



Grupo de Estudo de Sistemas de Informação e Telecomunicação para Sistemas Elétricos-GTL

Atualização de software em ambientes industriais, o cenário possível e principais dificuldades

**FABIO DOS SANTOS OLIVEIRA(1); JÉSSICA BARBOSA HELUANY(1);
VH(1);**

RESUMO

A evolução tecnológica tem afetado o setor elétrico. Ingressar na era digital é um diferencial para as empresas, independentemente do porte da organização e existem fatores críticos que asseguram este ingresso com menor exposição a riscos cibernéticos, como por exemplo a estratégia de Segurança da Informação, mais especificamente o processo de atualização de software, que deve atuar como uma das barreiras contra ataques cibernéticos.

As principais ideias aqui apresentadas envolvem melhores práticas, hipóteses para tratamento de problemas, identificar as principais dificuldades, requisitos necessários, avaliação da evolução dos requerimentos de Cyber Security em empreendimentos elétricos, além de criar oportunidades para pesquisas futuras.

PALAVRAS-CHAVE

Atualização, Risco, Automação, SCADA, Cyber

1.0 - INTRODUÇÃO

Mudanças que ocorreram em diferentes setores da economia obrigaram as organizações a ingressar na era digital. Este evento se deve por diferentes motivos e cada organização deve identificar quais ações implementar a médio e longo prazo. Muito mais do que um projeto ou uma iniciativa isolada, a digitalização, como toda e qualquer mudança de grande porte deve ser colocada em prática, independente do mercado de atuação ou porte da organização, de maneira a expor a operação a menor quantidade de riscos, inclusive os cibernéticos. Um dos fatores relevantes é a estratégia de Segurança da Informação que suportará o movimento de cada organização nos projetos de digitalização.

Dentro da estratégia de Segurança da Informação, o processo de Atualização de Software tem como uma das suas principais características atuar como uma das barreiras, visando limitar possíveis ataques cibernéticos, desde que seja gerenciado com o direcionamento técnico necessário, baseado nas melhores práticas de mercado e alinhado às necessidades de negócio sejam elas regulatórias, estratégicas, técnicas ou ainda de cultura de cada organização.

Com certa frequência, a imprensa especializada, grandes corporações de mercado de Tecnologia de Informação ou ainda institutos de pesquisa, veiculam informações indicando a quantidade crescente de ataques cibernéticos e os efeitos que tais incidentes causam às empresas ou países, gerando em alguns casos, a criação de uma

relação direta com o incidente ocorrido e o nome da empresa ou país, ou seja, estudos futuros ou análises de diferentes tipos, sempre terão relação com a empresa ou país atacado, algo que ficará marcado e será uma referência negativa ao longo do tempo. Podemos citar casos como Stuxnet, BlackEnergy ou até Wannacry.

É de conhecimento dos especialistas e estudiosos sobre o tema, que parte destes ataques foram perpetrados em organizações que não tinham um processo bem definido e eficaz de atualização dos sistemas operacionais e demais softwares utilizados.

A indústria por sua vez, tem características diferentes do ambiente dito corporativo, onde o processo de atualização está estabelecido e largamente utilizado. Um microcomputador pode, ainda que tal indisponibilidade gere algum inconveniente, passar por um processo de reinicialização ao final do expediente de um escritório, em função da instalação de uma atualização do sistema operacional, algo que não pode ser comparado a uma estação de operação executando um sistema supervisão durante uma manobra crítica em um centro de operações. Os sistemas de Automação são caracterizados por altos custos de licenciamento e hardware de grande durabilidade, esta é uma outra diferença considerável ao avaliar os sistemas corporativos tradicionais. Esta constatação, aliada a alta criticidade e disponibilidade dos sistemas de Automação reforçam a dificuldade para implementar um processo de atualização de software, já que afetariam a utilização de sistemas cujo funcionamento pode ultrapassar semanas sem interrupção.

As melhores práticas no processo de atualização de software descrevem ações específicas que devem ser executadas antes, durante e depois do processo de atualização, visando causar o menor impacto possível ao ambiente tecnológico. Igualmente relevante é identificar as principais dificuldades na adoção destas práticas no ambiente industrial, já que diferentemente do já citado “ambiente dito corporativo”, a disponibilidade é mais importante nos ambientes de Automação.

Os impeditivos para a implementação de uma estratégia de atualização de software em um ambiente de Automação Industrial, terão como base experiências práticas permitindo aos leitores estabelecer um paralelo com as respectivas organizações que estão inseridos e traçar estratégias para a implementação de soluções semelhantes, adequadas às suas realidades e requisitos técnicos.

A expectativa com este material é criar oportunidades para pesquisas futuras a fim de criar uma base de referência em diferentes setores da economia para lidar com este tema em especial o setor elétrico dada a sua relevância para o país.

2.0 - ATUALIZAÇÃO DE SOFTWARE

A fim de delimitar o tema atualização de software, é importante conceituar algumas nomenclaturas bastante difundidas no mercado de Tecnologia da Informação, mas que também são de conhecimento dos profissionais atuantes na área de Automação do setor elétrico. A atualização de software no contexto aqui abordado, consiste na instalação de updates e patches em sistemas operacionais, sistemas, aplicações ou firmware. Ao mencionar o update, que será tratado basicamente como atualização, deve-se considerar que a sua instalação significa modernizar ou levar ao último estágio de uma determinada tecnologia um sistema operacional, um hardware, um sistema, programa ou aplicativo. Por vezes, a versão mais atual não tem as falhas de segurança já identificadas em versões anteriores e portanto corrigidas na atualização. O patch por sua vez, tem relação direta com a correção de uma falha que pode ser de funcionamento, mas que também pode ser de segurança, também conhecida como vulnerabilidade de segurança.

Seja instalando um patch ou um update, deve-se considerar que uma atualização de software está em curso e que é uma das formas de eliminar vulnerabilidades de segurança da informação. Cada fabricante tem uma metodologia específica para disponibilizar estas atualizações, bem como recomendações relacionadas. Cabe ao responsável pelo sistema definir como, quando e qual atualização deve instalar em cada ativo, em função de funcionalidades que utiliza e cenário de sua organização.

A atualização de software é um processo antigo, mas com o aumento das vulnerabilidades de segurança, bem como a pressão por rapidez no lançamentos de novos produtos por parte de seus respectivos fabricantes, tornou-se um fator importante na estratégia de Segurança da Informação e tem demandado grande carga de trabalho nas organizações em função do volume da atualizações disponibilizadas periodicamente. Vale ressaltar que tanto os especialista sérios que identificam vulnerabilidades e comunicam aos fabricantes, como os aproveitadores que se utilizam das vulnerabilidades para implementar ataques cibernéticos, podem ser considerados fatores preponderantes para o aumento das vulnerabilidades e consequentemente a difusão do processo de atualização de software.

Por conta do exposto acima, lançar mão do processo de atualização de software como uma das opções para mitigar a exposição a riscos cibernéticos ou ainda tornar-se uma barreira contra ataques que se aproveitariam de vulnerabilidades disponíveis é um dado importante e reforça a relevância do processo. O que se procura com este informe técnico é esclarecer o processo e como lidar com esta realidade nas operações de alta criticidade do setor elétrico.

Por outro lado, não despreveremos aqui ferramentas disponíveis para a execução do processo de atualização. Com efeito, abordar o processo como um todo, permitirá que uma organização possa implementar a metodologia sem considerar produtos ou fabricantes específicos e terá a liberdade de ajustar sua estrutura ao processo desenhado.

2.1 CENÁRIO NAS ORGANIZAÇÕES

As organizações implementaram o processo de atualização de softwares no ambiente de Tecnologia da Informação corporativo. Esta implementação se deu por conta dos motivos já descritos e apoiada em algum framework de mercado. A definição prévia de um framework ou uma referência, auxilia a organização a estabelecer os critérios de implementação, métricas, políticas e a governança para o processo.

Muitas organizações utilizam a biblioteca ITIL¹, que é o acrônimo de Information Technology Infrastructure Library para gerenciar este processo. Utilizando ITIL, que nada mais é do que uma biblioteca, ou ainda um conjunto de publicações de melhores práticas para o gerenciamento de serviços de Tecnologia da Informação é possível criar uma série de procedimentos que visam trazer qualidade e visibilidade ao processo de atualização de software. São disciplinas descritas na ITIL como por exemplo o Gerenciamento de Mudanças e o Gerenciamento de Liberação e Implantação.

O Gerenciamento de Mudanças auxilia na garantia que métodos consistentes sejam usados para realizar alterações em serviços de Tecnologia da Informação. Esse movimento evita falhas que afetem a disponibilidade do serviço, já que utiliza um processo específico para aprovar (considerando a devida autoridade dos envolvidos) e implementar as mudanças, documentando todo o processo com planos de recuperação em caso de falhas.

Já o Gerenciamento de Liberação e Implantação suporta o processo envolvendo a construção e implantação de liberações, ou seja, controlar um ambiente de testes para homologar as mudanças antes de implementá-las em definitivo no ambiente tratado como produtivo.

O Gerenciamento de Liberação é responsável pelo planejamento, programação e controle das liberações nos ambientes de teste e produção. O processo trabalha em conjunto com os processos de Gerenciamento de Mudanças e Gerenciamento de Configuração e Ativos de Serviço.

Utilizando estes processos as equipes de Tecnologia da Informação criam uma cultura focada em testar as mudanças em ambientes segregados e executam por vezes roteiros de testes visando identificar anomalias após a atualização de um ou mais software. Há forte envolvimento da área usuária que deve se comprometer com o processo e aprovar a implementação no ambiente produtivo.

Considerando os sistemas de Automação executados nas redes de Tecnologia da Automação, que ainda hoje estão em funcionamento utilizando hardware sem garantia dos fabricantes ou que estão em pleno funcionamento a mais de 15 anos por exemplo, além de considerar que os sistemas, firmware e demais softwares também estão em avançado estado de obsolescência, a utilização dos mesmos processos apresentados acima se mostra quase que inviável pela falta de detalhes importantes para compor o processo, bem como a inexistência de tempo hábil para execução de baterias de testes ou dispor de hardware para implementação de ambientes de simulação.

Vale considerar que a grande diferença no que se refere a atualização de software nas redes de TI e TA (Tecnologia da Informação e Tecnologia da Automação respectivamente) é a implementação automatizada e rotineira das atualizações nas redes de TI enquanto que nas redes de TA tal implementação é feita com pouco frequência ou não é executada.

Fazendo um paralelo entre as redes de TI e TA, vale observar a recomendação contida na IEC 62443 relacionada ao gerenciamento de riscos em ativos voltados para Automação Industrial e Sistemas de Controle, pois diferentemente dos ambientes tradicionais de TI que priorizam confidencialidade, integridade e disponibilidade da informação, as redes de TA priorizam disponibilidade, integridade e confidencialidade, desta forma, a maneira de gerenciar a atualização de software deve ser totalmente revista e condicionada a uma

necessidade do setor elétrico no que se refere a causar o menor impacto a continuidade das operações, sob pena de interferir em indicadores e estratégias das organizações.

1 - A ITIL foi desenvolvida pelo governo do Reino Unido na década de 1980, com o objetivo de melhorar o nível de qualidade de serviços de Tecnologia da Informação que na época apresentava uma série de deficiências. O OCG (Office of Government Commerce) desenvolveu uma abordagem eficiente e financeiramente viável para gerenciar os recursos de Tecnologia da Informação que suportava o governo britânico. Por conta do êxito, passou a ser adotada pelo setor privado. Em 2013, a propriedade da ITIL passou a ser da Axelos®, uma joint-venture entre a OGC e a empresa privada CAPITA.

A diferenciação citada é bastante evidente se considerado o ciclo de vida de ativos em funcionamento atualmente, pois foram implementados tomando como base robustez, além das características específicas de cada projeto, mas não foram adquiridos com a premissa de atualização constante ou troca no espaço de tempo definido pelas equipes de TI, basicamente de 3 a 4 anos para substituição do hardware e por vezes dos sistemas operacionais e aplicações.

2.2 ATUALIZAÇÃO DE SOFTWARE COMO UM ITEM DE SEGURANÇA DA INFORMAÇÃO

Por conta dos fatores já descritos, a atualização de software é um componente relevante na estratégia de Segurança da Informação das organizações. Um fator que reforça demasiadamente esta relevância é a possibilidade de implementação de correções emergenciais. Este cenário se dá nos casos em que um ataque cibernético é iniciado ao se beneficiar de uma vulnerabilidade de segurança em um determinado produto em uma determinada empresa. Cabe ressaltar que não será avaliado aqui o método utilizado pelo atacante para ter acesso aos equipamentos, seja remotamente ou utilizando de algum usuário interno, o foco nesta análise é explanar sobre uma vulnerabilidade existente, o início de um ataque, a identificação do ataque e causa raiz do problema. Se a causa resulta de uma atualização que ainda não foi aplicada e existe condição de executar esta instalação (neste caso o sistema de Automação não foi corrompido), há de se colocar em prática um processo de instalação emergencial, visando eliminar o problema com brevidade e retornar à operação normal.

O processo de gerenciamento de mudança deve prever esta situação e uma análise posterior deve ser conduzida a fim de esclarecer possíveis falhas ou inconsistências no processo. Por se tratar de uma mudança emergencial, parte do processo de aprovação, testes e simulações que são partes relevantes no processo normal, são executados posteriormente ou não são executados em função do cenário apresentado. Em última análise, ter um processo geral bem como ferramentas que permitam a organização implementar a atualização necessária sem comprometer o funcionamento do sistema de Automação e na melhor das hipóteses sem interferir na disponibilidade dos serviços, será o melhor cenário do ponto de vista de Segurança da Informação e da estratégia corporativa da empresa afetada.

É importante destacar que criar um processo como este, mesmo com uma documentação e envolvimento das equipes não assegura por si só que as mudanças terão sucesso. Por este motivo, o processo de gerenciamento de mudanças sempre descreve uma estratégia de retorno, também conhecida como estratégia de rollback. Há casos também em que a mudança chegará em uma fase sem retorno, ou seja, somente com a restauração dos programas e projetos os sistemas de Automação voltarão a funcionar como identificado antes de uma mudança que não teve sucesso.

2.2.1. Melhores práticas

O processo de atualização de software pode ser conduzido de diferentes formas, na medida que determinados pontos sejam alinhados entre os envolvidos, ou seja, prover documentação clara e objetiva do processo como um todo. Desenvolver um fluxo de informações, uma matriz de responsabilidades e níveis de aprovação, além de documentar ao máximo as situações previstas de maneira a evitar que a equipe técnica tenha que tomar decisões em momentos críticos é o primeiro passo para atingir um nível de excelência neste tema.

Outro ponto importante é o suporte da alta direção da empresa que deve apoiar as ações neste sentido e assegurar que todos os envolvidos foram treinados, sem descartar revisões periódicas da documentação e dos treinamentos ministrados. Estes fatores visam fortalecer o processo e minimizar a perda de efetividade do tópico que pode ser assumido como um item de controle também.

Ainda no que se refere a governança deste processo, estabelecer relatórios periódicos e indicadores que serão reportados para a alta direção ou os principais envolvidos neste processo também reforça a importância deste item.

Com relação a infraestrutura necessária o estado da arte é a possibilidade de utilizar servidores, estações, sistemas operacionais e demais produtos em um ambiente de testes, completamente separado do ambiente de produção. Este ambiente teria a função principal de ser uma réplica do ambiente produtivo, ou seja, os serviços que são efetivamente utilizados pela equipe técnica de Automação são considerados os sistemas produtivos ou “de produção”, portanto, o ambiente de testes tem exatamente as mesmas versões de software, sistema operacional e configuração de hardware, bem como a última versão de patch, service pack ou similares para a instalação de novas atualizações.

Sistemas de redundância também facilitam a implementação de estratégias de atualização de software. Neste sentido, a ideia central é executar os sistemas de Automação em servidores duplicados, ou seja, ao implementar a atualização em uma máquina, limita-se o acesso às aplicações executadas sem interferência no funcionamento dos serviços. Se não houver problemas, basta implementar a atualização no outro servidor. Este serviço de redundância pode ser conhecido como cluster ou ainda load balance.

Uma observação importante quanto a separação dos ambientes de produção e testes. Tal separação deve considerar uma separação física, de modo que uma alteração no cenário de testes não interfira nos sistemas em uso, inclusive com possibilidade de identificação dos ambientes no caso de impressão de documentos ou relatórios, além da interface de acesso, para que o usuário final tenha completa ciência que está utilizando um ambiente de testes.

Ao implementar estas medidas a organização terá reduzido o risco de implementar alterações no ambiente produtivo e não perceber as mudanças ou ainda identificar falhas de funcionamento no ambiente de produção. Este cenário é o melhor possível e reduz riscos também para os casos de atualização de software com urgência. Não seria a mudança emergencial, mas que clara e rapidamente pode mudar para uma emergência.

O licenciamento dos produtos utilizados (software) no ambiente de testes é parte relevante no processo de atualização de software. É fundamental utilizar software licenciado, bem como ter contratos de suporte. Quanto ao licenciamento, para garantir que a organização está em Compliance. O fundamental neste ponto é o contrato de suporte. Este contrato deve assegurar, de acordo com a criticidade do sistema e também do hardware, uma estratégia de suporte com características como suporte no idioma da equipe de Automação e Operação, tempo máximo de resposta no caso de incidentes, duas opções de contato para abertura de chamados técnicos, eventualmente suporte remoto (neste caso uma solução segura de acesso é fundamental), definir faixas de horário ou contratá-lo na modalidade 24x7. Além do serviço de suporte, será possível trazer algumas garantias para a operação pois este tipo de suporte pode indicar quais atualizações devem ser instaladas além de, por analogia com outros clientes por exemplo, indicar os principais problemas em aplicar ou não uma determinada atualização.

Por fim o contrato de suporte deverá auxiliar as organizações no upgrade dos sistemas, desde que os contratos sejam honrados, ou seja, requer planejamento financeiro para renovações periódicas. Neste caso, o upgrade será a mudança de versão de um determinado software que em geral trará melhores funcionalidades, bem como maior Segurança, já que por vezes se trata de um novo produto.

Ainda no que se refere a recursos, promover a integração entre as equipes de TI e TA para que desenvolvam estas atividades em parceria, trás grande benefício para a organização, já que atuando em conjunto, haverá transferência de conhecimento e principalmente crescimento organizacional e profissional entre os envolvidos. Estas equipes têm níveis de aceitação diferentes quando algumas questões são levantadas. A necessidade de desenvolver ações em conjunto bem como a documentação destes detalhes também deve ser considerada uma boa prática.

Rotinas de Backup também são importantes em cenários deste tipo. A ideia em geral é executar um backup da sua estrutura e projetos em execução, antes de aplicar qualquer atualização. Ao proceder desta forma a organização garante que terá condições de restaurar os sistemas no caso de qualquer intercorrência após a instalação da atualização. Também se recomenda a execução periódica de testes dos backups, que nada mais são do que a restauração dos backups e validação se as principais funcionalidades dos sistemas operam corretamente.

Outra boa prática a ser implementada é a criação de máquinas virtuais para o ambiente de testes e a utilização de licenças de treinamento que em geral tem custo reduzido. Um ambiente virtual deve ocupar espaço físico reduzido, e permitirá algumas adequações aos serviços executados sem prejuízo aos sistemas de Automação que precisam receber atualizações. Esta estratégia tem relação direta com a redução dos custos envolvidos, na medida que diferentes sistemas podem ser virtualizados.

Algumas organizações têm pouca ou quase nenhuma restrição para contratar serviços terceirizados. O processo de atualização de software pode ser completamente terceirizado, sendo muito comum a terceirização

com o fornecedor da solução mais relevante ou crítica, no momento da contratação de novas soluções. Nestes casos, contratos são firmados e o provedor de serviços pode alocar recursos na planta do contratante ou ainda simular as atualizações em um ambiente controlado (fora dos domínios da empresa) e definir uma data, em geral durante paradas para manutenção ou manobras, para implementar estas atualizações.

Ainda na linha da terceirização de serviços, há a possibilidade da contratação de todo o serviço de processamento dos sistemas SCADA. Neste caso a empresa contratante não deverá investir em licenciamento, contratos de suporte ou ainda acompanhar o ciclo de vida do hardware e software utilizado. Nesta modalidade o fornecedor deve arcar com a gestão completa da infraestrutura e atualizações cabendo apenas ao contratante pagar pela infraestrutura utilizada.

2.2.2. Principais dificuldades e impeditivos

No item 2.2.1 apresentamos as boas práticas, mas o cenário encontrado nas organizações não necessariamente será este. Na prática, as organizações possuem recursos escassos com grande tempo de utilização e pouca ou quase nenhuma possibilidade de implementar as atualizações necessárias.

A falta de iniciativa das organizações em minimizar riscos cibernéticos através da atualização de software também pode ser classificada como uma das dificuldades. A escolha das empresas está relacionada ao produto propriamente dito, mas também a falta de ambientes de testes ou ainda definição estratégica, ainda que possa causar impactos ao longo do tempo.

A utilização de programas com alto grau de complexidade e conseqüentemente alto custo de manutenção e suporte também contribui para que as organizações não façam os investimentos e movimentos necessários neste sentido. Cada empresa pode e deve avaliar os riscos envolvidos ao definir uma determinada estratégia e criar ações de contenção.

Outro fator tem relação com a indisponibilidade de atualizações para sistemas obsoletos, não se trata de sistemas sem suporte por parte do fabricante, mas de produtos que chegaram ao final do ciclo de vida. Por conta de questões econômicas e técnicas os fabricantes de software estipulam um limite, ao longo do tempo, para determinados produtos e encerram o fornecimento de atualizações.

A integração inexistente entre as equipes de TI e TA também pode ser considerada como um dos impeditivos para a implantação de políticas ou estratégias de atualização de software. Certamente com esta integração um ponto médio entre a implementação automatizada, largamente utilizada pelas equipes de TI e um processo mais pontual, porém eficaz, gerenciado pelas equipes de TA atenderia a requisitos mínimos de atualização e Segurança da Informação.

No caso do setor elétrico a falta de uma política que remunere investimentos nestes serviços, também interfere de forma negativa na implementação de medidas desta natureza. Ainda que novos empreendimentos tenham implementado processos semelhantes, o setor não tem uma regra definida para tratar a proteção necessária de infraestrutura crítica.

2.3 Pesquisas futuras

Ao verificar as iniciativas em andamento, de fato existem atores do sistema elétrico que implementaram processos de atualização de software e muitas outras iniciativas relacionadas a Cyber Segurança com sucesso. Avaliando o ambiente de Geração, Transmissão e Distribuição os casos de sucesso podem ser vistos em eventos do setor, bem como nas redes de relacionamento que hoje também servem para coletar estas informações.

Por outro lado, a falta de regulamentação e sobretudo ações estratégicas relacionadas a Cyber Segurança são fatores críticos e decisivos para não identificarmos mais casos de sucesso, algo que sob o ponto de vista do consumidor de energia ou especialista em Segurança da Informação mostra uma perspectiva de grandes projetos a médio e longo prazo.

Em função dos estudos feitos e as constatações ao longo da confecção deste informe técnico, algumas oportunidades de pesquisa se apresentaram e serão sugeridas a seguir.

- a. Avaliar as oportunidades de contratação de serviços de suporte e modelos de atuação visando adequar os serviços ao setor elétrico.
- b. Envolvendo os principais atores do sistema elétrico, quais seriam as prioridades no que se refere a

Segurança da Informação e o nível de maturidade das organizações em relação ao tema.

- c. Identificar o nível de integração entre as equipes de TI e TA no setor elétrico. Quais atividades ou projetos já desenvolvidos, ganhos ou benefícios identificados.
- d. Qual a percepção do setor elétrico, quanto a utilização de cloud computing como opção para redução do custo de propriedade e principalmente no que se refere a atualização dos produtos.
- e. Qual a razão (ou razões) para não implementar um processo de atualização de software.
- f. Aplicados ao setor elétrico, que indicadores voltados para Cyber Segurança, poderiam ser um diferencial para a alta direção das organizações.

3.0 - CONCLUSÃO

A seguir algumas conclusões baseadas neste informe técnico.

O alto custo dos equipamentos, indisponibilidade de equipamentos idênticos para testes, falta de pacotes de licença para instalação e complexidade dos sistemas impedem uma abordagem semelhante ao ambiente de Tecnologia da Informação nos ambientes de Automação.

O processo de atualização de software pode evitar a propagação de um ataque, desde que todas as ferramentas, responsabilidades e identificação de causa do ataque leve a real necessidade de instalação de um update ou path.

Com a velocidade das mudanças dos produtos e aumento dos ataques, combinada a grande capacidade dos atacantes, a atualização de software deve minimizar a exposição a riscos cibernéticos, mas não elimina por completo a questão "proteção". Outros processos, produtos e serviços devem ser empregados visando aumentar a Segurança da Informação e manter a organização preparada para lidar com incidentes de Segurança da Informação.

A falta de uma política nacional voltada para Cyber Segurança, específica para o setor elétrico, além da opção das organizações no sentido de não fazer investimentos significativos neste tipo de proteção, inibe um aumento na gama de casos de sucesso relacionados a processos de atualização de software na área de Automação.

A integração entre equipes de Tecnologia da Informação e Tecnologia de Automação será de suma importância para a mudança do cenário atual, por outro lado, as organizações devem independentemente da integração, iniciar projetos de longo prazo voltados para a proteção de sua infraestrutura do ponto de vista físico e sistêmico.

REFERÊNCIAS BIBLIOGRÁFICAS

- (1) G1. Saiba como age o vírus que invadiu usinas nucleares no Irã e na Índia. 02 out. 2010. Disponível em: <http://g1.globo.com/tecnologia/noticia/2010/10/saiba-como-age-o-virus-que-invadiu-usinas-nucleares-no-ira-e-na-india.html>
- (2) CISA - Cyber+Infrastructure. Alert (IR-ALERT-H-16-056-01) 25 fev. 2016. Disponível em: <https://ics-cert.us-cert.gov/alerts/IR-ALERT-H-16-056-01>
- (3) ITIL. Disponível em: <https://www.axelos.com/best-practice-solutions/itil/what-is-itil> Acesso em 06 mar. 2019.
- (4) ANSI/ISA-TR99.00.01-2007 Security Technologies for Industrial Automation and Control Systems. Disponível em: www.isa.org Acesso em 18 abr. 2019.
- (5) Tecmundo. O que é patch? 21 jun. 2012. Disponível em: <https://www.tecmundo.com.br/software/1179-o-que-e-patch-.htm>
- (6) BRANQUINHO, Marcelo Ayres et al. *Segurança de Automação Industrial e SCADA*. Rio de Janeiro: Elsevier, 2014.
- (7) ISA/IEC 62443. Disponível em: www.iec.ch/index.htm Acesso em: 25 fev. 2019.

4.0 - DADOS BIOGRÁFICOS



Fábio dos Santos Oliveira
Coordenador de Segurança da Informação - Voith América Latina



Jéssica Barbosa Heluany
Engenheira de Aplicação