Recomendações sobre Cyber Security para plantas indústriais

Uma abordagem prática processual para proteção cibernética em Tecnologia Operacional

Por Patrik Boo
Gerente de Cyber Security
Process Automation, ABB, USA

Sumário Executivo

OT, ou a Tecnologia Operacional que controla os processos industriais, está ficando mais conectada a serviços em cloud externos. Isso permite novas capacidades e habilidades de gerenciar os sistemas de controle de automação industrial, mas ao mesmo tempo tem o risco de torná-los mais vulneráveis a cyber ataques. Decidir como obter esses benefícios enquanto protege suas operações pode gerar confusões.

Com base em nossa vasta experiência tanto com cyber security e sistemas de automação de processo industrial, o conselho mais importante que nós podemos dar é: Fazer algo é melhor que não fazer nada. Não há razão de deixar de aproveitar os benefícios dos novos serviços digitais e o que essas soluções podem fornecer simplesmente porque você está com receio de conectar seus sistemas de produção na rede corporativa e permitir tráfego da web. Aplicar cyber security em sistemas industriais não é tão complicado; há muitas empresas que podem ajudar e muitas vezes é mais econômico terceirizar essa parte. E por fim, não cuidar da segurança cibernética é um risco enorme que provavelmente não irá compensar.

Aqui nós vamos apresentar um passo a passo prático do qual você pode seguir as etapas necessárias para implementar cyber security nos seus processos e operações, enquanto aproveita as vantagens oferecidas dos muitos benefícios da manipulação moderna do big data.

Índice

04	Introdução - Há ganhos a serem feitos no setor industrial
06	O que é a cyber security para OT e qual a diferença de cyber security para IT
07	Ocorrências de cyber security industrial dignos de atenção
08	Não entre em pânico - Comece com uma avaliação
09	Sem um backup, você não tem nada
10	Agora, coloque os Controles de Segurança básicos
11	O envelhecimento também afeta a segurança
11	Treinando pessoas: Altamente efetivo para reduzir riscos
12	Sem atalhos até a verdadeira segurança
13	Etapas simples cobrem 85% dos riscos
14	Vale muito a pena considerar colaboração
15	Recursos compartilhados oferecem eficiência
16	Arquitetura de Referência
17	Medidas avançadas de segurança
18	Eventos notáveis - em retrospecto
19	Conclusão

Introdução
Há ganhos a serem feitos no setor industrial

Na era da informação de hoje, os dispositivos conectados nos dão conhecimento, poder de análise e capacidade de tomada de decisão que não podíamos imaginar há alguns anos.

Um exemplo simples é configurar seu smartphone ou dispositivo residencial inteligente para ajustar sua rotina matinal para obter máxima eficiência. O alarme da manhã é configurado, com base em diversos fatores como primeira reunião agendada do dia, sua média de tempo para tomar banho e se vestir e tempo real estimado para dirigir até o escritório. Seu dispositivo inteligente também irá informar o clima do dia, assim você poderá escolher com mais rapidez a roupa adequada, enquanto prepara seu café e lê as principais notícias do dia para você.

Cerca de cinco minutos antes de você sair, seu dispositivo inteligente vai ligar seu carro e ter certeza de que sua área interna esteja refrigerada ou aquecida, dependendo da estação do ano. Caso você utilize aplicativos de corrida compartilhada para chegar ao trabalho, este também poderá programar um carro para garantir que você chegue ao escritório para a primeira reunião. Todos esses passos otimizam a eficiência de seu tempo e de recursos, combinando para que resulte na mais alta produtividade sem estressar você.

Ganhos paralelos de eficiência na produção industrial
A pergunta natural agora é: Nós podemos colher melhorias de eficiência similares, e ganhos financeiros sem precedentes, nos sistemas de produção industrial de hoje ao usar tecnologias relacionadas?

A resposta é: Sim, a digitalização e princípios cibernéticos podem permitir isso. E na verdade não há nada de novo desde que nós aprendemos bastante de IT, e agora de OT, a tecnologia operacional que opera a indústria, está passando por uma imensa transformação similar da tecnologia. Você deve certamente já ter ouvido e lido bastante sobre inúmeras variações sobre esse tema.

Como muitas outras ideias em desenvolvimento, essa transformação é conhecida por diferentes nomes. Entre eles estão IIoT (Internet das Coisas Industrial), Indústria 4.0 e ABB Ability™.

Todos são similares em linhas gerais básicas, ainda que levemente diferentes nos detalhes; alguns se referem ao conceito geral (ex: Indústria 4.0) e outras em relação à estratégia específica da empresa para o conceito (ex: ABB Ability™).

Não importa qual nome é utilizado, o importante é que avanços na tecnologia e comunicação agora significam que você pode alavancar essas novas ferramentas para aumentar de forma significativa sua eficiência industrial e produtividade.

Como exemplos simples, imagine os benefícios financeiros gerais que seriam obtidos se você pudesse disponibilizar capital ao antecipar o que o mercado precisa e, assim, produzir exatamente e somente o que é necessário. Ou, poder reduzir sua matéria prima e custos de produção em 10% com apenas pequenos ajustes de eficiência no processo. Ou, aumentar sua produtividade total em 10% sem fazer qualquer investimento adicional de capital.

Todos esses ganhos são possíveis por meio do uso de advanced data analytics, e que pode ser realizado pela integração de processos de manufatura industrial com serviços e soluções digitais modernas.

O ponto fraco que não pode ser ignorado
Contudo, há um ponto fraco nesta cadeia que nós devemos tratar, conforme nos movemos nesta direção.

Para colher os benefícios que podem ser obtidos de advanced data analytics, os processos automatizados, e mesmo as tomadas de decisões automatizadas, nós devemos primeiro reconectar sistemas anteriormente desconectados. Para obter dados de/para redes, no local e cloud, nós devemos criar conexões que, infelizmente, expõem vulnerabilidades onde criminosos cibernéticos podem explorar.

Um ataque de êxito provavelmente acabaria com qualquer ganho financeiro das soluções digitais - sem mencionar a possibilidade de danos para a reputação e confiabilidade da empresa, ou ainda prejuízos referentes aos ativos ou lesões em pessoas.

Tal como diz o ditado, “a corda sempre arrebenta do lado mais fraco”, para obter o total potencial da cadeia de transformação digital, o lado de cyber security não pode ser o mais fraco.

Confiança e trabalho em equipe são absolutamente essenciais
No passado, e em alguns casos mesmo nos dias de hoje, os times de TI e de TO dentro de uma mesma empresa estavam longe da colaboração perfeita. Isso é muito comum devido à falta de confiança entre ambas as partes. O time de TO se preocupa se o time de TI não vai fazer o caos nos sistemas de TO e não entendem o que significa ser responsável pela produção industrial. Já para o time de TI falta tal confiança em relação à experiência e conhecimentos do time de TO quando se trata de proteger o que eles consideram sistemas comuns de TI e que eles já protegem há décadas.

Há inúmeras histórias sobre como TI, com boas intenções, aplicou medidas de segurança nos sistemas de OT e desligou toda a produção. Os culpados mais comuns são variações de scanners e ferramentas de coleta de informações computacionais. Essas ferramentas nunca foram desenvolvidas ou testadas em sistemas DCS, e os times responsáveis pelo DCS nunca consideraram que elas seriam utilizadas em seus sistemas.

No lado positivo, há também muitas histórias em que TI e TO decidiram trabalhar juntos e conseguiram implementar uma segurança robusta sem afetar a produção. Essas parcerias muitas vezes também resultaram em custos gerais menores.

Sem sombra de dúvidas, a empresa não tem interesse no conflito entre esses dois times. Para obter resultados duradouros e positivos, esses dois times devem trabalhar juntos e aprender uns com os outros. Talvez não seja fácil, mas certamente não é impossível.

O que é a cyber security para OT e qual a diferença de cyber security para IT?

OT significa a Tecnologia Operacional usada na produção industrial, e esta pode dizer que cyber security para OT é basicamente o mesmo que cyber security da Tecnologia da Informação (IT), visto que ambas na maior parte tem como base a mesma tecnologia. As principais diferenças são:

1. **Onde a tecnologia é aplicada: em um sistema industrial (TO) ou um sistema corporativo (TI).**
   Um sistema industrial nunca deve ser suspenso fora do período de interrupção planejado, o que significa que a disponibilidade do sistema pode de alguma forma ser prejudicada. Um operador não quer de forma alguma ver um alarme notificando que sua estação de trabalho será reiniciada em 30 minutos para instalar atualizações de segurança. As soluções de cyber security para OT precisam ser configuradas para trabalharem com seu cronograma da produção enquanto mantêm a segurança ideal.
   E mesmo a diferença mais básica é que os sistemas de TI controlam softwares relativamente modernos que rodam em hardware padrão, enquanto os sistemas de TO manipulam dispositivos físicos muitas vezes controlados por uma variedade de tecnologias novas e antigas.

2. **Como a segurança cibernética é implementada**
   Ainda que as ferramentas e metodologias utilizadas sejam muitas vezes a mesma para TO e TI, há diferenças essenciais em aplicá-las. Aplicar soluções comuns de cyber security para TI para sistemas de TO sem fazer mais considerações ou ajustes, provavelmente irá, em algum momento, levar a problemas operacionais.
   Uma prática de segurança comum e sensível do mundo de TI que não se aplica tão bem para TO é a ação de bloquear a conta de um usuário se a senha for inserida incorretamente muitas vezes. Se usarmos a mesma abordagem em TO, o resultado pode ser um operador bloqueando o sistema de produção industrial, incapacitado de controlar o processo, ou até mesmo de evitar um estrago, simplesmente porque a senha foi digitada incorretamente algumas vezes.

3. **Quanto tempo espera-se que o equipamento permaneça em operação**
   Um dispositivo de TI como um laptop será facilmente substituído a cada 3-5 anos, enquanto componentes em um sistema DCS permanecerão em operação por muito mais tempo. Controles de cyber security modernos podem ser aplicados no laptop sem muita contrapartida, porque ele é relativamente novo e raramente dependente, ou necessita de suporte de outros dispositivos. Porém, um sistema DCS é constituído de alguns diferentes dispositivos que devem funcionar juntos. Aplicar cyber security em um servidor moderno dentro do sistema DCS pode afetar negativamente outras funções que não podem controlar o novo recurso de segurança - simplesmente porque eles têm como base uma tecnologia mais antiga.

Ocorrências de cyber security industrial dignos de atenção

Vamos olhar alguns exemplos. Mesmo que alguns deles sejam um pouco antigos agora, eles foram selecionados devido às diferenças de como o ataque foi orquestrado e devido às suas informações estarem na rede, facilmente disponíveis.

Merck:
A companhia farmacêutica Merck foi submetida a um ataque Ransomware em 2017. O malware entrou em mais de 30.000 computadores e 7.500 servidores. Anos de pesquisa foram perdidos, operações normais foram seriamente afetadas. Não se sabe o impacto financeiro que foi para a Merck, mas a companhia finalmente processou suas operadoras de seguro, pedindo $1.3 bilhão[1] pelos prejuízos.

Energia Ucraniana:
Em 2015, uma geradora de energia Ucraniana foi atacada por um grupo de hackers, provavelmente estado-nação. O ataque fez com que mais de 225.000 consumidores[2] ficassem sem energia por 6 horas. Os criminosos cibernéticos usaram diversas estratégias e métodos para acessar o sistema e desligar a geração de energia. O fator principal foi que os criminosos tiveram bastante tempo para entender o sistema, incorporá-lo, e então aguardar pelo momento certo para atacar.

Instalação de enriquecimento Natanz:
Esse caso, mais conhecido como Stuxnet[3], é um dos cyber ataques mais famosos no setor industrial, tanto pela sofisticação quanto pelo seu impacto. Ele foi um dos primeiros arquivos malware criado para atacar um sistema industrial. O vírus entrou na instalação e mudou o código do sistema SCADA que controlava as centrífugas usadas para enriquecer urânio, com a intenção de fazê-las operar de forma que conduzisse a falhas. Como isso ocorreu em uma instalação nuclear confidencial no Irã, o impacto exato do ataque é desconhecido. O que podemos especular é a extensão dos danos que poderiam ser causados no manuseio de materiais radioativos.

O que poderia ter sido feito, se possível, para evitar, ou reduzir, o impacto desses ataques? As seguintes seções deste artigo irão descrever sistematicamente boas medidas que podem ser aplicadas para aumentar a resiliência cibernética de um sistema de controle de automação industrial. No final, nós iremos revisitar os três exemplos citados para ver se a segurança cibernética teria tido um impacto menos desastroso.

—
01 https://www.bloomberg.com/news/features/2019-12-03/merck-cyberattack-s-1-3-billion-question-was-it-an-act-of-war
—
02 https://us-cert.cisa.gov/ics/alerts/IR-ALERT-H-16-056-01
—
03 https://en.wikipedia.org/wiki/Stuxnet

Não entre em pânico
Comece com uma avaliação

Pelo motivo de muitos sistemas OT terem sido desenvolvidos muito antes da segurança cibernética, para os sistemas OT ser considerada necessária, os hackers muitas vezes acham mais fácil hackear esses sistemas do que sistemas de IT - usando a bagagem de experiência obtida ao hackear sistemas de TI. Pelo motivo de TI e TO estarem convergindo ou fundindo-se, e os sistemas industriais estarem potencializando soluções e dispositivos comerciais de TI, vemos um número cada vez maior de cyber ataques em sistemas industriais.[4]

Embora a frequência dos cyber ataques em sistemas industriais estar aumentando e vimos exemplos o quão ruim podem ser os impactos financeiros, para a reputação e ao meio ambiente com cyber ataques bem sucedidos, nem pense em desistir e ignorar a realidade. Implementar cyber security em sistemas TO não é muito diferente do que qualquer outro projeto ou iniciativa que você possa se encarregar.

Comece com uma avaliação verdadeira para ter o entendimento do escopo geral de suas necessidades de cyber security. Isso é mais fácil de fazer respondendo a essas perguntas: O que você está protegendo? Como o sistema é projetado e essa arquitetura suporta uma segurança cibernética robusta? Quais ativos você tem no sistema? E qual é o elo mais fraco na rede?

Se você não sabe todas as respostas, é difícil saber por onde começar ou como avaliar se os recursos que estão sendo usados para tarefas protetivas realmente trarão melhorias consideráveis em defesa em cyber security.

As etapas de uma avaliação eficaz podem ser definidas com o que vem a seguir:

1. Começar percebendo todos os cyber ativos no sistema. Considera-se cyber ativo qualquer dispositivo conectado à rede industrial que é usado pelo sistema DCS. Geralmente, os dispositivos são conectados a uma rede usando uma conexão Ethernet, mas não se esqueça dos outros links de comunicação entre os dispositivos no sistema geral visto que esses podem também ser usados em um ataque. Por exemplo, uma conexão Modbus pode ser “influenciada” a enviar dados falsos para o sistema para iniciar uma falha ou para mascarar um ataque em andamento.
   Criar esse inventário é um trabalho difícil, mas há ferramentas e soluções que podemos usar para reduzir o trabalho manual. Apenas lembre-se de somente usar as ferramentas e soluções DCS validadas e homologadas pelo fornecedor para conter o risco de problemas.

2. O próximo passo é atualizar os desenhos das redes do sistema e colocar todos os dispositivos neste desenho de arquitetura. Esse é um passo crítico conforme ele mostra como os dispositivos estão conectados e como eles interagem e se comunicam um com o outro. Certifique-se de incluir a maior quantidade de detalhes possíveis visto que um bom desenho da rede serve para diversos objetivos, não somente aos relacionados à cibernética. Outros tipos de desenho que valem considerar são a visão geral, "conduítes" e zonas, redes físicas, VLAN e desenhos de fluxo de dados. Se isso é feito manualmente, certifique-se de ter um processo documentado para atualizá-los regularmente.

3. E por último, deve-se realizar uma avaliação de risco. Essa avaliação irá identificar e ajudar a priorizar as partes do sistema que podem causar maiores prejuízos, tanto financeiro ou aqueles relacionados à saúde e segurança, se estes forem atacados. O processo de avaliação de risco força você a focar em cada dispositivo e função para responder duas perguntas críticas: Qual a probabilidade disto estar sujeito a um incidente cibernético? E qual é o impacto do incidente em termos de escala e consequência? Esses dois componentes, a semelhança e o impacto, são o que faz o risco total, e uma boa avaliação de risco irá fornecer orientação em como melhor priorizar seus recursos e budget.

Vale o esforço

Embora o processo esboçado anteriormente exija um certo nível de esforço, valem muito a pena. Quando feito, você terá até este ponto uma imagem excelente de quais dispositivos você tem no sistema, como eles estão conectados, onde os riscos estão e quais riscos são os mais sérios. Sabendo isso, você pode começar a implementar vários controles de cyber security, mas somente após você ter cuidado de outras tarefas cruciais, como backups.

—
04 O mais recente X-Force da IBM Threat Intelligence Index descobriu que os ataques em instalações industriais e de manufatura aumentaram mais de 2000% desde 2018.

Sem um backup, você não tem nada

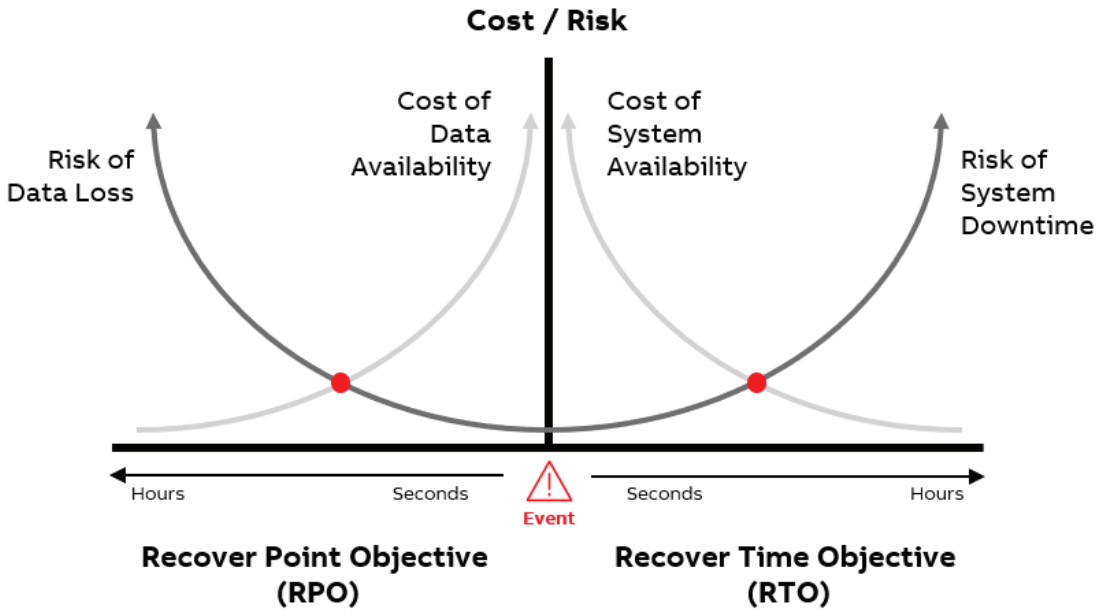
Uma vez que o sistema ou os sistemas foram avaliados, seu primeiro passo deve ser implementar e configurar uma solução de backup. Essa é sua última linha de defesa. Uma solução de backup é essencial desde que um bom backup assegure que o investimento feito no sistema DCS esteja protegido. No caso de um incidente ou falha com o hardware ou software, você pode facilmente restaurar o sistema DCS por completo ou partes e, então, retomar a a produção rapidamente. Tais incidentes ou falhas podem estar relacionadas à cibernética, mas muitas vezes elas são simplesmente erros do operador ou usuário.

Outro aspecto dos backups que deve ser considerado é o plano de continuação do negócio em que você define o volume de dados que você está disposto a perder (Ponto de retomada em contingência - Recovery Point Objective[5]) e o depois de quanto tempo após um desastre você deve estar com a produção na ativa (Tempo para retomada em contingência - Recovery Time Objective[5]). Esses fatores determinam a configuração do sistema backup, esquemas de backup e preço. Um plano de continuação do negócio com baixo RPO e/ou RTO requer mais do sistema de backup do que um plano em que é menos crítico restaurar a produção rapidamente de forma excepcional.

Saber que o sistema tem uma cópia de segurança segura também significa que você pode implementar atualizações, melhorias de desempenho, e soluções de cyber security mais rápidas porque você sabe que há uma forma de restaurar para a versão mais recente do sistema se algo der errado.

Agora, você pode começar a assumir os controles de segurança.

—
05 https://www.msp360.com/resources/blog/rto-vs-rpo-difference/



Agora, coloque os Controles de Segurança básicos em funcionamento

Até essa parte do processo, na verdade, o que nós fizemos não deixou o sistema mais seguro. Nós somente o avaliamos para nos certificar de que aplicamos os controles de segurança certos, nos lugares certos - onde eles terão os impactos mais consideráveis e benéficos. Nós também nos certificamos de que nós podemos nos recuperar de um desastre usando um backup.

Controles de segurança são essenciais
Controles de segurança é tudo aquilo que funciona ativamente para proteger o sistema. Os controles de segurança mais comuns são atualizações de segurança e proteção contra malwares. Para um profissional de TI ou até mesmo um amador, utilizar-se dessas medidas é tão básico que é impensável que qualquer computador esteja rodando sem eles. Porém, a realidade é que muitos sistemas industriais estão operando sem esses controles ou desatualizados.

As razões dadas para explicar porque as atualizações e proteção contra malware não são aplicadas é muitas vezes uma dessas três desculpas:

"Eu nunca tive problemas no passado"

"Eu não quero arriscar fazer essas atualizações no sistemas ativo, pois tenho que mantê-lo em operação"

"Nosso sistema é totalmente isolado (não está conectado a nenhum outro sistema ou rede)"

Experiências anteriores são boas, mas com certeza não garantem o que pode acontecer no futuro. Ameaças evoluem e mudam, então o que funcionava ininterruptamente no passado provavelmente não funcionará no futuro.

Quando alguém aplica as atualizações de segurança e proteção contra malware corretamente, o risco para a produção é muito menor do que operar sem nenhuma proteção atualizada. E, por último, isolamento físico NÃO é um controle de segurança. A Instalação Nuclear Natanz era fisicamente isolada, sem conexão à rede para qualquer instalação externa. Se uma instalação nuclear não consegue isolar com sucesso um sistema localizado em uma instalação isolada longe do invasor, quem poderá?

A proteção contra malware e procedimento para atualização de segurança
Mesmo controles tão básicos como proteção contra malware e atualizações antivírus devem ser implementados com cuidado para evitar um impacto negativo na produção, tanto durante a implementação e em uma operação normal. Somente atualizações de segurança aprovadas pelo provedor do DCS devem ser instaladas, e somente proteção contra malware devem ser utilizadas.

Controles de segurança adicionais
Outros controles de segurança que vale mencionar incluem whitelisting de aplicações, inventário de ativos e hardening do sistema. Cada um desses melhora a defesa em termos de cyber security ao adicionar proteção em vários aspectos.

- Uma whitelisting evita que aplicações não aprovadas operem, o que é um controle de segurança robusto, mas somente quando combinado com atualizações de segurança e proteção contra malware.

- Um inventário automatizado de ativos bem projetado ajuda o usuário a detectar quaisquer novos dispositivos conectados ao sistema. Uma vez detectado, eles podem ser adicionados ao conjunto de itens protegidos pelos controles de segurança. Porém, se o dispositivo detectado não é conhecido, ele pode estar relacionado com um ataque.

- O hardening configura o computador para ser o mais seguro possível ao mesmo tempo em que continua desempenhando suas funções primárias. Um sistema que monitora as configurações de hardening fica atento a essas configurações e certifica-se de que ninguém as mude para um estado menos seguro, reduzindo ainda mais o risco de alterações intencionais ou não que tornam o sistema vulnerável a ataques.

Além desses controles de segurança, há muitos outros produtos e soluções disponíveis no mercado. Suponha que alguns deles apareçam para resolver um problema específico ou risco que você identificou durante a avaliação de risco. Neste caso, é necessário ter certeza de que eles adicionam segurança ao seu sistema e não irão impactar negativamente na disponibilidade do sistema e na produção.

O que nós cobrimos até agora relacionado a controle de segurança enquadra-se na categoria de controles chamada controles técnicos que significa que nós aplicamos tecnologia para tratar de riscos cibernéticos. Há também controles físicos (think locks etc.) e controles administrativos (treinamentos e tal)[6] que podem ser usados para criar uma defesa holística contra riscos cibernéticos.

—
06 https://www.f5.com/labs/articles/education/what-are-security-controls

O envelhecimento também afeta a segurança

Como qualquer outra coisa, os sistemas operacionais envelhecem, e em algum ponto o fabricante irá encerrar o suporte de aplicações antigas. Uma vez que isso acontece, nenhuma segurança ou atualizações de proteção contra malware serão lançadas para o sistema desatualizado. Isso deve ser evitado porque uma vez que as atualizações param de chegar, é só uma questão de tempo antes do sistema ficar aberto às vulnerabilidades, como permitir um vírus entrar e deixar o sistema instável e inutilizável. Não entre nessa em que você é forçado a tomar uma atitude apenas porque um software não suportado ficou antigo. Em vez disso, seja proativo, assuma o controle da segurança cibernética, e conduza isso da maneira que você achar melhor.

Treinando pessoas
Altamente efetivo para reduzir riscos

Falamos até aqui das avaliações e controles de segurança, mas até agora deixamos para trás o risco mais considerável em qualquer organização: os funcionários. Inúmeros ataques devastadores que deram certo usaram os funcionários das empresas para entrarem nos sistema-alvo[7]. Isso pode ser alguém que faz de maneira deliberada ou sendo forçado a realizar a tarefa para um cyber criminoso.

Porém, o caminho mais comum é que o hacker engana alguém para ajudá-los sem saber. Um exemplo comum é usar e-mail para conseguir que o destinatário clique no link que faz o download de um vírus no computador do usuário. Uma vez inserido, o vírus pode se espalhar por si só e fazer o estrago ou estabelecer um vínculo com o hacker para acessar e manipular o computador para chegar ao alvo. Isso é chamado de phishing ou spear-phishing, dependendo se é um e-mail enviado em massa ou para uma pessoa específica.

Mesmo os sistemas fisicamente isolados são vulneráveis visto que os estudos mostram que você poderia simplesmente “deixar” pen drives infectados no estacionamento local do alvo pretendido e esperar que alguém apareça para pegá-lo e depois conectá-lo a um computador[8].

Adicione a isso o fato que pouquíssimos sistemas realmente são isolados[9].

A forma mais eficaz de tratar esses riscos é com treinamento de conscientização. No treinamento haverá debates de cyber security, formas de ataque e comportamento para reduzir riscos com alguém que estará perto do sistema e seus componentes. Essa abordagem de baixo custo costuma dar muito certo. Apenas lembre-se que o treinamento deve ser sistemático, recorrente e obrigatório. Qualquer novo funcionário ou contratado deve realizar o treinamento antes de acessar ou estar em contato com o sistema.

Você também deve treinar seu time de cyber security para eles aproveitarem o máximo do investimento nos controles de cyber security. Os controles são tão bons quanto as pessoas que estão usando e gerenciando-os.
Você pode pagar milhões de dólares por controles cibernéticos, mas se ninguém souber utilizá-los ou mantê-los, eles não agregam absolutamente nenhum valor. Se seus controles de segurança avisam você sobre potenciais violações, mas ninguém está olhando para isso, um criminoso pode ter livre reinado. O mesmo acontece se os controles de segurança não estão funcionando devido a uma falha na manutenção.

—
07 Acredita-se que o ataque Shamoon usou funcionários para que o vírus entrasse nos sistemas. https://en.wikipedia.org/wiki/Shamoon

—
08 https://www.blackhat.com/docs/us-16/materials/us-16-Bursztein-Does-Dropping-USB-Drives-In-Parking-Lots-And-Other-Places-Really-Work.pdf

—
09 Conforme dito por Sean McGurk, ex-diretor do Centro de Integração Nacional de Segurança Cibernética e Comunicação (NCCIC) do departamento de Segurança Nacional https://blog.safe-t.com/industrial-security-is-the-air-gap-still-viable

Sem atalhos até a verdadeira segurança

Porque, algumas vezes, a segurança cibernética tem um estigma de ser muito complicada, e nós tendemos a ter uma necessidade inerente por resultados rápidos, seja na tentação ao receber ofertas de marketing de produtos que prometem resolver todas as suas necessidades de proteção cibernética de vez. Esse produto não existe! Devemos sempre começar com o básico, conforme mencionado anteriormente.

Se alguém prometer solucionar todos os problemas cibernéticos sem explicar como e sem cobrir o básico, você deve ter cuidado. Você não quer gastar dinheiro ou confiar em algo que provavelmente não irá proteger seus processos de OT e da produção. Ou, pior, dar uma falsa sensação de segurança para fazer você baixar a guarda.

Proteção é igual a segurança; você nunca pode relaxar ou parar de melhorá-la.

Etapas simples cobrem 85% dos riscos

Até aqui, se você tomou nota das medidas anteriores, você deve ter um sistema razoavelmente seguro do qual você cuidou dos riscos e que já são capazes de evitar a maioria das ameaças. O CIS (Centro para Proteção na Internet) estima que até 85% dos riscos cibernéticos podem ser tratados com simples medidas que visto até aqui[10]. Vamos rever o que nós temos:

1. Conheça seu sistema

   a. Um inventário de ativos completo de todos os ativos cibernéticos que assegure que nenhum dispositivo fique para trás ou tenha menos proteção do que o resto.

   b. Uma visão geral completa da rede e como os dispositivos interagem uns com os outros para criar o sistema de produção.

   c. Conhecimento de onde os maiores riscos estão, qual a probabilidade de um ataque dar certo e qual será o seu impacto.

2. Controles Básicos de Proteção

   a. Todos os computadores com Windows no sistema operacional estão em dia com as atualizações de proteção mais recentes e aprovadas pelo provedor para minimizar o número de vulnerabilidades que os criminosos virtuais podem tirar vantagem.

   b. Todos os computadores com Windows têm proteção contra malware que seja atualizado frequentemente, o que mantém a proteção do sistema ao detectar e defender contra os últimos vírus.

   c. Se as coisas ainda assim derem errado, o que pode acontecer, visto que não existe um sistema 100%, e que os computadores quebram, há backups para permitir uma restauração rápida e produção continuada em caso de um problema.

3. Treinamento

   a. Todos que podem vir a entrar em contato com o sistema, ou qualquer parte dele, sabem o que fazer ou o que não fazer com ele. Isso limita o risco da entrada de um malware no sistema, assim como interrupção acidental devido a falta de cuidado.

   b. Aqueles que mantêm e utilizam os controles de proteção entendem como os controles funcionam, como se mantêm em operação, e o que fazer se algo acontecer.

Conforme discutido anteriormente, controles adicionais podem ser instalados, mas passos mencionados anteriormente devem ser considerados nas ações fundamentais de segurança cibernética que qualquer proprietário de sistema OT deve tomar.

—
10 https://www.cisecurity.org/media-mention/implementing-the-cis-20-critical-security-controls-slash-risk-of-cyber-attacks-by-85/

Colaboração, vale muito a pena considerar

Considere o investimento necessário para cyber security, desconsiderando os custos de hardware e software visto que isso é o de menos. Gerenciar cyber security in-house pode ser caro e toma tempo. Há muitos aspectos a considerar, tais como treinamento, ferramentas e procedimentos. Os proprietários do sistema devem equilibrar o investimento de empregar pessoas que tenham conhecimentos em cyber com o fato de que eventos cibernéticos não são tão frequentes.

Uma abordagem melhor e muitas vezes mais barata é buscar um parceiro para ajudar com a proteção cibernética. Uma empresa que forneça serviços de cyber security muitas vezes tem os melhores e mais experientes engenheiros porque eles lidam com cyber security todos os dias, durante todo o ano. A experiência que os especialistas dos parceiros podem fornecer é robusta para construção in-house, especialmente se o engenheiro cibernético trabalhar somente em uma localização e com um sistema. Ao aproveitar a parceria, o proprietário do sistema não precisa descobrir uma forma de maximizar o tempo do seu time de especialistas de segurança, mas tenha acesso aos especialistas do parceiro de segurança quando necessário.

Outra vantagem de um fornecedor externo é que você se beneficia de seus processos eficientes e ferramentas que muitas vezes já foram desenvolvidas ao longo dos anos e são frequentemente ajustadas e atualizadas. Como uma empresa externa trabalha com diversos clientes e outros fornecedores, eles têm uma boa noção do que está acontecendo no mundo e na indústria e muitas vezes estarão por dentro sobre as últimas tendências e as ameaças.

Ao selecionar uma empresa externa para ajudar com a segurança cibernética OT você deve considerar algumas coisas importantes:

- **Conhecimentos no sistema DCS:**
  A empresa está acostumada com OT ou são puramente especializados em IT? Você precisa de um parceiro que entenda cyber security para OT, como um sistema de controle funciona, e o que você precisa para manter a produção em operação.

- **Suporte:**
  A empresa será capaz de dar pronto atendimento caso algo aconteça? Você pode obter suporte 24/7?

- **Serviço centralizado:**
  O parceiro pode fornecer uma ampla variedade de soluções de cyber security? É muito menos provável que algo passe despercebido se você tiver um único responsável por cyber security, reduzindo o risco de gaps e simplificando as discussões.

- **Uma ampla seleção de soluções cibernéticas:**
  O fornecedor possui parceria com outras empresas de cyber para fornecer as melhores soluções e tecnologia, e essa tecnologia pode ser implementada de forma segura e correta?

- **Recursos:**
  Eles possuem os recursos corretos próximos da localidade de suas operações, caso você opere localmente ou em qualquer lugar do mundo? Existe algum risco que eles possam deixar você sem recursos suficientes, local ou globalmente?

- **Flexível:**
  O parceiro pode te atender independentemente de qual seja sua jornada em cyber security? Lembre-se, você deve construir a segurança do zero, e as coisas vão acontecendo sempre sem pular nenhum passo.

Recursos compartilhados oferecem eficiência

Um passo natural, uma vez que um parceiro foi encontrado é considerar as possibilidades de eles lidarem com a manutenção de cyber security e operação da segurança. A manutenção é basicamente deixar alguém, seu parceiro de confiança, ficar responsável por manter os controles de segurança, assim eles estão sempre operando e têm as atualizações e configurações corretas. Isso muitas vezes é fornecido remotamente para reduzir custos. Portanto, nunca se deve subestimar o valor que vem com conexões pessoais. Conhecer os engenheiros do seu parceiro pode ser útil quando um problema aparece ou ainda quando você tem dúvidas.

As boas relações pessoais são sempre valiosas, e é bom ter pessoas acostumadas com o parceiro para sua instalação, seus processos e seu pessoal.

O próximo passo após a manutenção são as reais operações, onde seu parceiro assume o trabalho real quando se trata de segurança cibernética. A manutenção descrita anteriormente garante que seus controles estejam funcionando, enquanto as operações garantem que seu sistema esteja protegido de acordo com o contrato de serviço. As operações podem ser tão simples quanto validar backups, reinicializando computadores após redistribuição das atualizações ou tão avançadas quanto monitoramento da segurança 24/7.

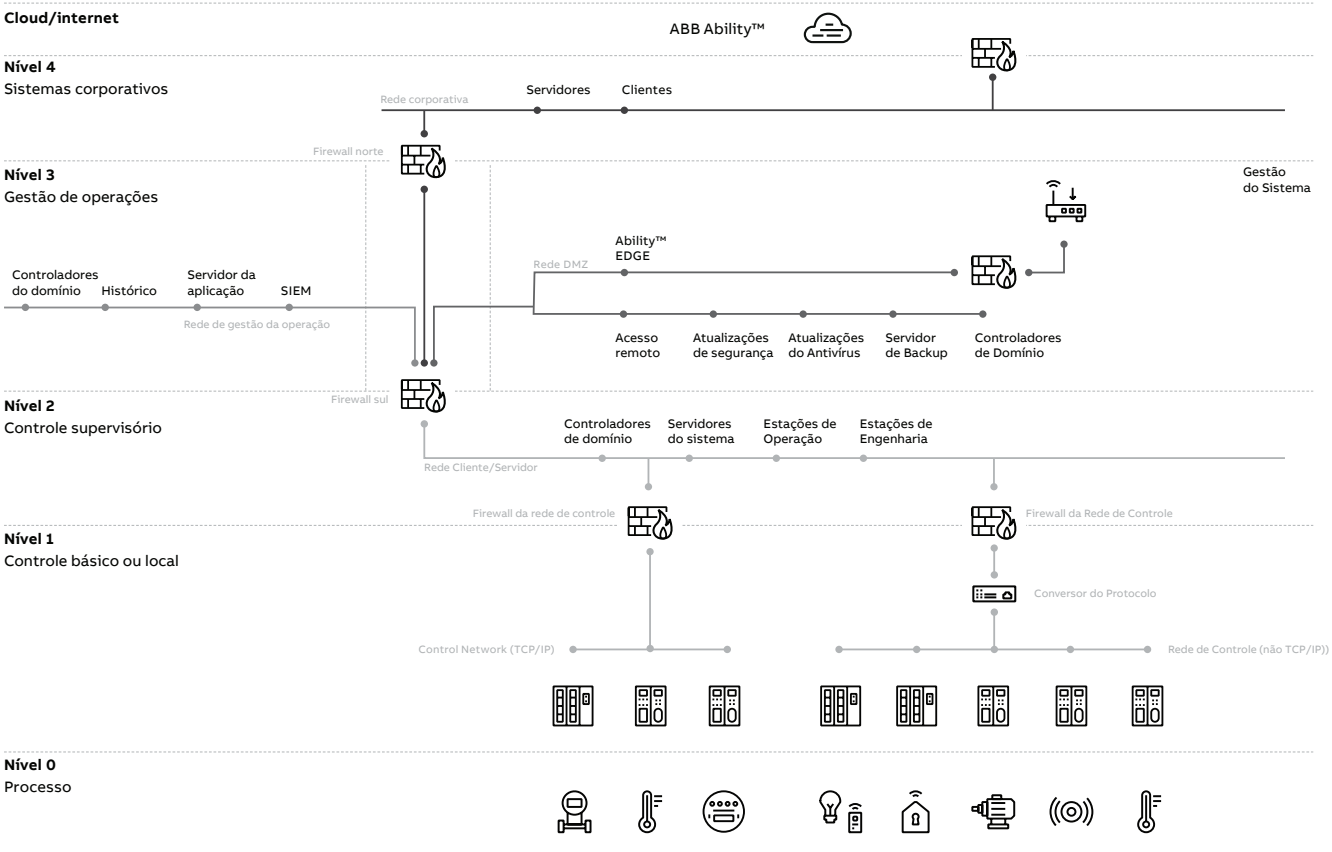
Arquitetura de Referência

No início desse artigo, vimos como a interconectividade hoje beneficia todos nós e como a indústria deveria também poder usar o insight que vem com a interconectividade para melhorar as operações e tomar melhores decisões para a produção. Aplicar uma boa segurança cibernética é um dos passos críticos necessários para aproveitar os benefícios do cloud computing de maneira segura.

Outro passo essencial é ter uma rede bem projetada em que o cuidado especial foi tomado para permitir o ir e vir dos dados necessários dos sistemas industriais, enquanto os mantêm seguros. A maioria dos padrões de segurança e melhores práticas cobrem essa necessidade em um grau ou outro. Transformar as recomendações desses documentos em um design real que permita dados entre seu sistema DCS e um serviço cloud não é muito difícil. Mesmo assim, há muitos aspectos a se considerar que podem ser complexos.

Uma opção melhor do que fazer isso sozinho, é confiar nos diversos modelos ou arquiteturas de referência disponíveis. Algumas dessas arquiteturas de referência são feitas para sistemas de TI e algumas para TO. Algumas são de natureza geral e outros são projetadas para vender mais produtos de um fornecedor.
Enquanto a maioria são muito boas e fornecem a segurança necessária, você deve ter cuidado ao escolher uma que funcione da melhor maneira para você, suas necessidades, sua empresa e seus sistemas.

Uma boa arquitetura é também necessária se sua ambição é atender certas normas e padrões, tais como nível de segurança específicos como um definido na IEC62443-3-3. Você economiza mais esforço se você escolher uma arquitetura que já atenda ou esteja acima do nível que você está almejando.



Medidas avançadas de segurança

Sem uma segurança construída em uma base forte, seu sistema está extremamente vulnerável. Conforme indicado anteriormente, com uma boa proteção básica você pode evitar mais de 85% das ameaças que correm o risco de impactar constantemente sua produção. Portanto, você pode querer ou precisar de um nível ainda maior de proteção.

Primeiro, você deve entender qual é sua tolerância a risco e qual o impacto financeiro que um incidente cibernético poderia ter. Somente quando você conhecer essas coisas você poderá decidir gastar mais em segurança ou não. Não há razão para pagar mais por segurança do que você tem a perder em caso de um incidente.

Naturalmente, muitos fatores geram o impacto financeiro - não somente nas perdas diretas da produção, mas também em outras coisas como reputação, multas ou saúde e segurança. A segurança básica pode ser suficiente, ou você pode precisar implementar mais segurança para alcançar o nível de proteção certo. Se você achar que 85% da proteção não é suficiente, então você precisa de medidas adicionais de cyber security.

Para ser claro, não importa o que você faz, você pode nunca estar 100% protegido. Não dá para conseguir isso.

Vigilância para atividades suspeitas
Mas para chegar perto de 100%, você deve aumentar os controles básicos com monitoramento. O monitoramento ajuda a detectar atividade anormal, então se algo ultrapassar pela primeira linha de sua defesa cibernética, você pode tomar a ação para reduzir o risco recém detectado.

Há basicamente dois métodos de monitoramento: Monitoramento de Evento e Monitoramento de Rede. Monitoramento de Rede usa logs disponíveis nos sistemas OT e dispositivos para detectar atividade suspeita, enquanto o monitoramento da Rede utiliza o tráfego da rede para fazer o mesmo. Eles complementam um ao outro e decidem qual deles começar dependendo de muitas coisas. Monitoramento do Evento é uma metodologia comprovada que alerta o usuário sobre qualquer atividade suspeita com base em regras (ex: pen drive inserido na máquina ou usuário tentou logar várias vezes com a senha incorreta). O monitoramento da rede é outra solução popular que detecta anomalias no tráfego da rede (ex: uma máquina na rede tenta alcançar um endereço IP de destino em outro país). O monitoramento da rede muitas vezes requer um investimento no equipamento em atualização da rede antes da implementação.

Independentemente de como você irá começar, é essencial ter uma equipe que monitore os alertas gerados para respondê-los, se necessário. Sem isso, você não pode perceber qualquer valor do investimento em segurança.

Até ter uma equipe monitorando essas funções, você mesmo também pode montar uma equipe ou pode encontrar um parceiro para te ajudar. A menos que você tenha um amplo sistema de produção ou vários deles, é mais provável que, em termos financeiros, valha a pena recrutar, treinar e montar seu próprio time.

O próximo componente de segurança, que se encaixa em monitoramento, é a resposta ao incidente. Essa é a ação tomada após o monitoramento do evento ou sistemas de monitoramento da rede detectarem algo suspeito. Quando isso acontece, o tempo e uma ação rápida são críticos se você quiser ter sucesso ao proteger suas operações, assim é vital ter as pessoas certas no lugar que você sabe que irão agir da forma correta para reduzir riscos. Essa é outra tarefa que você pode escolher fazer você mesmo ou realizar por meio do seu parceiro, dependendo do custo/benefício.

Eventos notáveis - em retrospecto

Sobre os ataques mencionados no começo deste artigo, vamos adicionar alguns pequenos insights nesses casos.

Merck:
Ransomware é um vírus terrível e algo que você quer evitar.

- Controles básicos: A melhor defesa contra isso é ter certeza de que as últimas correções de erros de segurança e proteção contra malware estejam instaladas assim que estiverem disponíveis. Infelizmente, ainda pode haver vulnerabilidades (também conhecidas como dia zero) desconhecidas que o criminoso virtual pode se aproveitar.

- Treinamento: a segunda medida que pode reduzir consideravelmente a probabilidade de ser infectado com ransomware, ou qualquer vírus, é o treinamento de conscientização que ensina a cada funcionário e terceirizado a identificarem um phishing ou ataque spear-phishing. São muitas vezes a forma como o ransomware entra no sistema. Outro método que é reduzido pelo treinamento é o golpe do pen driver no estacionamento que falamos antes.

- Backup: Faça backups e certifique-se de que eles estejam funcionando.

Energia Ucraniana
Esse ataque poderia ter sido evitado, ou pelo menos ter um impacto drasticamente reduzido, com um programa de cyber security bem implementado.

- Controles básicos: Algumas das superfícies de ataque teriam sido fechadas se os sistemas tivessem sido atualizados corretamente, com atualizações de segurança e proteção contra malware.
- Arquitetura de Referência: Uma rede bem projetada com zonas e "conduítes" teriam tornado mais difícil para o criminoso de se movimentar por ali.
- Monitoramento: Monitoramento de Evento ou Rede teriam fornecido um aviso prévio do que estava acontecendo e, se houvesse uma atuação, isso teria parado o ataque antes da produção ser impactada.

Instalação de enriquecimento Natanz:
O caso Stuxnet é diferente da maioria porque ele foi um ataque com alvo onde o objetivo dos hackers era somente interromper uma instalação. É complicado se defender contra ataques se você tiver o azar de se tornar um alvo explícito. Porém, as mesmas proteções básicas discutidas neste artigo ainda se aplicam e irão reduzir os riscos, mas não eliminá-las. Conforme mencionado anteriormente, não existe nada absolutamente seguro.

05 https://www.msp360.com/resources/blog/rto-vs-rpo-difference/

Conclusão

Se você não já implementou cyber security nos seus processos de OT, por favor comece já. Não é tão tarde, e não é tão complicado. Os passos aparentemente semelhantes que falamos anteriormente irão aumentar significativamente a resiliência cibernética do seu sistema e permitirá que você aproveite as vantagens dos novos serviços digitais entregues no local ou cloud. Se feita corretamente, seu sistema poderá lidar com a grande maioria de cyber ataques, e como um bônus, é provável que você fique com um sistema mais estável que funcione melhor e seja mais fácil de se manter.

Imagine um futuro em que o sistema de manutenção preditiva em cloud forneça para você - com antecedência - informações acionáveis que fazem seu processo industrial operar de forma mais tranquila, mais previsível, com mais eficiência e maior tempo em atividade. Muitos desses benefícios já estão disponíveis. Por exemplo, você não tem que gastar tempo com verificações regulares do seu sistema DCS visto que alguns serviços fazem isso por você e te avisam se algo precisa de sua atenção. Isso economiza tempo para você gastar em coisas mais importantes e também dá maior disponibilidade direta do sistema.

Similarmente, você pode usar dados de processo pertinentes para determinar quando as válvulas e loops de controle precisam de atenção.
Loops de controle otimizados estão diretamente correlacionados à qualidade aprimorada, custos com material reduzidos, e produção aumentada.
Para controles de cyber security, você muitas vezes desbloqueia funções e recursos adicionais ao permitir uma conexão para vários banco de dados online e sistemas. A avaliação da vulnerabilidade vinculada aos inventários de ativos, feito via monitoramento de rede, é apenas um exemplo em que uma conexão de internet fornece consideravelmente mais valor para seu investimento.

Finalmente, no topo de todos os benefícios listados anteriormente, você também sabe que você tem um sistema que é protegido contra mais de 85% de todas as ameaças cibernéticas.
Eu não sei você, mas eu com certeza dormiria melhor à noite sabendo que o sistema pelo qual sou responsável está protegido.

—
Para mais informações, você pode entrar em contato com a ABB Automation Brasil.

Antonio Carvalho
antonio.carvalho@br.abb.com
Digital Lead

Renato Martins
renato.martins@br.abb.com
Head of Sales

Créditos do artigo para:
Patrik Boo
Cyber Security Manager
Process Automation, ABB, USA