Cibersegurança na indústria de laticínios e refrigerantes

Minimização de riscos de acordo com CRITIS
www.siemens.com.br/alimentosebebidas

SIEMENS

Índice

A crescente digitalização das empresas e o networking associado de quase todas as indústrias estão gerando um enorme potencial econômico. Hoje, mais de 20 bilhões de dispositivos e máquinas já são conectados pela internet. Em 2030, esse número crescerá para cerca de meio trilhão. A digitalização e conectividade podem ser impulsionadores de crescimento e prosperidade, mas aumentar a conectividade também cria novas vulnerabilidades que precisam ser respondidas de forma rápida e consistente.

Isso também é aplicável às empresas do setor de alimentos e bebidas

Em 2017, uma das maiores empresas de alimentos e bebidas do mundo foi vítima do ransomware Trojan. O malware "Petya" atacou sistemas de computador do mundo todo e bloqueou seus usuários para extorquir dinheiro de resgate. De acordo com as próprias estimativas da empresa, o ataque cibernético resultou em uma perda de receita de cerca de US$140 milhões. Foram necessários vários dias até que os sistemas mais importantes estivessem funcionando novamente e várias semanas até que os sistemas restantes pudessem ser usados.

Esse e outros incidentes semelhantes nos últimos anos fizeram com que legisladores em diversos países adotassem regras e regulamentações referentes à segurança cibernética. Essas normas têm como objetivo proteger as infraestruturas críticas de forma a assegurar a confiabilidade do fornecimento aos cidadãos e a estabilidade para os próprios países.

Na Alemanha, por exemplo, a "Gesetz zur Erhöhung der Sicherheit informationstechnischer Systeme" (Lei para Reforçar a Segurança dos Sistemas de Tecnologia da Informação = Lei de Segurança de TI) entrou em vigor em julho de 2015. Essa lei exige que os operadores de infraestruturas críticas (CRITIS) implementem determinadas medidas. "Operadores de infraestruturas críticas" também incluem empresas do setor de alimentos e bebidas, pois os ataques cibernéticos contra essa indústria não apenas interrompem a produção e causam danos financeiros, mas também podem representar riscos à saúde.

A prioridade máxima é prevenir erros na fabricação, manipulação da produção e evitar prejuízo à reputação da empresa. As medidas de segurança adequadas não são um luxo, são uma necessidade.

Legisladores regulamentam a segurança de TI no mundo todo

Desde julho de 2015, a Lei de Segurança de TI da Alemanha exige a comunicação de incidentes de segurança que afetam certas infraestruturas críticas. Com o tempo, os operadores CRITIS também serão obrigados a cumprir padrões mínimos de segurança cibernética. A implementação dessas normas é baseada principalmente na IEC 27001 e na IEC 62443. Os fabricantes de componentes de rede e automação e os operadores de instalações devem implementar medidas de segurança cibernética no estado atual da técnica. O termo "estado atual da técnica" é usado porque a experiência mostra que o desenvolvimento tecnológico progride mais rápido do que a legislação. O estado atual da técnica em qualquer ponto no tempo pode ser determinado com base em normas nacionais ou internacionais existentes, como DIN e IEC, ou com base nas melhores práticas para a indústria específica.

Estado atual da técnica de acordo com a IEC 62443

Os documentos IEC 62443 são organizados da seguinte forma:

- A IEC 62443-1 inclui terminologia, conceitos, casos de uso e modelos.
- A IEC 62443-2 tem como foco operadores de instalações e descreve atividades como a implementação de um sistema de gestão da segurança e gerenciamento de patches.
- A IEC 62443-3 descreve tecnologias de segurança para controladores e componentes de rede.
- A IEC 62443-4 tem como foco fabricantes e estabelece procedimentos para proteger o processo de desenvolvimento e outras atividades.

Essa divisão de informações mostra que a segurança cibernética é vista como um processo abrangente e que as normas de segurança devem ser cumpridas enquanto os componentes estiverem sob desenvolvimento.

A lei de modernização da segurança de alimentos Food Safety Modernization Act (FSMA) da FDA dos EUA inclui normas semelhantes que compreendem uma combinação de monitoramento, opções de intervenção e verificação de medidas de segurança cibernética, entre outros aspectos. Na Grã-Bretanha, a PAS 96:2017 regula medidas preventivas e de segurança contra ataques à indústria de alimentos e bebidas.

Basicamente, o que todas as leis e normas têm em comum é que são compostas por uma mistura de normas técnicas, obrigações de relatar incidentes e monitoramento da conformidade com as normas.

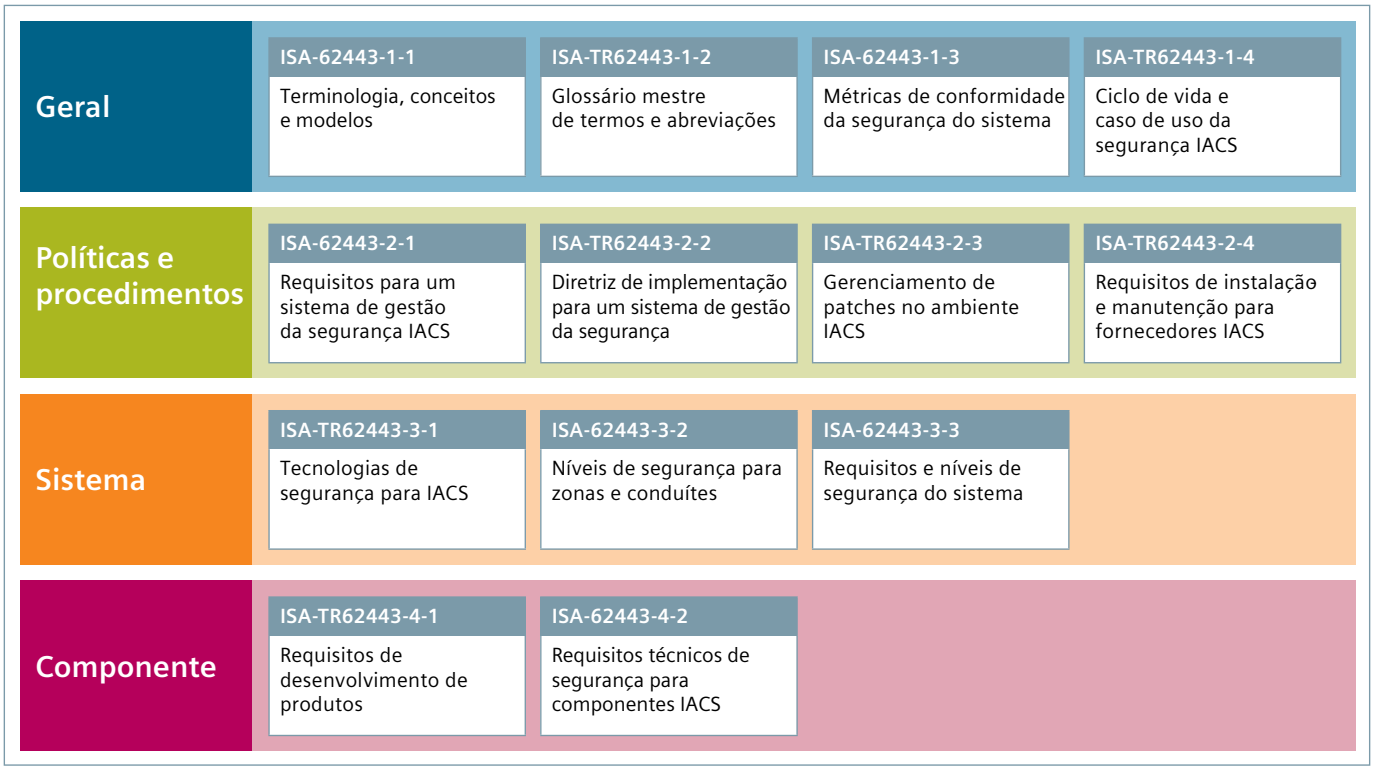

Fig. 1: Documentos da norma IEC 62443

Segurança Cibernética: Um processo contínuo

A proteção eficaz contra ataques cibernéticos não é atingida por uma implementação única de medidas de segurança: trata-se de um processo contínuo.

Após uma análise (avaliação) de riscos de um processo automatizado, medidas precisam ser implementadas para minimizar os riscos (implementação). Essas medidas devem ser monitoradas e deve haver uma verificação contínua da necessidade de revisão em função de uma mudança no cenário de ameaça (gestão). As medidas necessárias são tão variadas quanto os riscos avaliados. Com base no nível de automação, na tecnologia utilizada e na conectividade de TO (tecnologias operacionais) e TI (tecnologias da informação), os especialistas em segurança desenvolvem mecanismos de segurança sob medida para cada empresa e seus processos.

O operador da instalação sempre é responsável pela segurança de TI. Mesmo que as operações da instalação não sejam parcial ou inteiramente realizadas pela equipe própria da empresa em função da terceirização, o operador da instalação ainda é responsável. As ameaças decorrentes da terceirização também precisam ser avaliadas. Geralmente, recomenda-se que a equipe passe por treinamentos que aumentem sua consciência sobre ataques cibernéticos e que os qualifiquem a responder de maneira rápida e objetiva em caso de emergência.

Fig. 2: As três fases da segurança de TI/TO ou segurança industrial

Ameaças:
Alvos de ataque e tipos de invasores

Quais são os objetivos dos invasores que tentam superar as medidas de segurança? Os invasores geralmente se enquadram em quatro categorias.

Invasores não treinados (script kiddies) usam scripts finalizados da internet como um meio simples de atacar vulnerabilidades conhecidas "apenas porque conseguem".

Invasores treinados (hackers) lançam ataques mais complexos com o objetivo de obter e, por exemplo, extorquir dinheiro de resgate de dados criptografados.

A espionagem industrial geralmente é praticada por invasores que usam seu conhecimento especializado para roubar dados ou prejudicar a empresa. Nesse caso, (ex-)colaboradores visam uma empresa específica.

Tecnicamente, os ataques orientados pelo estado são os mais perigosos. Esses ataques geralmente tiram proveito de vulnerabilidades previamente desconhecidas com vários objetivos em mente: acesso a dados confidenciais, manipulação de dados, interrupção de processos de fabricação ou até mesmo a destruição de seções inteiras da instalação. Além do ganho financeiro, a motivação também pode ser desestabilizar um país – por exemplo, atacando o abastecimento de alimentos.

Ameaças

O Departamento Federal Alemão de Tecnologia da Informação (Bundesamt für Sicherheit in der Informationstechnik = BSI) identificou como os dez ataques mais frequentes em instalações industriais (Status: BSI-CS 029 | Versão 2.0 datada de 11 de julho de 2018):

1. Uso não autorizado de acesso de manutenção remota que possibilita o acesso externo a sistemas de controle industrial (ICSs) que muitas vezes são insuficientemente protegidos.
2. Ataques online por meio de TI do escritório, geralmente conectada à internet e que também pode estabelecer uma conexão com a rede IC.
3. Ataques a componentes padrão, como sistemas operacionais, servidores de aplicações ou bancos de dados que normalmente contêm erros e vulnerabilidades que os invasores podem explorar. Esses componentes também podem ser implementados em sistemas ICS, o que aumenta o risco.
4. Ataques (D)DoS em conexões de rede podem sobrecarregar os sistemas e interromper a funcionalidade da rede ICS ou do próprio ICS.
5. O erro humano e a sabotagem por perpetradores internos ou externos são uma grande ameaça. A negligência e o erro humano também ameaçam a confidencialidade e a disponibilidade.
6. O malware frequentemente é introduzido por meio de dispositivos de armazenamento removíveis ou componentes de TI móveis de colaboradores externos (exemplo: Stuxnet).
7. Os comandos de controle podem ser facilmente lidos e importados porque a maioria dos componentes de controle comunica-se por meio de protocolos de texto simples, o que significa que sua comunicação é desprotegida.
8. O acesso não autorizado aos componentes da rede é possível se membros internos – ou estranhos que superaram as medidas de segurança – acessarem os componentes usando métodos de autenticação e autorização inseguros.
9. Os invasores podem manipular os componentes da rede a fim de conduzir ataques do tipo man-in-the-middle ou facilitar o sniffing.
10. O potencial de falhas resultantes de influências ambientais extremas ou defeitos técnicos nunca pode ser completamente eliminado, mas o risco e os danos emergentes podem ser minimizados usando os devidos componentes e medidas de segurança.

Segurança Cibernética: Procedimento passo a passo

A lista de ameaças mostra que métodos muito diferentes podem ser usados para lançar ataques, e o processo precisa ser protegido contra essa ampla série de ameaças. A norma da indústria alemã e a IEC 62443 definem um processo de múltiplas etapas para a implementação da segurança cibernética.

1. A seleção de objetos serve para registrar e documentar todos os sistemas da instalação, incluindo subsistemas e um plano de rede.
2. As ameaças são derivadas de uma seleção de casos de uso: por exemplo, o fato de que um sistema pode ser atacado por meio de um acesso de manutenção remota.
3. A avaliação de ameaças identifica as ameaças para cada caso de uso: por exemplo, o acesso de manutenção remota pode ser usado por uma pessoa não autorizada.
4. A análise de riscos envolve a identificação de possíveis ameaças com base em uma matriz de riscos.

   Uma ameaça com alta probabilidade de ocorrência e alto potencial de dano aparece na área vermelha no canto superior direito da matriz (alto risco). Uma baixa extensão de dano e baixa probabilidade de ocorrência significa ter um risco baixo e aparece na área verde no canto esquerdo inferior. A norma BSI 200-3 fornece um detalhamento preciso da extensão do dano (grau de limitação da operação da instalação), probabilidade de ocorrência e risco.
5. Um processo para determinar as medidas necessárias define opções concretas que são descritas detalhadamente na próxima seção.
6. A implementação de medidas inclui a programação e o planejamento organizacional da implementação. Ela também inclui definir responsabilidades e alocar claramente o orçamento para a implementação de medidas.
7. Para a auditoria, as medidas devem ser verificadas, a documentação da instalação deve estar completa e as listas de verificação devem ser preenchidas. A eficácia das medidas deve ser verificada em intervalos regulares. Caso falhas sejam identificadas – por exemplo, de riscos alterados ou novos tipos de malware – todo o processo deve ser reiniciado, começando com a avaliação da ameaça.

Conceito de segurança

Uma vez que as ameaças diferem em termos de natureza, podendo ser originadas interna ou externamente, e diferentes invasores têm diferentes níveis de especialização, é importante criar um conceito de segurança de múltiplas camadas para fornecer um processo que proporcione a melhor proteção possível. Por exemplo, mesmo que o firewall tenha sido violado porque o invasor entrou fisicamente na instalação, mecanismos de segurança adicionais precisam proteger os dispositivos terminais.

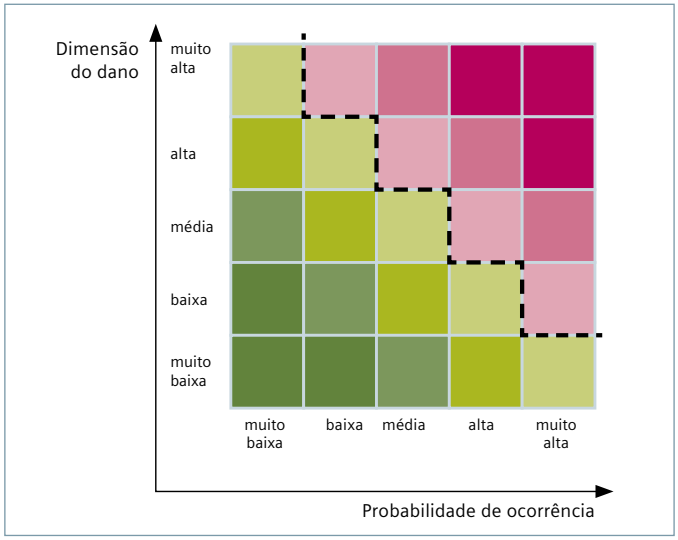

Fig.3: Matriz de riscos com base na norma BSI 200-3

Fig. 4: Conceito de segurança de "Defesa em Profundidade"

A figura mostra um conceito de segurança de múltiplas camadas que define a segurança da instalação, a segurança da rede e a integridade do sistema como as três camadas essenciais da segurança eficaz.

Medidas de segurança da instalação

As medidas organizacionais incluem todas as medidas para proteger fisicamente a instalação. Além da proteção contra invasões, também deve haver procedimentos para proteger a instalação contra influências ambientais.

Ameaças

- Arrombamento/vandalismo
- Acesso não autorizado
- Inundação
- Incêndio
- Fumaça/poeira/gases corrosivos
- Relâmpago/sobretensão/EMC

Medidas organizacionais

Dependendo das ameaças específicas, medidas apropriadas devem ser adotadas para proteger a instalação. É necessário ter atenção especial com estações externas (por exemplo, armazéns) que geralmente estão desocupadas e são monitoradas remotamente a partir do centro de controle. As estações externas devem ser protegidas contra arrombamentos e as portas e janelas devem estar devidamente protegidas.

Os contatos de portas/janelas podem notificar o controlador caso sejam abertas e o controlador pode notificar o centro de controle. Uma câmera IP pode ajudar a detectar invasores e monitorar o prédio.

Diferentes áreas de produção também devem ser fisicamente separadas por meio de um controle de acesso diferenciado. Como exemplo, os componentes críticos precisam ser protegidos em um gabinete de controle trancado (consulte também a página 13).

As diretrizes para medidas de proteção contra acesso físico também determinam as medidas de segurança cibernética necessárias e a força dessas medidas. Por exemplo, em áreas que são acessadas somente por pessoas autorizadas selecionadas, as interfaces de acesso à rede e os sistemas de automação não precisam ser protegidos com tanta segurança como seriam em áreas acessíveis ao público.

Com a certificação de acordo com a IEC 27001, as empresas podem reduzir os riscos de segurança da informação, cumprir em maior grau os regulamentos e requisitos de segurança relevantes e promover uma cultura de segurança interna.

Medidas de segurança da rede

A rede deve ser estruturada para resistir ao maior grau possível de ataques em potencial, ao mesmo tempo que leva em consideração as opções de acesso, disponibilidade e proteção.

Opções de acesso

Como regra, as redes são sistemas abertos com conexão à internet. Para a maioria dos operadores de instalações, o acesso externo para fins de manutenção, diagnóstico, otimização, patches, atualizações e outras atividades tornou-se essencial.

Disponibilidade

O processo automatizado – que é controlado, por exemplo, por meio da rede usando a comunicação PROFINET – deve ser executado independentemente de interrupções de linhas individuais. Os sistemas de monitoramento no centro de controle devem seguir sendo capazes de monitorar o processo mesmo quando os roteadores individuais falharem.

Proteção

O processo deve ser protegido contra todos os potenciais riscos que podem ameaçar a rede, incluindo acesso não autorizado, malware e ataques (D)DoS. Todos os tipos de comunicação, exceto o acesso autorizado e permitido, devem ser bloqueados com as devidas medidas.

A IEC 62443 requer os seguintes elementos para proteção da rede:

- Segmentação da arquitetura da rede
- Isolamento ou segmentação de componentes de alto risco
- Bloqueio de comunicação desnecessária
- Acesso via firewalls

Segmentação da rede

A segmentação da rede usando firewalls proporciona proteção contra ataques da rede. A rede é dividida em grupos funcionais – por exemplo, redes de produção, rede da instalação e rede do escritório – e o acesso é controlado com precisão por firewalls.

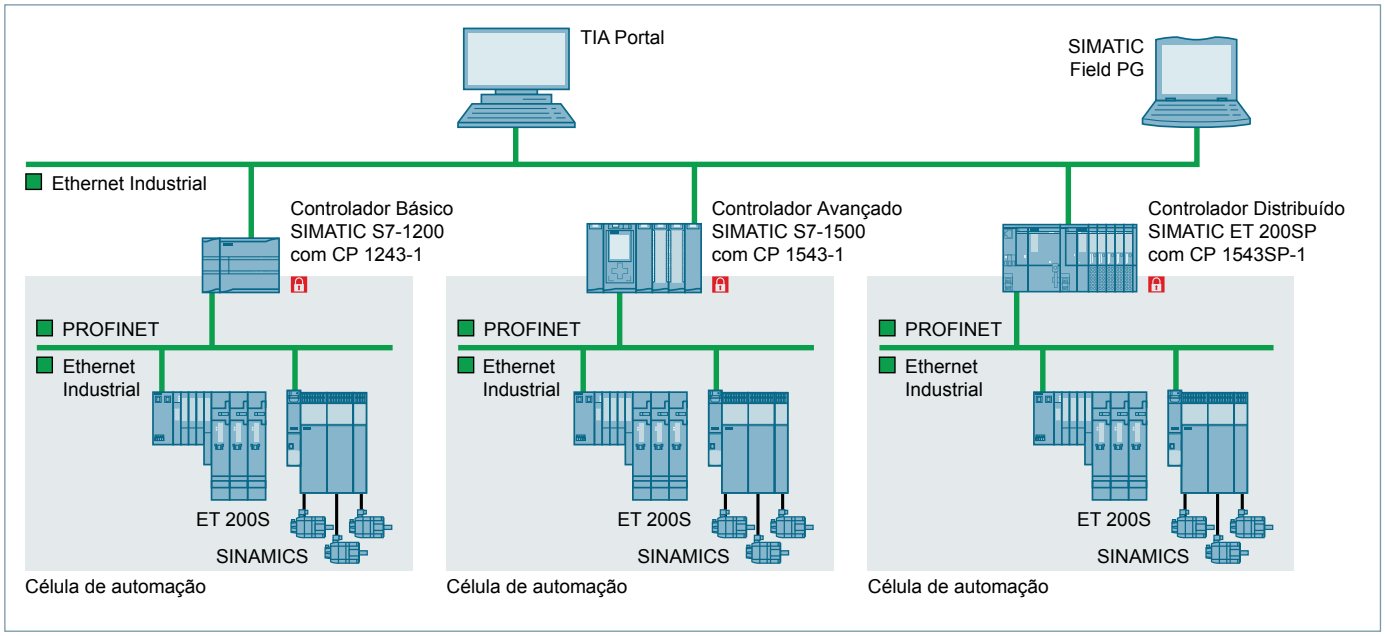

Fig. 5: Segmentação da rede de acordo com a IEC 62443-2-1

Zona Desmilitarizada (DMZ)

A Figura 5 mostra uma configuração de rede recomendada na IEC 62443-2. As células de automação na parte inferior são combinadas como unidades funcionais e cada uma é separada da rede no nível da instalação por um firewall. A rede da instalação no topo contém todos os dispositivos de nível superior importantes para a operação da instalação, como o centro de controle e os servidores. A interface entre a rede da instalação e a rede do escritório é novamente separada por um firewall. Uma ou mais zonas desmilitarizadas (DMZs) podem ser configuradas aqui. Em uma DMZ, os dispositivos das redes de nível superior e inferior não se comunicam entre si diretamente. Em vez disso, eles se comunicam por meio de um servidor que, por exemplo, recupera o status da instalação das células de automação e disponibiliza essas informações para a rede de nível superior. A rede do escritório também é protegida da internet por um ou mais firewalls.

Nesse exemplo, a configuração cria três barreiras de defesa para as células de automação que controlam o processo. A rede do escritório, que é afetada em potencial pela introdução de malware mais frequente (por exemplo, pen drives), é separada da célula de automação por dois firewalls. Quanto mais próximo da célula de automação um determinado colaborador trabalhar, mais importante será que ele tenha conhecimento dos aspectos de segurança cibernética.

Acesso remoto e estações externas distribuídas

A conexão de estações externas distribuídas apresenta um desafio especial. Embora essas estações devam conseguir funcionar independentemente, também deve ser possível monitorá-las a partir do centro de controle. A rede de uma estação externa deve ser protegida e o acesso deve ser seguro, mesmo em caso de conexão por uma rede separada ou pela própria conexão da empresa. A estação externa pode ser conectada por cabo (como ADSL ou SHDSL) ou conexão de rádio (por exemplo, LTE ou UMTS). O modem deve conter um firewall e ter compatibilidade com a VPN.

Para aumentar a segurança, a conexão VPN pode ser configurada para acesso remoto de acordo com a IEC 62443 de modo que o túnel seja estabelecido somente quando um técnico no local ativa a VPN no módulo.

Conexões sem fio via WLAN

Uma atenção especial deve ser prestada à transmissão sem fio via WLAN ou outras tecnologias. No caso da comunicação com fio, um invasor deve ter acesso físico aos cabos ou componentes de rede a fim de ler dados ou adulterar o tráfego de dados. Com a comunicação sem fio, as ondas de rádio se espalham por uma área maior, tornando o ataque mais fácil.

Caso uma WLAN seja necessária na célula de automação, uma WLAN separada deve ser configurada para automação. A WLAN do escritório deve ser operada por meio de diferentes pontos de acesso a fim de manter a segmentação da rede.

Medidas organizacionais para uma WLAN

O ponto de acesso deve ser instalado de modo que seja inacessível ou protegido em um gabinete de controle fechado e as antenas WLAN devem ser instaladas remotamente. Isso impedirá que os invasores acessem fisicamente o ponto de acesso. A frequência da WLAN também precisa ser escolhida com cuidado, pois outras aplicações que usam a mesma frequência podem interferir na transmissão de maneira semelhante aos jammers ou mesmo interrompê-la completamente.

Mecanismos técnicos de segurança para uma WLAN

A criptografia WPA2 é o estado atual da técnica. Os métodos de criptografia mais antigos (WEP e WPA) não devem mais ser usados porque não são seguros e são fáceis de descriptografar. A senha padrão e o SSID precisam ser alterados, e o SSID deve ser oculto.

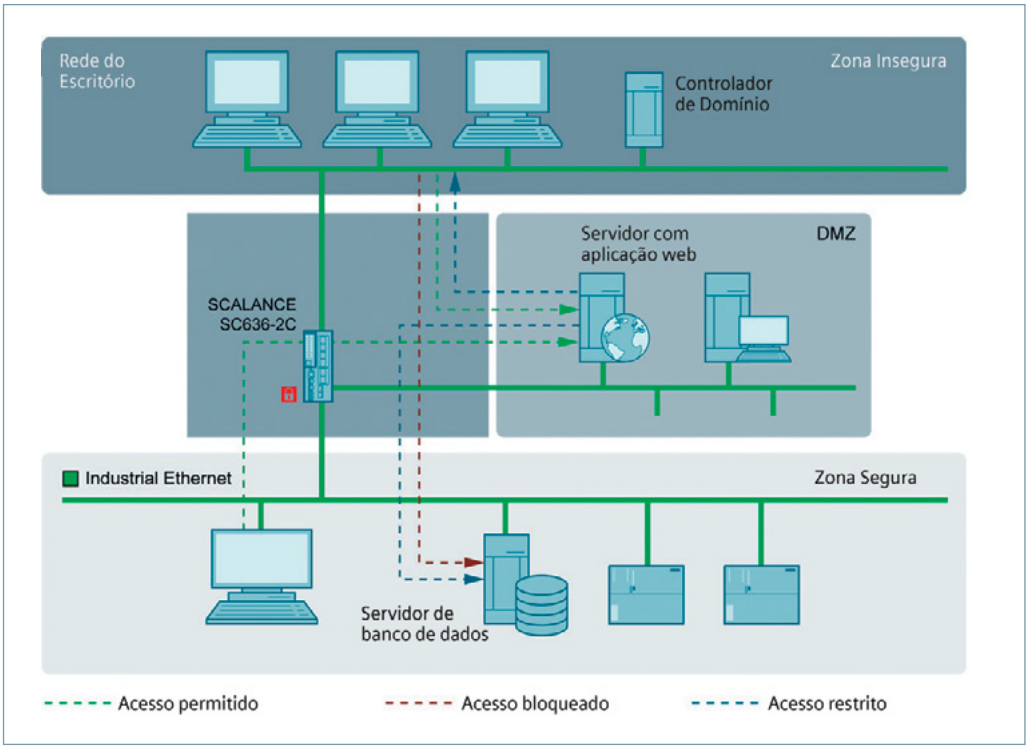

Fig. 6: Conexão de um PC de serviço local por meio de uma porta DMZ no SCALANCE S615

Requisitos gerais para elementos de rede

O padrão internacional para configuração e gerenciamento seguros de componentes da rede, de acordo com a norma IEC 62443, recomenda os seguintes recursos e mecanismos de segurança para configurar e proteger dispositivos.

Proteção de acesso e gerenciamento de contas

Para proteger os componentes da rede contra acesso não autorizado, deve ser possível gerenciar e, quando necessário, bloquear contas às quais o acesso foi habilitado. Deve haver os seguintes recursos:

- Configurar opções de acesso
- Identificar usuários/tornar os usuários identificáveis por meio de contas
- Configurar/alterar/encerrar contas por meio de um gerente central
- Contas de documentos e usuários de contas
- Excluir ou bloquear contas não utilizadas
- Verificar direitos de acesso regularmente
- Alterar senhas padrão

Os requisitos de proteção de acesso podem ser implementados por meio de componentes de gerenciamento de usuários (UMCs). Com os UMCs, diferentes contas de usuário são criadas em um servidor central conhecido como servidor em anel UMC. Os projetos do TIA Portal podem utilizar esses usuários e eles podem receber direitos de acesso aos componentes e participantes da rede.

Controle de acesso: autenticação

Quando um componente é acessado, deve ser possível identificar o usuário que está acessando. A autenticação deve fornecer os seguintes mecanismos:

- Acesso possível somente quando o usuário tiver sido autenticado (ou houver controle de acesso suficiente)
- Fortes mecanismos de segurança para acesso administrativo
- Registro de todos os acessos a sistemas críticos
- Identificação de todos os usuários de acesso remoto
- Diretrizes para acesso remoto e logout automático após um período de inatividade
- Acesso remoto bloqueado após repetidos logins com falha
- Nova autenticação durante o acesso remoto após um período de inatividade
- Um mecanismo de autenticação também deve ser configurado para comunicação tarefa a tarefa

Esses requisitos referem-se a diferentes sistemas e, portanto, devem ser levados em consideração para toda a instalação. Para o acesso remoto, por exemplo, os requisitos podem ser cumpridos pelo SINEMA Remote Connect, pois, entre outras coisas, o logout automático após a inatividade e o bloqueio de um IP após várias tentativas de login sem sucesso já estão implementados e os acessos remotos são sempre registrados. No TIA Portal, os usuários podem ter acesso ao projeto e acesso separado à configuração de segurança. Como a configuração de segurança requer seus próprios direitos de acesso, o requisito de segurança adicional para acesso administrativo também é atendido.

Controle de acesso: Autorização

Autorização significa conceder direitos específicos a usuários previamente autenticados: por exemplo, acesso a um componente. A IEC 62443 menciona os seguintes pontos em relação à autorização:

- Método lógico ou físico para permissão de acesso
- Acesso baseado em função ao sistema ou às informações
- O direito de acesso a recursos de segurança deve ser um direito separado
- Múltiplos níveis de acesso devem ser configurados para sistemas críticos

Gerenciamento de rede

O SNMP, que agora é compatível com todas as interfaces de rede, pode ser usado para o gerenciamento de rede. Em conjunto com o servidor SINEMA, o SNMP pode ser usado para monitorar a rede e as seções da instalação conectadas via VPN. Isso possibilita que todas as seções da rede sejam gerenciadas e as falhas sejam identificadas mais rapidamente.

Plano da rede

Um plano físico da rede – uma visão topológica – é necessário para documentar a instalação e mostrar como os participantes estão interconectados. Esse plano da rede deve indicar endereços (IP e MAC), conexões de porta e locais de instalação. Ele pode ser impresso no TIA Portal ou a ferramenta de planejamento de rede SINETPLAN pode ser usada.

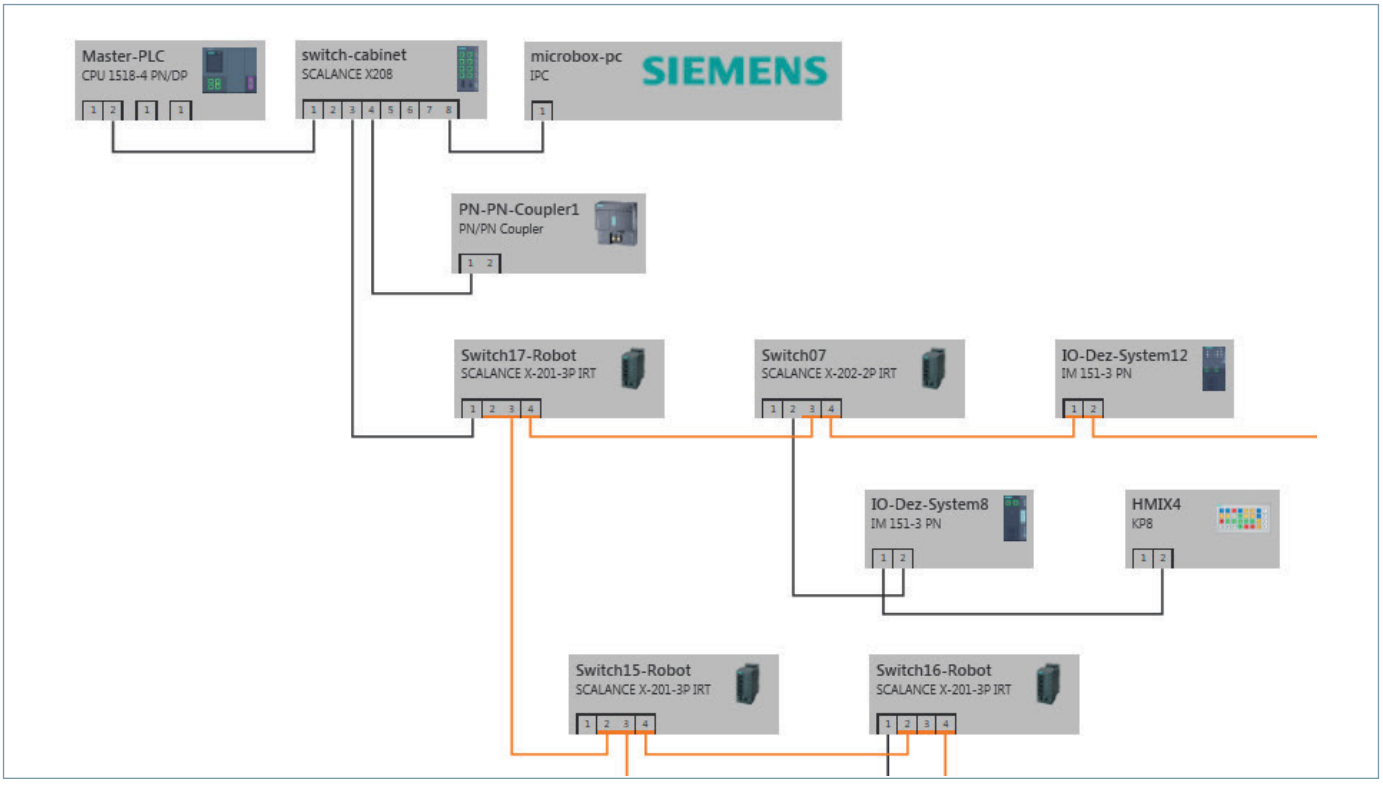

Fig. 7: Rede topológica no SINETPLAN

Medidas de integridade do sistema

Integridade do sistema significa que a autenticidade dos dados e programas dentro de um sistema são garantidas. Ninguém tem permissão para alterar o programa, adulterar dados (seja no canal de comunicação ou no sistema), copiar o programa ou dados sem autorização.
A especialização no controle de processos também deve ser protegida.

Acesso ao programa
Os controladores programáveis (PLCs) também fazem parte da segurança cibernética, por isso o acesso ao projeto e aos escritórios deve ser protegido. O projeto geralmente pode ser protegido usando o log do Windows. A partir do TIA Portal V15, todo o projeto pode ser criptografado. Isso significa que o projeto somente pode ser aberto com um nome de usuário adicional e uma senha adicional, o que garante a segurança quando várias pessoas trabalham no mesmo projeto simultaneamente.

Proteção contra acesso à CPU
Diferentes senhas podem ser configuradas com base nos diferentes níveis de acesso à CPU, de modo que apenas membros qualificados da equipe tenham pleno acesso.

Servidores web
Cada vez mais soluções de controle estão usando o acesso por meio de servidores web, que muitas vezes também são usados para acesso remoto. Nesse caso, os servidores web também devem estar completamente protegidos.

O HTTPS é a versão segura do HTTP e é a escolha preferida. A autenticação e a autorização exigidas pelo padrão da indústria podem ser obtidas configurando diferentes usuários e níveis de acesso.

Comunicação segura
Caso o controlador se comunique fora de sua célula segura, essa comunicação deve ser criptografada. O estado atual da técnica é a criptografia TLS, que pode ser usada no S7-1500 via OPC UA ou uma conexão TCP.

Outra opção de criptografia é usar firewalls integrados para configurar uma conexão VPN. O túnel VPN é estabelecido entre os firewalls e a comunicação entre as células de automação é transmitida pela rede de nível superior criptografada e é descriptografada pela rede de destino.

Medidas de segurança em PCs industriais
Os PCs usados no ambiente industrial (IPCs) exigem medidas especiais por estarem diretamente expostos a várias ameaças – incluindo dispositivos de armazenamento infectados – enquanto os dispositivos USB não podem ser conectados diretamente a um controlador. As medidas a seguir servem para proteger um IPC contra ataques de segurança cibernética.

Contas de usuário
É recomendável configurar contas de administrador e usuário. Somente o administrador está autorizado a fazer alterações nas configurações de segurança ou a (des)instalar o software.

O usuário padrão não consegue executar essas funções, o que impede a instalação de malware durante operações normais.

Configuração de diretrizes
Com o auxílio do Microsoft Management Console, diretrizes podem ser estabelecidas para a utilização de dispositivos de armazenamento, controle do sistema, entre outros. Um documento que descreve essas diretrizes e como elas podem ser estabelecidas está disponível online em: **https://support.industry.siemens.com/cs/ww/en/ view/109475014**

Enhanced Write Filter (EWF)
Esse recurso está disponível em IPCs SIMATIC: ele protege uma porta do sistema de arquivos contra a modificação de dados, redirecionando o acesso de gravação para a memória RAM. Quando o IPC é reiniciado, o sistema de arquivos retorna ao seu estado original. O malware introduzido não está mais presente após uma reinicialização.

Firewall
Os firewalls padrão (firewalls do Windows) já fornecem uma proteção básica importante. Eles sempre devem permanecer ativados. Usando regras apropriadas, os firewalls precisam ser configurados de modo que somente os dados do usuário possam ser comunicados e todas as outras comunicações sejam bloqueadas.

Proteção contra vírus
Um software antivírus pode detectar vírus e malware. Na Siemens, usamos uma instalação McAfee para nossa automação. Um servidor de gerenciamento lida com os clientes de antivírus nos sistemas de PC e fornece as assinaturas de vírus mais recentes. O servidor de gerenciamento também pode notificar a equipe de serviços por meio de alarmes via e-mail.

Produtos certificados pela IEC 62443
Os controladores, PCs e outros sistemas selecionados para uso devem conter mecanismos de segurança e ter sido testados quanto a vulnerabilidades. Esses testes são padronizados: por exemplo, um Certificado Achilles indica que o sistema foi submetido a testes de carga e vulnerabilidade. Os fabricantes também podem realizar o desenvolvimento seguro de produtos para assegurar um alto nível de qualidade. O processo de desenvolvimento da Siemens foi testado e aprovado conforme a IEC 62443-4: **https://www.siemens.com/press/PR2016080373DFEN**

Medidas para a equipe

As melhores medidas de segurança técnicas e organizacionais são inúteis quando os colaboradores da empresa são negligentes. É por isso que cursos de treinamento e claras definições das áreas de responsabilidade são partes integrais da segurança cibernética. A IEC 62443 recomenda que novos membros da equipe passem por triagem para determinar sua confiabilidade e avaliar se podem cumprir suas responsabilidades. A confiabilidade da equipe existente também deve ser determinada. Membros de equipes externas também podem participar dos treinamentos, mas devem estar sempre acompanhados e supervisionados por colaboradores treinados da própria empresa.

Responsabilidade

A norma da indústria exige que os operadores de infraestruturas críticas (CRITIS) designem a organização UP KRITIS como seu contato de segurança cibernética. Geralmente, recomenda-se que um indivíduo ou grupo seja responsável pela segurança cibernética dentro da empresa.

Treinamento

Cursos regulares de treinamento devem ser oferecidos abordando a devida administração dos sistemas instalados, dispositivos de armazenamento removíveis e software; também deve haver um curso de treinamento sobre como responder a incidentes e todas as possíveis outras ameaças. A norma da indústria exige expressamente que os administradores sejam treinados sobre o manuseio correto dos componentes da rede para assegurar que as configurações sejam devidamente realizadas.

Plano de emergência e recuperação

A norma da indústria exige um conceito para lidar com uma emergência quando uma ameaça surge e o processo é interrompido. Esse conceito também é conhecido como gerenciamento da continuidade dos negócios. As seguintes questões precisam ser respondidas:

- Qual é o período de inatividade máximo aceitável?
- Como o processo pode continuar a funcionar independentemente do sistema de controle/escritório?
- Quão bem outras seções da instalação podem compensar o fornecimento?
- Como o sistema afetado será revisado?
  - Por meio de redundâncias
  - Por meio de backup
- Como a recorrência dessa falha será evitada?
  - Relatórios
  - Otimização

Siemens ProductCERT

A Siemens tem uma equipe de especialistas em segurança que atua como ponto de contato para clientes e seus especialistas em segurança quando uma vulnerabilidade de segurança é identificada. Essa equipe – conhecida como ProductCERT (Product Computer Emergency Response Team) – avalia e analisa imediatamente as vulnerabilidades de segurança relatadas.

Informações de Segurança da Siemens

A Siemens ProductCERT investiga todos os problemas relatados e publica Informações de Segurança sobre vulnerabilidades validadas que envolvem diretamente os produtos da Siemens e exigem uma atualização de software, melhoria de software ou outra ação por parte do operador da instalação. Usufrua dessa fonte de informações para avaliar os efeitos de uma vulnerabilidade na segurança. A Siemens lida abertamente com suas próprias vulnerabilidades para que você possa responder antes que afetem você. Mantenha-se atualizado assinando nossos feeds RSS: **https://new.siemens.com/global/en/products/services/cert.html**

Panorama geral

A segurança industrial abrangente exige que todos os níveis de proteção sejam levados em consideração. As medidas de segurança devem ser tão variadas quanto os possíveis riscos. Uma abordagem de ponta a ponta e várias linhas de defesa podem proteger instalações industriais de maneira confiável. Para simplificar essa complicada questão para a indústria, a Siemens oferece um portfólio de soluções customizadas voltado especificamente para a segurança de instalações industriais e tecnologias operacionais.

A figura abaixo representa uma arquitetura de rede típica para uma fábrica de bebidas. Ela mostra os níveis nos quais as medidas de segurança descritas neste documento foram implementadas de acordo com as recomendações da norma IEC-62443.

Por que a Siemens?

A Siemens oferece uma base confiável para soluções de automação inovadoras e seguras.

Na Siemens:

- Entendemos a digitalização;
- Entendemos a indústria de alimentos e bebidas;
- Entendemos a comunicação industrial;
- Entendemos a segurança industrial; e
- Oferecemos processos e produtos de segurança comprovados e certificados

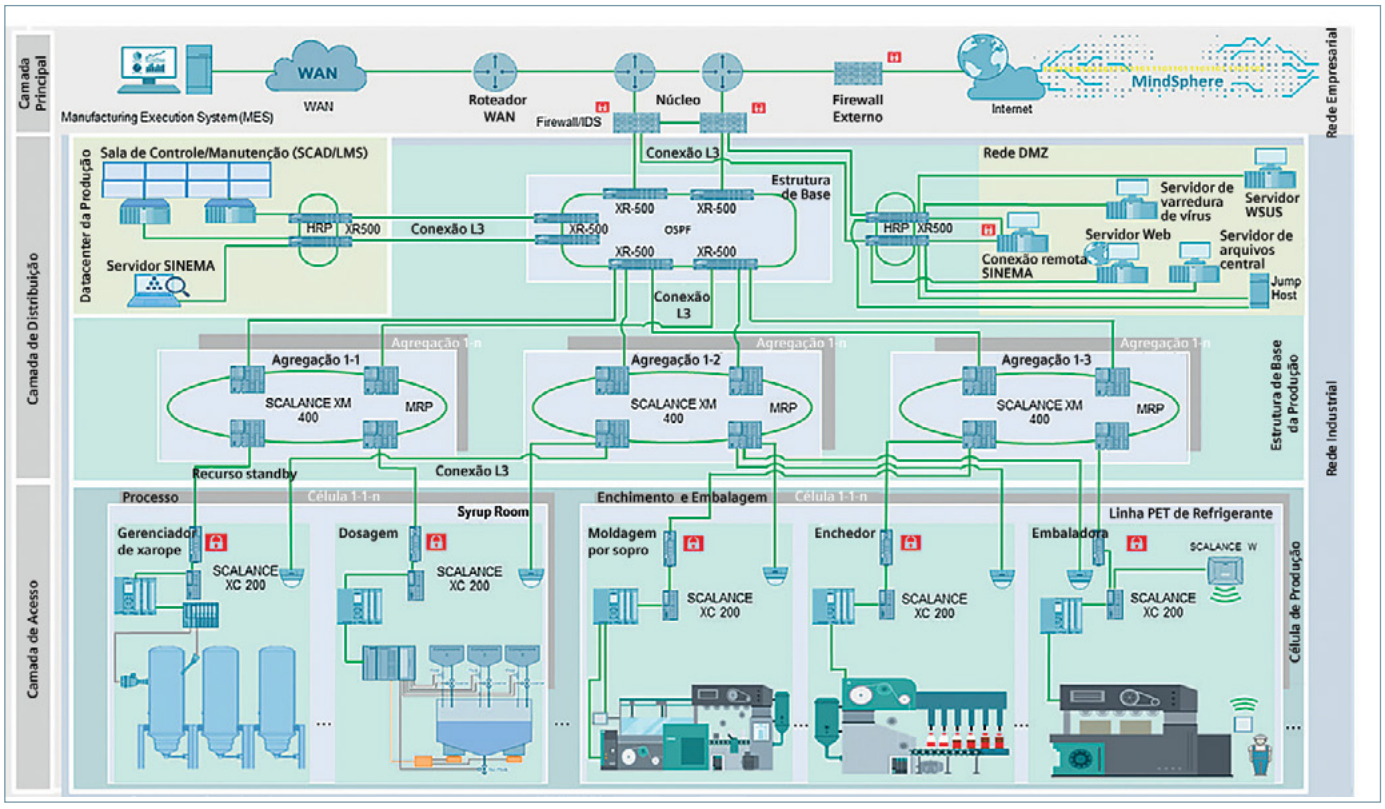

Fig. 8: Arquitetura de rede de uma fábrica de bebidas

Termos e abreviações

Autenticação
A detecção e identificação de um usuário ou (no caso de instalações em rede) outro sistema.

Autorização
O direito de acesso a um sistema ou uma seção (software) de um sistema ou programa.

Segurança Cibernética
Todas as medidas técnicas para proteger uma instalação, incluindo proteção da rede, fortalecimento do sistema e monitoramento de incidentes.

Processo
O processo de produção real – por exemplo, produção de queijo ou envase – independentemente de ser um processo discreto ou contínuo.

Rede privada virtual (VPN)
Uma VPN fornece conexão criptografada entre usuários de VPN. Isso também é conhecido como grupo VPN. Uma VPN se assemelha a um túnel no qual o tráfego de dados pode ser enviado a partir de qualquer direção. No túnel, o tráfego de dados é transmitido de forma criptografada e no fim do túnel – ou seja, no outro dispositivo VPN – é entregue de forma descriptografada. Os dispositivos terminais não precisam ter suporte para criptografia porque a criptografia é realizada pelos dispositivos VPN.

Publicado por
Siemens Infraestrutura e Indústria Ltda.

Av. Mutinga, 3800
05110-902 - São Paulo - SP
www.siemens.com.br