que:

Segurança cibernética engloba tudo que protege organizações e indivíduos de ataques intencionais, falhas e incidentes assim como suas consequências. Na prática, segurança cibernética refere-se primariamente a tipos de ataque, falhas e incidentes que são visados, sofisticados e difíceis de detectar ou gerenciar. A maior parte dos ataques oportunistas e crimes geralmente podem ser evitados utilizando ferramentas e estratégias simples, mas eficazes. Como resultado, o foco da segurança cibernética está no que ficou conhecido como ameaças persistentes avançadas (do inglês, Advanced Persistent Threats – APT), guerra cibernética e seus impactos em organizações e indivíduos. Independentemente do uso comum do termo, segurança cibernética deve estar alinhada com todos os outros aspectos da segurança da informação dentro de uma organização. (ISACA, 2013)

Segundo Wamala (2011), também é importante contrastar os termos segurança da informação e segurança cibernética, uma vez que os entendimentos dos mesmos podem levar a um falso sentimento de segurança ou a uma confusão no que tange os riscos cibernéticos. Para ele, "os dois conceitos visam a atender e manter as propriedades de segurança de confidencialidade[1], integridade[2] e disponibilidade[3]. Porém, o alcance global da Internet dá à segurança cibernética um caráter especial. Enquanto o conceito de segurança da informação iniciou-se quando a maioria dos sistemas atuava de maneira isolada e raramente em jurisdições transversas, a segurança cibernética trabalha com ameaças globais sob incerteza legal". E, citando Sinks (2012), adiciona: "a segurança cibernética tem de rivalizar com uma arquitetura de Internet que torna virtualmente impossível de atribuir um ataque a um ator. "

Finalmente, Wamala (2011) expõe que, devido à sua origem militar e diplomática, a segurança da informação tipicamente foca na confidencialidade enquanto que a segurança cibernética tem um foco maior em integridade e disponibilidade e conclui: "a segurança

[1] Confidencialidade foca na garantia de que o acesso à informação é restrito somente a partes autorizadas.

[2] O princípio da integridade lida com a prevenção da modificação não autorizada da informação. Integridade também cobre os conceitos de acuidade, completeza e confiança da informação.

[3] Disponibilidade tem a finalidade de assegurar que ativos serão passíveis de acesso por usuários atualizados de uma maneira tempestiva quando for necessário.

cibernética é a segurança da informação com incertezas jurisdicionais e questões de atribuição".
Numa visão similar, Somls e Niekerk (2013) propõem que as fronteiras da segurança cibernética como um conceito são mais amplas que aquelas da segurança da informação no que tange a sua definição formal. Segundo eles, "segurança da informação é a proteção da informação, que é um ativo, contra possíveis danos resultantes de diversas ameaças e vulnerabilidades. Segurança cibernética, por outro lado, não é necessariamente apenas a proteção do ciberespaço por si só, mas também a proteção daqueles que trabalham no ciberespaço e qualquer um de seus ativos que podem ser alcançados através do ciberespaço".
Para Brookson et al (2015), "segurança cibernética deve referir-se à segurança do ciberespaço, em que ciberespaço se refere ao conjunto de conexões e relacionamentos entre objetos que são passíveis de acesso através de uma rede de telecomunicações generalizada; e, ao conjunto de objetos por si só onde os mesmos apresentem interfaces permitindo seu controle remoto, acesso remoto à dados ou suas participações em ações de controle dentro deste ciberespaço".

2.2.2 Segurança Cibernética em Sistemas de Controle Industrial

Especialistas em segurança ao redor do mundo continuam a soar os alarmes sobre a segurança em SCI que se parecem cada vez mais com computadores pessoais, pois são utilizados em qualquer lugar e envolvem uma quantidade considerável de software, muitas vezes desatualizados. No contexto industrial, incidentes de segurança recentes enfatizam a importância da boa governança e controle da infraestrutura de SCI. Em particular, na habilidade de responder a incidentes críticos e em analisar e aprender com o ocorrido (Pauna et al 2013).
De acordo com Stouffer et al (2015):
Inicialmente, SCI tinham pouca semelhança com sistemas de tecnologia da informação (TI) tradicionais visto que os SCI eram sistemas isolados executando protocolos de controle proprietários utilizando hardware e software especializados. Largamente disponíveis, dispositivos de Protocolo de Internet (do inglês, Internet Protocolo – IP) de baixo custo estão agora substituindo soluções proprietárias, o que aumenta a possibilidade de vulnerabilidades e incidentes de segurança cibernética. Na medida que SCI estão adotando soluções de TI com a finalidade de promover sistemas de negócios corporativos e funcionalidades de acesso remoto [...] eles começam a parecer com sistemas de TI. Tal integração suporta novas funcionalidades de TI, mas traz significantemente menos isolamento para os SCI [...] criando uma necessidade maior de proteger esses sistemas. Enquanto que soluções de segurança foram projetadas para lidar com as questões de segurança em sistemas de TI típicos, precauções especiais devem ser consideradas quando essas mesmas soluções são levadas para os ambientes de SCI.

Desta forma, os desafios são abundantes independentemente do setor industrial. Diferentemente da defesa tradicional de TI, as defesas relacionadas aos SCI requerem que seus profissionais de segurança enfrentem a tarefa esmagadora de defender uma infraestrutura crítica que está aparelhada de tecnologia ultrapassada (ISACA, 2015).
Byres et al (2007) destacam que, de 1982 até 2000, 74% dos problemas em sistemas SCADA provinham de acidentes, atividades inapropriadas de empregados e colaboradores insatisfeitos, indicando que a maioria das ameaças, maliciosas ou não, vinha de dentro da

organização. Por outro lado, de 2002 até 2006, 60% de todos os eventos ocorridos foram gerados por incidentes externos, indicando uma mudança surpreendente e significativa na fonte de ameaças.
Segundo Nicholson et al (2013), tal comportamento é compreensível, visto que o uso de métodos de comunicações padrões como os TCP/IP[4] se tornaram mais aceitos e divulgados nesse período. É improvável que o número de ataques internos tivesse diminuído; simplesmente, o número de ataques externos aumentou drasticamente ao ponto de quase reverter esses números.

3 METODOLOGIA

3.1 Classificação da Pesquisa

A presente pesquisa classifica-se, quanto aos fins, como sendo qualitativa, descritiva e aplicada, e quanto aos meios, como documental, bibliográfica e estudo de caso.
Com esta pesquisa, buscou-se analisar e ressaltar a importância da segurança cibernética em sistemas de controle industrial através da coleta e análise de dados relevantes tais como relatórios de organismos especializados no assunto e os casos adiante exemplificados.

3.2 Premissa

A premissa básica formulada a ser avaliada no presente trabalho é:

- A segurança cibernética em sistemas de controle industrial é crucial para a manutenção dos processos de produção.

3.3 Coleta e Análise de Dados

Os dados coletados foram do tipo secundário e obtidos por meio de levantamento bibliográfico, sites da Web e de outros trabalhos acadêmicos correlatos, bem como de relatórios e incidentes relacionados à segurança cibernética industrial disponíveis na Internet.
Os relatórios analisados foram:

- 1º Relatório Anual TI Safe sobre incidentes de segurança em redes de automação brasileiras elaborado pela empresa TI Safe Segurança da Informação em maio de 2014. Disponível em *http://docslide.com.br/technology/1o-relatorio-anual-ti-safe-sobre-incidentes-de-seguranca-em-redes-de-automacao-brasileiras.html; e,*
- *2015 Year in Review* publicado em abril de 2016 pelas instituições norte americanas *National Cybersecurity and Communications Integration Center* (NCCIC) e *Industrial Control Systems Cyber Emergency Response Team* (ICS-CERT). Disponível em *https://ics-cert.us-cert.gov/Year-Review-2015.*

Os incidentes de segurança cibernética industrial expostos foram:

- Ukrainian Kyivoblenergo, empresa de distribuição elétrica Ucraniana, dezembro de 2015;

[4] É um modelo de redes de computadores e conjunto de protocolos de comunicação utilizados na Internet e em redes de computadores semelhantes.

- Siderúrgica alemã de nome não divulgado, dezembro de 2014;
- Saudi Aramco, do setor petrolífero saudita, agosto de 2012; e,
- Usina Nuclear de Natanz, Irã, segundo semestre de 2009.

4 ANÁLISE DOS RESULTADOS E DISCUSSÃO

4.1 1º Relatório Anual TI Safe sobre incidentes de segurança em redes de automação brasileiras

4.1.1 Entidade envolvida

A TI Safe Segurança da Informação é uma empresa brasileira fundada em 2007 especializada em produtos e serviços de segurança da informação e redes industriais. De acordo com seu website institucional[5], foi a primeira empresa brasileira a fornecer soluções para a segurança de redes industriais baseadas nas normas ANSI/ISA-99 e NIST SP 800-82. Atualmente, é integrante do comitê internacional da norma ANSI/ISA-99.

4.1.2 Resultados encontrados

O trabalho cataloga incidentes de segurança em redes de automação de empresas brasileiras como uma iniciativa da TI Safe em compreender a situação das ameaças cibernéticas contra plantas industriais. Apesar de utilizar o termo mais abrangente "rede de automação", o relatório trata de incidentes de segurança em sistemas de controle industrial do tipo SCADA, descrito anteriormente.
Todos os dados analisados foram obtidos no período de setembro de 2008 a abril de 2014 a partir de projetos executados pela empresa em seus clientes no Brasil. É necessário colocar que os dados analisados não correspondem à totalidade dos incidentes de segurança de automação em plantas industriais brasileiras. Eles representam única e exclusivamente uma fotografia dos incidentes ocorridos em clientes da TI Safe Segurança da Informação no Brasil. Segundo a empresa, a falta de fontes oficiais de informações sobre incidentes de segurança em redes e sistemas de controle industriais no Brasil gera uma lacuna importante no ciclo de proteção de infraestruturas críticas. Sem dados estatísticos sobre incidentes, investimentos necessários na segurança dessas infraestruturas não são realizados, deixando-as vulneráveis. Os dados quantitativos referentes aos incidentes reportados no período da coleta são exibidos no quadro I.

[5] Website institucional: *http://www.tisafe.com/*

Quadro 1 - Quantitativo de Incidentes de segurança em redes de automação Brasileiras

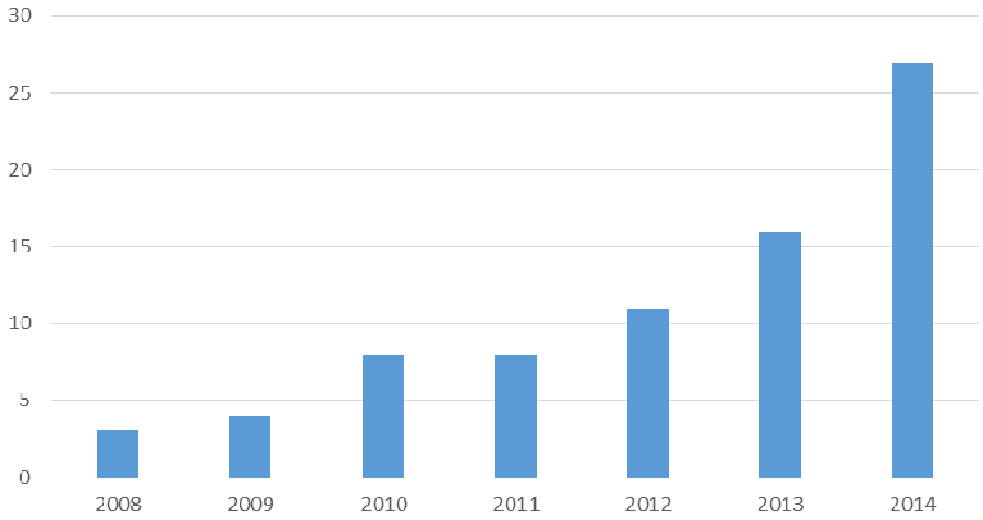
Tipo de Ameaça	**2008**	**2009**	**2010**	**2011**	**2012**	**2013**	**2014**	**Total**	**Porcentagem**
Malware[6]	1	1	2	2	3	7	11	27	35,06%
Erro Humano	2	2	3	4	3	3	7	24	31,17%
Falhas em dispositivos	0	0	1	2	4	4	4	15	19,48%
Sabotagem	0	0	1	0	0	0	1	2	2,60%
Não identificados	0	1	1	0	1	2	4	9	11,69%
Total	**3**	**4**	**8**	**8**	**11**	**16**	**27**	**77**	**100,00%**

Fonte: Adaptado de TI Safe, 1º Relatório Anual TI Safe sobre incidentes de segurança em redes de automação brasileiras

Na análise da empresa, o *worm*[7] "*Conficker Win 32*" dominou a contagem de *malware* no relatório, respondendo por 14 das 27 infecções computadas. Esta alta incidência mostra que a maioria das redes de automação no país não possui recursos mínimos de segurança contra *malware*, contendo máquinas sem antivírus e com *patches*[8] na maioria das vezes desatualizados, quando existem. Este frágil cenário se deve basicamente a dois fatores: a demora dos fabricantes em liberar e testar patches após eles terem sido liberados e a falta de políticas e boas práticas de segurança da informação em redes de automação.
Como mostra o gráfico 1, percebe-se que, os grupos hackers, que antes apenas interessavam-se em atacar bancos e instituições financeiras, estão gradativamente descobrindo novos alvos em infraestruturas críticas, o que tem aumentado ano a ano a quantidade de incidentes de segurança nesses ativos.

[6] Malware, comumente conhecido e generalizado como vírus, agrupa todo software ou programa criado com a intenção de abrigar funções para penetrar em sistemas, quebrar regras de segurança, roubar informações e servir de base para demais operações ilegais e/ou prejudiciais.
[7] Um worm pode ser projetado para tomar ações maliciosas após infectar um sistema, além de se replicar automaticamente, pode deletar arquivos em um sistema ou ser usado para instalação e propagação de outros softwares maliciosos.
[8] Patch é um software ou parte de um software projetado para atualizar um programa de computador ou seus dados de suporte a fim de consertá-lo ou melhora-lo.

Gráfico 1 - Evolução dos incidentes de segurança atendidos pela TI Safe



Fonte: Adaptado de TI Safe, 1º Relatório Anual TI Safe sobre incidentes de segurança em redes de automação brasileiras

Ao concluir o relatório, a empresa expõe sua preocupação pelo fato do Brasil ter ganhado destaque nos últimos anos e, por consequência, atrair mais ataques cibernéticos de todas as ordens, incluindo ataques às suas infraestruturas críticas. Ano a ano a quantidade de ataques tem crescido de forma considerável. Somente nos 4 primeiros meses de 2014 já tinham sido computados mais incidentes de segurança em redes de automação do que em todo o ano de 2013. Além disso, o país já conta com 2 casos comprovados de sabotagem cibernética que ocasionaram graves incidentes de segurança em plantas industriais.
Se por um lado ocorre o crescimento dos incidentes de segurança em redes de automação no país, por outro lado os investimentos em segurança de automação ficam abaixo do necessário.

4.2 *2015 Year in Review*

4.2.1 Entidades envolvidas

O *National Cybersecurity and Communications Integration Center* (NCCIC) é uma divisão do *National Protection and Programs Directorate* (NPPD) dos Estados Unidos da América responsável por prover monitoramento, compartilhamento de informação, análise e resposta a incidentes em tempo integral para proteger as redes e infraestruturas críticas e recursos chaves, tais como sistemas de controle industrial, de agências Federais americanas.
O Industrial *Control Systems-Cyber Emergency Response Team* (ICS-CERT) foi criado pelo *Department of Homeland Security* (DHS) dos Estados Unidos da América para reduzir os riscos de segurança cibernética dentro dos setores de infraestrutura crítica do país. Sua função é prover análises e respostas a incidentes cibernéticos; abordar a segurança, ameaças e conscientização referentes a sistemas de controle; e, prover um meio de compartilhar informação entre as entidades com infraestrutura crítica e recursos chaves do país.

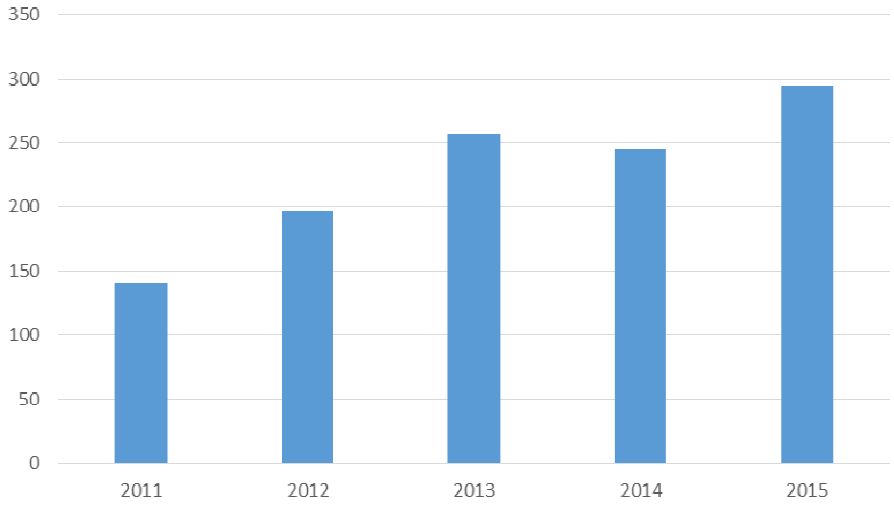
4.2.2 Resultados encontrados

O *Year In Review* é um relatório anual sobre segurança cibernética em setores de infraestrutura crítica[9] em que são detalhadas todas as atividades realizadas pelas entidades no ano anterior à sua publicação. Nele são abordados os temas como: operações de vigilância, resposta a incidentes, coordenação de vulnerabilidades, análise técnica, avaliações de segurança cibernética, distribuição de ferramentas, treinamento e manutenção de grupos de trabalho.

Apesar do relatório abordar setores não industriais, o mesmo torna-se relevante para a pesquisa visto que se constata que a maioria dos incidentes atendidos provieram de plantas industrias onde atuam sistemas de controle industrial.

Assim como no cenário brasileiro, as instituições americanas atenderam a mais incidentes com o passar dos anos. Conforme mostra o gráfico 2, em 2015 houve um aumento de 20% em relação ao ano de 2014 e 210% em relação a 2011.

Gráfico 2 - Evolução dos incidentes de segurança atendidos pela ICS-CERT



Fonte: Autoria própria

Em 2015, o ICS-CERT respondeu a 295 incidentes cibernéticos. O setor de manufaturas críticas praticamente dobrou para um registro de 97 incidentes, tornando-se o setor líder, seguido pelos setores de energia com 46 e sistemas de água com 25. O quadro 2 exibe de maneira mais clara as informações acima.

Quadro 2 - Quantidade de incidentes por setor

Setor	**Incidentes**	**Porcentagem**
Manufaturas Críticas	97	33%

[9] As instituições consideram como setores de infraestrutura crítica: Manufaturas Críticas; Energia; Sistemas de Água e Esgoto; Sistemas de Transporte; Instalações Governamentais; Saúde Pública; Comunicações; Reatores e Materiais nucleares; Tecnologia da Informação; Represas; Indústria Química; Instalações Comerciais; Alimentação e Agricultura; Instituições Financeiras; e, Bases de Defesa Industrial.

Energia	46	16%
Não informado	27	9%
Sistemas de Água e Esgoto	25	8%
Sistemas de Transporte	23	8%
Instalações Governamentais	18	6%
Saúde Pública	14	5%
Comunicações	13	4%
Reatores e Materiais nucleares	7	2%
Tecnologia da Informação	6	2%
Represas	6	2%
Indústria Química	4	1%
Instalações Comerciais	3	1%
Alimentação e Agricultura	2	1%
Instituições Financeiras	2	1%
Bases de Defesa Industrial	2	1%
Total	**295**	**100%**

Fonte: Adaptado de 2015 Year Review, ICS-CERT

Conforme mostra o quadro 3, somente os ataques do tipo *spear phishing*[10] representaram 37% desses incidentes enquanto que varreduras de rede[11], em segundo lugar, ficou com 11%. Outros tipos de ataques como força bruta[12], SQL *Injection*[13], dentre outros, tiveram pouca expressão e 110 incidentes não puderam ser identificados.

Quadro 3 - Quantidade de incidentes por tipo de ataque

Tipo de Ataque	**Quantidade**	**Porcentagem**
Desconhecido	110	37%
Spear Phishing	109	37%
Varredura de Redes	26	9%
Autenticação Fraca	18	6%
Outros	17	6%
Abuso de Acesso	7	2%
Força Bruta	4	1%

[10] Spear phishing é uma tentativa de ataque por meio de e-mail direcionado com o objetivo de obter acesso não autorizado a dados sigilosos. Esses ataques se diferenciam de outro mais conhecido como phishing, visto que é focado em um grupo ou organização específica.

[11] Varreduras de rede: trata-se do uso de redes de computadores para agregar informações referentes a sistemas de informação. Tal prática é principalmente utilizada para avaliações de segurança, manutenção de sistemas e também para realizar ataques cibernéticos.

[12] Ataques do tipo força bruta são métodos de tentativa e erro usados por programas aplicativos para quebrar senhas através de esforço exaustivo, daí o nome força bruta.

[13] SQL Injection - Trata-se de uma técnica de inserção de código utilizado para invadir aplicações orientadas a dados, em que códigos maliciosos do tipo SQL são inseridos num campo de formulário para serem executados.

SQL Injection	4	1%
Total	**295**	**100%**

Fonte: Adaptado de 2015 Year Review, ICS-CERT

O relatório também pôde identificar a profundidade dos ataques dentro das redes corporativas das empresas. Para tal, as instituições dividiram as redes em 6 níveis de camadas em que quanto menor o número mais superficial era a camada. O quadro 4 mostra os níveis estipulados e suas quantidades de incidentes.

Quadro 4 - Quantidade de incidentes por profundidade de ataque

Nível	**Incidentes**
1 – Zona Desmilitarizada[14] de Negócio	230
2 – Rede Corporativa	39
3 – Gestão da Rede Corporativa	3
4 – Zona Desmilitarizada com Sistemas Críticos	0
5 – Gestão de Sistemas Críticos	1
6 – Sistemas Críticos	22
Total	**295**

Fonte: Adaptado de 2015 Year Review, ICS-CERT

As instituições terminam seu relatório com a previsão de expandir suas atividades e de contratar mais funcionários para atender à demanda crescente referente à segurança cibernética em plantas industriais. Outros objetivos são a maior oferta de treinamentos e expansão da utilização de ferramentas e equipes técnicas localmente nas organizações assessoradas.

4.3 Ukrainian Kyivoblenergo

Em dezembro de 2015, a Ukrainian Kyivoblenergo, uma empresa regional da Ucrânia de distribuição elétrica, sofreu um ataque cibernético que, segundo o governo Ucraniano, foi originado pelo Serviço Secreto Russo. O ataque acabou atingindo mais outras duas companhias elétricas deixando 225.000 usuários sem energia em diversas áreas do país durante algumas horas (Lee et al: 2016).
Segundo Lee et al (2016), os atacantes utilizaram-se de diversas técnicas, incluindo *spear phishing,* variações do *malware BlackEnergy 3* e a manipulação de documentos infectados do *Microsoft Office*, para ganhar acesso às redes de tecnologia da informação das companhias elétricas. Além de conhecerem a infraestrutura conectada à rede, eles demonstraram habilidades na operação dos sistemas de controle industrial, tais como os equipamentos de interface homem-máquina. Finalmente, os atacantes demonstraram aptidão e determinação em

[14] Uma zona desmilitarizada é uma subrede física ou lógica que contém e oferece serviços de uma organização para uma rede maior e insegura, geralmente a internet.

selecionar dispositivos em subestações, como conversores, como alvos e deixá-los inoperantes e até mesmo irrecuperáveis.
Entretanto, o mais surpreendente nos atacantes foi sua capacidade em realizar operações de reconhecimento de longo prazo, necessárias para conhecer o ambiente das empresas e executar um ataque tão sincronizado, multifaseado e em diferentes localidades (Lee et al: 2016).

4.4 Siderúrgica alemã

Em dezembro de 2014, o Escritório Federal de Segurança da Informação Alemão divulgou em seu relatório anual o caso de uma invasão maliciosa numa instalação siderúrgica não revelada. O incidente impactou componentes críticos de processo resultando em danos físicos massivos (Lee et al: 2014).
O relatório indica que o passo inicial para a invasão da rede corporativa foi um ataque de *spear phishing* e que, desse acesso, os atacantes navegaram até as redes dos sistemas de controle industrial. Segundo relatado, houve um acúmulo de panes em componentes individuais do sistema de controle ou da planta como um todo, impedindo que um forno industrial fechasse devidamente, o que resultou em condições inesperadas e danos físicos ao sistema (Lee et al: 2014).
Através do estudo de outros incidentes de *spear phishing* em SCI, é bastante provável que o e-mail enviado contivesse algum documento, como um PDF, que ao ser aberto executaria um código malicioso no computador. Por sua vez, esse código malicioso deve ter aberto uma conexão entre os atacantes e as instalações (Lee et al: 2014).

4.5 Saudi Aramco

Em agosto de 2012, a empresa nacional de petróleo e gás da Arábia Saudita, Saudi Arabian Oil Company, ou Saudi Aramco, sofreu um ataque cibernético através de um vírus de computador apelidado de Shamoon que infectou até 30.000 computadores de plataforma Windows operando dentro da rede corporativa da empresa (Bronk et al: 2013).
Seu principal objetivo era a deleção indiscriminada de dados nos discos rígidos dos computadores infectados. Apesar de não ter acarretado nenhum derramamento de óleo, explosão ou grande falha nas operações, o ataque impactou nos processos de produção e de negócios, visto que dados de perfuração e produção foram apagados. O vírus também se propagou para as redes corporativas de outras companhias de petróleo e gás, incluindo RasGas e ExxonMobil. Acredita-se que o ataque partiu de alguém que tinha acesso a um computador na própria rede corporativa da Saudi Aramco (Bronk et al: 2013).

4.6 Usina Nuclear de Natanz

Em novembro de 2009, o *Institute for Science and International Security (ISIS)* divulgava seu relatório sobre o enriquecimento de urânio no Irã. Dentre outras informações, o documento citava que o número de centrífugas de enriquecimento em funcionamento na usina nuclear de Natanz havia caído em 15% desde agosto do mesmo ano (Albright, 2009).
Quase um ano depois, em setembro de 2010, a mídia noticiava uma nova forma de ataque cibernético que, a princípio, havia selecionado o Irã como alvo. Segundo as informações, através do uso de discos removíveis em computadores desconectados da *Internet,* um vírus de

computador chamado de Stuxnet havia infectado computadores utilizados para o controle de operações de uma usina nuclear. Uma vez dentro do sistema, o vírus tinha a capacidade de destruir ou degradar o sistema sobre o qual operava (Kerr, 2010).
Pouco antes do noticiário midiático em setembro, ainda em junho de 2010, uma empresa de segurança estabelecida na Bielorrússia fazia o primeiro relatório que citava o vírus Stuxnet. Segundo eles, o *malware* havia sido projetado especialmente para atacar um tipo de SCI particular: um que controlava usinas nucleares, tanto para geração de energia quanto para enriquecimento de urânio. O vírus atacava uma aplicação baseada em Windows que é utilizada por um SCI produzido pela fabricante alemã Siemens (Kerr, 2010).
Paralelamente às atividades midiáticas de setembro de 2010, a empresa de segurança cibernética Symantec divulgava um relatório específico sobre o vírus Stuxnet. Neste documento, a organização citava que no dia 29 de setembro de 2010 o Irã possuía mais de 60.000 equipamentos infectados. Além disso, relatava-se que o *malware* havia se expandido para outros países, chegando a 100.000 máquinas infectadas em todo o mundo. Porém, tudo indicava que as primeiras infecções haviam começado em junho de 2009 no Irã (Falliere et al: 2010).
O ataque do vírus Stuxnet contra a usina nuclear iraniana de Natanz demonstra o impacto que um adversário sofisticado com conhecimentos específicos sobre sistemas de controle pode causar a infraestruturas críticas. Acredita-se que o *malware* foi responsável pela destruição de cerca de 984 centrífugas de enriquecimento de urânio (Kesler, 2011).

5 CONCLUSÃO

Traçando um paralelo entre os dois relatórios analisados, pôde-se perceber o aumento dos incidentes de segurança em sistemas de controle industrial com o passar dos anos tanto no Brasil quanto nos EUA. Tal observação mostra que a ameaça de incidentes cibernéticos não é algo local ou dirigido, mas um movimento global e abrangente em ascensão.
Além disso, os relatórios destacam, no Brasil, a maior proporção de incidentes causados por *malware* e falhas de dispositivos, enquanto que nos EUA destacam a quantidade de incidentes oriundos de *spear phishing* e varreduras de redes. As instituições norte americanas puderam verificar ainda a profundidade dos incidentes, observando que 7% deles chegaram até os sistemas críticos das organizações.
Através de uma análise mais detalhada de casos reais, pôde-se exemplificar os impactos desses tipos de incidentes e constatou-se que ataques cibernéticos bem-sucedidos tem alto poder destrutivo podendo causar grandes danos tangíveis, intangíveis e, em alguns casos, irreversíveis.
Tal cenário perigoso, aliado a alta competividade inerente ao mercado industrial, torna crucial a adoção de medidas de fortalecimento da segurança cibernética em sistemas de controle industrial, evitando, assim, eventos indesejados que possam prejudicar as organizações.

REFERÊNCIAS

ALBRIGHT D.; SHITE, J.; (2009). *IAEA Report on Iran.* Disponível em *http://www.isisnuclearIrã.org/assets/pdf/ISIS_Analysis_IAEA_Report_16Nov2009.pdf*

BRONK, C.; TIKK-RINGAS, E., (2013). *Hack or Attack? Shamoon and the evolution of cyber conflict.* Disponível em *http://bakerinstitute.org/media/files/Research/dd3345ce/ITP-pub-WorkingPaper-ShamoonCyberConflict-020113.pdf*

BROOKSON, C.; et al (2015). *Definition of Cybersecurity.* Disponível em *https://www.enisa.europa.eu/publications/definition-of-cybersecurity*

BYERS, E.; LEVERSAGE, D.; KUBE, N.; (2007). *Security incidents and trends in SCADA and process industries.* Disponível em *http://www.mtl-inst.com/images/uploads/datasheets/IEBook_May_07_SCADA_Security_Trends.pdf*

FALCO J.; STOUFFER, K.; WAVERING, A.; PROCTOR, F., (2003), *IT Security for Industrial Control Systems, NIST IR 6859*. Disponível em *http://www.nist.gov/customcf/get_pdf.cfm?pub_id=821684*

FALLIERE, N.; MURCHU, L.; CHIEN, E.; (2010). *W32.Stuxnet Dossier*. Disponível em *http://www.symantec.com/content/en/us/enterprise/media/security_response/whitepapers/w32_stuxnet_dossier.pdf*

GROOVER, M., (2011). *Automação Industrial e Sistemas de Manufatura.* 3º Edição. Editora Pearson.

HUBKA, V., EDER, W. E, (1988). *Theory of technical systems*. Editora Springer-Verlag;

INFORMATION SYSTEMS AUDIT AND CONTROL ASSOCIATION (ISACA), (2013). *Transforming Cybersecurity*. Rolling Meadows: ISACA.

_____, (2015). *Industrial Control Systems: A Primer for the Rest of Us.* Disponível em *http://www.isaca.org/knowledge-center/research/researchdeliverables/pages/industrial-control-systems-a-primer-for-the-rest-of-us.aspx*

KERR, P.; ROLLINS, J.; THEOHARY, C.; (2010). *The Stuxnet Computer Worm: Harbinger of an Emerging Warfare Capability.* Disponível em *https://www.fas.org/sgp/crs/natsec/R41524.pdf*

KESLER, B.; (2011). *The Vulnerability of Nuclear Facilities to Cyber Attack.* Disponível em *http://large.stanford.edu/courses/2015/ph241/holloway1/docs/SI-v10-I1_Kesler.pdf*

LEE, R.; ASSANTE, M.; CONWAY, T., (2014). *German Steel Mill Cyber Attack.* Disponível em *https://ics.sans.org/media/ICS-CPPE-case-Study-2-German-Steelworks_Facility.pdf*

LEE, R.; ASSANTE, M.; CONWAY, T., (2016). *Analysis of the Cyber Attack on the Ukrainian Power Grid.* Disponível em *https://ics.sans.org/media/E-ISAC_SANS_Ukraine_DUC_5.pdf*

MATTIOLI, R.; MOULINOS, K., (2015). *Analysis of ICS-SCADA Cyber Security Maturity Levels in Critical Sectors*. Disponível em *https://www.enisa.europa.eu/publications/maturity-levels*.

NICHOLSON, A.; WEBBER, S.; DYER, T.; PATEL, T.; JANICKE H., (2012). *SCADA security in the light of Cyber-Warfare.* Computer & Security, Volume 31. Disponível em *http://www.sciencedirect.com/science/article/pii/S0167404812000429*

PAUNA, A.; MOULINOS, K.; LAKKA, M.; MAY, J.; TRYFONAS, T.; (2013). *Can we learn from SCADA security incidents?* Disponível em *https://www.enisa.europa.eu/publications/can-we-learn-from-scada-security-incidents*

SINKS, M., (2012). *Cyber Warfare and International Law.* 1º Edição. Editora Biblioscholar.

SOLMS, R.; NIEKERK, J., (2013). *From information security to cyber security*. Computer & Security, Volume 38. Disponível em *http://www.sciencedirect.com/science/article/pii/S0167404813000801*

STOUFFER, K., FALCO, J., SCARFONE, K., (2015). *Guide to Industrial Control Systems (ICS) Security.* Disponível em *http://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-82r2.pdf*

THE INTERNACIONAL TELECOMMUNICATIONS UNION (ITU), (2008). *Overview of Cybersecurity.* Disponível em https://www.itu.int/rec/T-REC-X.1205-200804-I

WAMALA, F., (2011). *The ITU National Cybersecurity Strategy Guide.* Disponível em http://www.itu.int/ITU-D/cyb/cybersecurity/docs/ITUNationalCybersecurityStrategyGuide.pdf