Livro Branco da DITTA sobre segurança cibernética:

Práticas recomendadas para compartilhar informações de segurança cibernética

A tradução e divulgação deste documento pela ABIMED - Associação Brasileira da Indústria de Tecnologia para Saúde, foi previamente autorizada pela DITTA - GLOBAL DIAGNOSTIC IMAGING, HEALTHCARE ICT, AND RADIATION THERAPY TRADE ASSOCIATION, detentora de todos os direitos de seu conteúdo original em inglês e disponível em: https://www.globalditta.org/media-centre/positions-papers/article/white-paper-best-practices-for-sharing-cybersecurity-information.html

Resumo executivo

Propósito

Práticas recomendadas para compartilhar informações de segurança cibernética identifica as melhores práticas e diretrizes do setor que os fabricantes de tecnologia médica podem considerar ao fornecer informações de segurança cibernética a seus clientes. Essas informações destinam-se a ajudar os clientes a gerenciar efetivamente suas expectativas de segurança cibernética à medida que usam o equipamento no contexto de seus respectivos mercados. O documento também fornece sugestões de como os fabricantes podem trabalhar com seus clientes para melhorar o nível de segurança cibernética por meio das melhores práticas e diretrizes do setor. As diretrizes descritas neste documento se concentram em pessoas, processos e produtos.

Estrutura do documento

Para cada princípio fundamental, são fornecidas as seguintes informações:

a. Identificação de ameaças e análise de suas implicações;
b. Documentos de referência adicionais;
c. Recomendações que os fabricantes de tecnologia médica podem considerar ao fornecer informações de segurança cibernética a seus clientes e:
d. Sugestões de como os fabricantes podem trabalhar com seus clientes para melhorar o nível de segurança cibernética.

RESTRITO

CONTEÚDO

Resumo Executivo 2

Introdução 5

Escopo do Documento 5

Definições 5

Educação 7

Avaliação de risco 7

Comunicação eficaz de informações de segurança cibernética aos clientes 8

Princípios fundamentais 9

1. Segmentação de redes 9

Identificação de ameaças e análise de suas implicações 9

Documentos de referência 10

Recomendações dos fabricantes 10

2. Entendimento dos tipos de dados e fluxos 12

Identificação de ameaças e análise de suas implicações 12

Documentos de referência 12

Recomendação do fabricante 13

3. Monitoramento de Dispositivos e Sistemas 13

Identificação de ameaças e análise de suas implicações 14

Documentos de referência 14

Recomendação dos fabricantes 14

4. Gerenciamento de usuários 15

Identificação de ameaças e análise de suas implicações 15

Documentos de referência 16

Recomendação do fabricante 16

RESTRITO

5. Fortalecimento dos dispositivos ..... **Erro! Indicador não definido.**

Identificação de ameaças e análise de suas implicações 18

Documentos de referência 19

Recomendações do fabricante 19

6. Atualizando dispositivos 20

7. Fornecimento de um Plano de Recuperação/Escalonamento de Processos 22

Identificação de ameaças e análise de suas implicações 22

Documentos de referência 22

Recomendação dos fabricantes 23

Tabela

Tabela 1—Exemplo de uma configuração de rede necessária ..... **Erro! Indicador não definido.**

RESTRITO

Introdução

Este documento identifica as melhores práticas e diretrizes do setor que os fabricantes de tecnologia médica podem considerar ao fornecer informações de segurança cibernética a seus clientes. Essas informações destinam-se a ajudar os clientes a gerenciar efetivamente suas expectativas de segurança cibernética à medida que usam o equipamento no contexto de seus respectivos mercados. O documento também fornece sugestões de como os fabricantes podem trabalhar com seus clientes para melhorar o nível de segurança cibernética por meio das melhores práticas e diretrizes do setor. As diretrizes descritas neste documento se concentram em pessoas, processos e produtos.

Escopo do Documento

O documento fornece orientação sobre os tipos e níveis de informações que os fabricantes podem fornecer a seus clientes para gerenciar efetivamente suas expectativas de segurança cibernética. Este documento também aborda o aumento do nível de segurança cibernética de um cliente seguindo sete princípios fundamentais:

a. Segmentação de redes,
b. Entendimento dos tipos e fluxos de dados,
c. Dispositivos e sistemas de monitoramento,
d. Gerenciamento de usuários,
e. Fortalecimento de dispositivo
f. Atualização de dispositivos e
g. Fornecendo um plano de recuperação/processo de escalonamento.

Este documento não pretende ser exaustivo. É um conjunto representativo de melhores práticas que os fabricantes de tecnologia médica podem considerar ao fornecer informações de segurança cibernética a seus clientes à medida que utilizam equipamentos fabricados no contexto de seus respectivos mercados. Este documento também não se destina a descrever as práticas recomendadas de segurança (como controle de acesso e criptografia de dados) para os dispositivos fabricados em si.

Definições

Diretório Ativo (Active Directory): O serviço de diretório de marca registrada da Microsoft, que é um sistema centralizado e padronizado que automatiza o gerenciamento de rede de dados de usuários, segurança e recursos distribuídos e permite a interoperação com outros diretórios.

Chaves assimétricas (Asymmetric Keys): Um algoritmo de criptografia que usa um par de chaves pública/privada para criptografia e descriptografia.

Higiene Cibernética (Cyber Hygiene): Uma referência às práticas e etapas que os usuários de computadores e outros dispositivos devem seguir para manter a integridade do sistema e melhorar a segurança online.

Zona Desmilitarizada (DMZ) (Demilitarized Zone): Uma sub-rede física ou lógica que contém e expõe os serviços externos de uma organização a uma rede não confiável, geralmente uma rede maior, como a Internet.

RESTRITO

Servidor de nomes de domínio (DNS) (Domain Name Server): O sistema que traduz automaticamente os endereços da Internet para os endereços numéricos que os computadores usam.

Autoridade de Números Atribuídos pela Internet (IANA) (Internet Assigned Numbers Authority): Uma corporação americana privada sem fins lucrativos que supervisiona a coordenação global da zona raiz do DNS, atribui endereços IP e outros recursos de protocolo da Internet.

ICS-CERT: Um componente do Centro Nacional de Integração de Comunicações e Segurança Cibernética (NCCIC) do Departamento de Segurança Interna dos EUA (DHS) que coordena incidentes de segurança envolvendo sistemas de controle, facilita o compartilhamento de informações e fornece programas de treinamento on-line. (https://ics-cert.us-cert.gov/)

Internet das Coisas (IoT) (Internet of Things): A IoT refere-se à rede cada vez maior de objetos físicos que possuem conectividade com a Internet e a comunicação que ocorre entre esses objetos e outros dispositivos e sistemas habilitados para a Internet.

Protocolo de Internet (IP) (Internet Protocol): Um protocolo de comunicação para computadores conectados a uma rede, especialmente a Internet, especificando o formato de endereços e unidades de dados transmitidos.

Protocolo de acesso ao diretório leve (LDAP) (Lightweight Directory Access Protocol): Um protocolo de aplicativo para consultar e modificar itens em provedores de serviços de diretório, como o Active Directory.

Provedor de Serviços de Segurança Gerenciada (MSSP) (Managed Security Service Provider): Uma organização que fornece monitoramento e gerenciamento terceirizados de dispositivos e sistemas de segurança.

Senha (Passphrase): Uma sequência de palavras ou outro texto usado para controlar o acesso a um sistema de computador, programa ou dados.

Serviço de usuário de discagem de autenticação remota (RADIUS) (Remote Authentication Dial-In User Service): Um protocolo de rede que fornece autenticação centralizada, autorização e gerenciamento de contabilidade para usuários que se conectam e usam um serviço de rede.

(SAFECODE) : O Software Assurance Forum for Excellence in Code (SAFECODE) é uma organização sem fins lucrativos dedicada exclusivamente a aumentar a confiança em produtos e serviços de tecnologia da informação e comunicação por meio do avanço de métodos comprovados de garantia de software. (https://safecode.org/)

Informações de segurança e gerenciamento de eventos (SIEM) (Security Information and Event Management): Uma abordagem de gerenciamento de segurança para fornecer uma visão holística das informações relacionadas à segurança que são coletadas, correlacionadas e analisadas.

Acordo de Nível de Serviço (SLA) (Service Level Agreement): Um contrato entre um fabricante e um cliente que documenta e define os serviços que o fabricante é obrigado a fornecer.

Contrato de Manutenção de Software (Software Maintenance Agreement): Um contrato que fornece suporte contínuo ao software após sua entrega.

RESTRITO

Chave simétrica (Symmetric Key): Um algoritmo de criptografia que usa as mesmas chaves criptográficas para criptografia e descriptografia.

O Instituto SANS (The SANS Institute): Uma empresa privada com fins lucrativos especializada em segurança da informação, treinamento em segurança cibernética e venda de certificados. (https://www.sans.org/)

Barramento serial universal (USB) (Universal Serial Bus): Um padrão do setor que define cabos, conectores e protocolos de comunicação para conexão, comunicação e fonte de alimentação entre computadores e dispositivos.

Lista de permissões (Whitelisting): Uma abordagem de controle de acesso baseada em uma lista de entidades aceitáveis que têm permissão de acesso a um sistema ou rede bloqueando todo o resto.

Educação

A educação do cliente é um dos aspectos com menos investimento e mais subestimados da segurança cibernética. Um componente-chave da implementação da higiene cibernética é obter conhecimento dos fundamentos da segurança cibernética e aumentar a conscientização sobre como praticá-la. Muitos recursos educacionais e de treinamento podem ajudar nessa área, incluindo o Instituto SANS (https://www.sans.org/), ICS-CERT (https://us-cert.cisa.gov) e o SAFECODE (**Erro! A referência de hiperlink não é válida.**https://safecode.org/).

Os objetivos de treinamento devem ser estabelecidos para os clientes, incluindo a garantia de que o pessoal seja capaz de realizar as seguintes atividades:

a. Reconhecer e relatar suspeitas de incidentes cibernéticos à autoridade competente,
b. Entender como lidar e proteger informações confidenciais,
c. Garantir que a segurança cibernética esteja na agenda em reuniões de equipe semelhantes a briefings de segurança ou outros tópicos importantes que são discutidos com frequência, e
d. Realizar treinamento de segurança cibernética como uma atividade contínua ao longo do ano.

Avaliação de risco

Os fabricantes de tecnologia médica precisam garantir que seus clientes entendam que pode haver riscos na aplicação de práticas de higiene cibernética a qualquer sistema. Como tal, os fabricantes precisam enfatizar a importância de seus clientes realizarem uma avaliação de risco antes de aplicar quaisquer novas políticas ou incorporar novas tecnologias. As avaliações de risco permitem que um cliente entenda os sistemas que possui e planeje onde podem precisar de contramedidas adicionais ou compensatórias para lidar com os riscos.

Os fabricantes devem fornecer informações sobre como mitigar os diferentes tipos de riscos potenciais que podem estar relacionados aos seus produtos. Os riscos potenciais discutidos pelo fabricante não precisam ser uma lista abrangente, mas devem estar relacionados a alguns dos casos de uso planejados pelo fabricante durante o desenvolvimento do produto. Ao recomendar que os clientes realizem uma avaliação de risco e apresentar alguns dos riscos potenciais da aplicação de diferentes políticas e tecnologias, os fabricantes podem ajudar seus clientes a mitigar os riscos a um nível aceitável.

Os fabricantes também devem enfatizar que os clientes não se concentram estritamente nos riscos no nível do dispositivo durante a avaliação. Algumas das principais fontes de vulnerabilidades de segurança

RESTRITO

cibernética são sistêmicas e resultam da integração de vários dispositivos em sistemas. Embora não se deva esperar que um fabricante discuta os produtos de outro, eles devem conscientizar seus clientes de que devem prestar atenção especial aos pontos de integração entre os dispositivos.

Se uma organização não possui uma estrutura de avaliação de risco existente, alguns exemplos são:

a. Avaliação de Ameaças, Ativos e Vulnerabilidades Operacionalmente Críticas (OCTAVE)

   https://resources.sei.cmu.edu/library/asset-view.cfm?assetid=309051

b. Análise Fatorial de Risco de Informação (FAIR)

   https://www.fairinstitute.org/fair-risk-management

c. Estrutura de Gerenciamento de Risco (RMF) do Instituto Nacional de Padrões e Tecnologia (NIST)

   https://www.nist.gov/cyberframework/risk-management-framework

d. Avaliação de risco do agente de ameaça (TARA)

   https://itpeernetwork.intel.com/whitepaper-prioritizing-information-security-risks-with-threat-agent-risk-assessment/#gs.9trytf

A avaliação de risco deve levar em consideração o possível impacto na segurança. Ao lidar com medidas de segurança em um ambiente de saúde, padrões como o ISO/IEC 80001-1 podem ajudar no gerenciamento dessas preocupações.

Comunicação eficaz de informações de segurança cibernética aos clientes

Para permitir que os clientes gerenciem efetivamente suas expectativas de segurança cibernética, vários tipos de informações relevantes de segurança podem ser fornecidos a eles pelo fabricante. Isso pode incluir, mas não se limita a:

a. Orientação de segurança através de Instruções de Uso.

   Observação: As instruções de uso devem atender às expectativas de controles de segurança presentes na rede do cliente (o ambiente de uso pretendido) e devem fornecer mais orientações sobre proteção contra malware, acesso baseado em função, backups e outras responsabilidades dos usuários.

b. Informações genéricas sobre segurança de produto e capacidade de privacidade conforme capturadas, por exemplo, na Declaração de divulgação dos fabricantes para segurança de dispositivos médicos (MDS2).

c. Avisos de segurança e notificações de segurança de campo em caso de vulnerabilidades não mitigadas.

   Observação: Para agilizar a informação aos clientes, além de fornecer notificações de segurança de campo para problemas de segurança, pode ser aconselhável publicar avisos de segurança no site do fabricante e/ou por meio de organizações de segurança como H-ISAC (https://h-isac.org/) e a Agência de Segurança Cibernética e de Infraestrutura nos EUA (https://us-cert.cisa.gov/).

RESTRITO

d. Informações de atualizações de segurança e upgrades onde o cliente é responsável pela segurança da plataforma (por exemplo, para SaMD).

   Observação: quando o cliente é responsável por atualizações e upgrades de segurança, como é o caso de alguns produtos somente de software, o fabricante pode informar a seus clientes quando os patches são compatíveis ou não com o produto.

e. Informações sobre fim de vida/fim de suporte, obsolescência de componentes do dispositivo e transferência de risco.

   Observação: Em geral, o fabricante tem a obrigação de garantir que o produto seja mantido seguro, mas essa obrigação passa para o cliente quando o produto é declarado em fim de vida. Nesse caso, o fabricante pode fornecer ao cliente informações de risco mais detalhadas para o uso contínuo de produtos obsoletos/sem suporte.

f. Conselhos para ingressar em organizações de compartilhamento de informações de segurança para obter informações de segurança relevantes.

   Observação: Aconselhar os clientes a ingressarem em CERTs, ISACs nacionais ou outras organizações de compartilhamento de informações para aprender rapidamente sobre ameaças de segurança relevantes.

g. Informações de contato de Divulgação Coordenada de Vulnerabilidades e outros meios para o cliente informar o fabricante sobre vulnerabilidades descobertas e entrar rapidamente em contato com as equipes de segurança apropriadas.

Princípios fundamentais

Para cada um dos princípios fundamentais a seguir, este documento contém uma identificação de ameaças, sua relevância (incluindo padrões de referência informativos apropriados ou outros documentos que possam ser aplicáveis), uma análise para determinar as implicações e recomendações que os fabricantes de DITTA podem fornecer a seus clientes.

Embora as recomendações individuais sejam muito valiosas, as atividades de segurança não gerenciadas podem não ser muito eficazes ou sustentáveis em uma organização. Portanto, os prestadores de serviços de saúde devem entender a importância de um Sistema de Gerenciamento de Segurança da Informação geral, como pode ser estabelecido usando o padrão ISO/IEC 27001.

Segmentação de redes

Este princípio se concentra na prática de dividir uma rede de computadores em sub-redes (também chamadas de zonas), cada uma sendo segmentos de rede independentes. Isso fornece a capacidade de segmentar zonas com diferentes requisitos de segurança. Compartimentar dispositivos em zonas não significa necessariamente isolá-los.

Identificação de ameaças e análise de suas implicações

A segmentação de redes fornece uma maneira de monitorar e gerenciar a comunicação através dos limites da zona. Se o tráfego de rede está entrando (ingressando) ou saindo (egressando) da zona, ele deve representar o conjunto mínimo de comunicação necessário para manter as operações adequadas.

A segmentação de redes também fornece alguma proteção contra a propagação de um incidente. Ao limitar o tráfego de rede que pode entrar ou sair de uma zona, a propagação de um incidente de uma

RESTRITO

zona para outra através de uma rede pode ser retardada ou interrompida. Isso geralmente reduz as consequências de um incidente.

Documentos de referência

a. IEC 62443-2-1:2010 Redes de comunicação industrial—segurança de rede e sistema—Parte 21: Estabelecendo um programa de segurança de sistema de controle e automação industrial
    1. A.3.3.4 Segmentação de Rede
b. IEC 62443-3-3:2013 Redes de comunicação industrial—segurança de rede e sistema—Parte 33: Requisitos de segurança do sistema e níveis de segurança
    1. SR 5.1 Segmentação de Rede
c. NIST SP 800-53 Rev 5 Controles de segurança e privacidade para sistemas de informação e organizações
    1. AC-4 Aplicação do Fluxo de Informação
    2. SC-7 Proteção de Limite
d. ISO/IEC 27001:2013 Tecnologia da informação — Técnicas de segurança — Sistemas de gerenciamento de segurança da informação — Requisitos
    1. 5.2, 5.3, 7.5.1, 7.5.2, 7.5.3, A.13.1.1, A.13.1.3, A.13.2.1, A.14.1.2, A.14.1.3
e. NIST SP 800-82 Rev 2 Guia para Segurança de Sistemas de Controle Industrial (ICS) (maio de 2015)
f. NIST SP 800-125B Configuração de rede virtual segura para proteção de máquina virtual (VM) (março de 2016)
g. NIST SP 800-153 Diretrizes para proteger redes locais sem fio (WLANs) (fevereiro de 2012)

Recomendações dos Fabricantes

Os fabricantes devem fornecer orientação de segmentação de rede para seus clientes, para que eles saibam o que esperar quando seus produtos forem implantados. Por exemplo, se o produto for projetado para ser implantado em uma rede industrial protegida da Internet por um ou mais firewalls, o cliente deve ser informado desse fato. Ao fornecer ao cliente um conjunto de expectativas, o fabricante pode ajudar a seus clientes em seu processo de design. Os fabricantes também podem dissuadir a seus clientes de implantar os produtos de maneira que possam introduzir vulnerabilidades desnecessárias.

Quando os fabricantes recomendam o uso de seus dispositivos em redes segmentadas, eles também devem fornecer informações ao cliente sobre como se comunicar com os produtos por meio de dispositivos como firewalls. Isso pode significar fornecer informações sobre as metodologias de implantação recomendadas, como o uso de um servidor intermediário localizado em uma zona desmilitarizada (DMZ). Os fabricantes também devem fornecer recomendações sobre portas de rede específicas a serem abertas no firewall para permitir que a comunicação flua adequadamente. A tabela 1 fornece um exemplo de como descrever as características de comunicação de um dispositivo em uma configuração de rede.

RESTRITO

Tabela1—Exemplo de uma configuração de rede necessária

Nome do Serviço	Descrição	Protocolo	Identificador de Interface	Porta	Cliente esperado
Use as descrições da IANA sempre que possível	Descreva o protocolo	Normalmente TCP, UDP, IP	Quando um dispositivo tiver mais de uma interface, forneça um identificador	Identifique as portas padrão e o intervalo configurável	O que se espera para conectar a porta e para que finalidade
HTTPS	Hypertext Transfer Protocol Secure - transportando HTML/JavaScript	TCP	ETH 1	443	O dispositivo hospeda um servidor web para que os usuários administrativos possam conectar e configurar o dispositivo por meio de uma interface gráfica do usuário.
Mbap	Protocolo de Aplicação Modbus	TCP	ETH 2	502 [1025-32768]	O dispositivo responde ao Modbus nesta porta

Outra situação que os fabricantes devem considerar ao fornecer orientação de segmentação de rede para seus clientes é o caso em que o produto é isolado e pode não ter conexão com os sistemas de negócios e/ou Internet. Embora essa situação possa parecer desejável como um método para fornecer mais segurança, geralmente apresenta outros riscos ao não permitir que os dispositivos sejam atualizados com tanta frequência ou facilidade e ao exigir que tecnologias como unidades USB (Universal Serial Bus) sejam empregadas que tenham suas próprias vulnerabilidades. As recomendações fornecidas pelo fabricante devem incluir procedimentos para inicialização e atualização offline se essas funções forem suportadas.

Os fabricantes também devem considerar a possibilidade de que seus produtos sejam implantados por um cliente que utilize redes sem fio e devem planejar seguir as diretrizes apropriadas para proteger as redes sem fio. Se o fabricante tiver instruções ou precauções específicas relacionadas à implantação sem fio de seu produto, ele deverá informar o cliente.

Por fim, os fabricantes devem considerar um cenário de implantação envolvendo acesso remoto e/ou manutenção do produto. O fabricante possui algum recurso especial que permita que o produto seja acessado remotamente pela equipe de operações e manutenção do cliente? O fabricante tem algum recurso especial que permite que o dispositivo seja atendido e/ou mantido remotamente pelo fabricante? Em caso afirmativo, estes devem ser comunicados ao cliente. Não devem permanecer backdoors

RESTRITO

secretas para o fabricante, pois podem ser encontrados por um pesquisador ou adversário e se tornar uma vulnerabilidade. Se o cliente souber sobre o recurso, ele poderá planejar contramedidas de acordo.

Entendimento dos tipos de dados e fluxos

Esse princípio se concentra em entender os aplicativos e os protocolos de rede que estão sendo implantados em um produto. Os clientes devem iniciar seu exercício de análise de fluxo de dados segmentando seus ativos de dados em categorias com base nos níveis de sensibilidade e proteção necessários. Essa categorização permitirá o escopo e a priorização adequados da implementação de técnicas de mitigação de risco. Para os clientes, é importante entender a origem e os 'endpoints' dos dados à medida que eles fluem pela rede, juntamente com as funções e privilégios de acesso aos dados. Também é importante que os clientes saibam quais softwares e portas de rede em potencial eles podem precisar gerenciar e monitorar junto com o produto. A partir da lista fornecida por um fabricante, os clientes podem estabelecer um mapa de fluxos de dados autorizados para seu sistema.

Identificação de ameaças e análise de suas implicações

Dentro de uma rede industrial, a quantidade e os tipos de dados enviados e recebidos são relativamente estáticos. A introdução de padrões de fluxo de dados atípicos pode representar atividades maliciosas que podem comprometer ou desligar a rede. Nas redes onde os dados são mais dinâmicos, outras técnicas de segurança devem ser utilizadas para monitorar possíveis atividades maliciosas, dada a falta de padrões de fluxo típicos.

Documentos de referência

a. IEC 62443-2-4:2015 Segurança para automação industrial e sistemas de controle - Parte 2-4: Requisitos do programa de segurança para provedores de serviços IACS
    1. SP 03.09 Arquitetura, Proteção de Dados, Comunicações
    2. SP 03.10 Arquitetura, Proteção de Dados, Dados Sensíveis
b. IEC 62443-3-2 (Rascunho) Segurança para automação industrial e sistemas de controle—Parte 3-2: Avaliação de risco de segurança e projeto do sistema
    1. ZCR 6.4 Zona e características do conduíte
c. NIST SP800-53, Rev 5: Controles de segurança e privacidade para sistemas de informação e organizações
    1. AC-4 Aplicação do Fluxo de Informação
    2. CA-9 Conexões do Sistema Interno
d. ISO/IEC 27001:2013 Tecnologia da informação — Técnicas de segurança — Sistemas de gerenciamento de segurança da informação — Requisitos
    1. 5.2, 5.3, 7.5.1, 7.5.2, 7.5.3, A.13.1.3, A.13.2.1, A.14.1.2, A.14.1.3
e. NIST SP 800-82 Rev 2 Guia para Segurança de Sistemas de Controle Industrial (ICS) (maio de 2015)
f. Ferramentas de software de fluxo de dados NIST – Sistema de fluxo de dados NIST Versão 2– disponível para download em -https://www.nist.gov/itl/iad/mig/nist-smart-space-project/nist-smart-space-project-data-flow/data-flow-downloads

RESTRITO

g. Guia do usuário do sistema de fluxo de dados NIST versão 2 - disponível para download em - https://www.nist.gov/itl/iad/mig/nist-smart-space-project/nist-smart-space-project-data-flow/nist-data-flow-system-ii

Recomendação do fabricante

Os clientes precisam entender os fluxos de dados esperados em uma rede específica. Especificamente, como os dados fluem do Ponto “A” para o Ponto “B” em uma rede, pode não ser apropriado revelá-los a qualquer outro dispositivo na rede, ou os dados em si não devem ser modificados em seu formato ou conteúdo. Outras considerações precisam ser abordadas se os dados estiverem entrando em uma rede de uma fonte externa (como a nuvem) por meio de um firewall ou gateway.

Como diretriz geral, os fluxos de dados em uma rede devem ter os seguintes recursos:

a. **Pontualidade:** Os dados devem ser transmitidos em um período limitado e controlado.
b. **Precisão:** As alterações não devem ser feitas enquanto os dados estão sendo transmitidos.
c. **Entrega:** Os dados devem ser entregues apenas ao usuário pretendido.

Além de explicar a segmentação de rede conforme a seção 1, os fabricantes também devem explicar a seus clientes os aplicativos e portas de rede que acompanham o produto. Em alguns casos, como produtos baseados no Microsoft Windows, pode haver aplicativos instalados no produto não diretamente associados à funcionalidade do produto desejada pelo fabricante. Estes podem fornecer recursos adicionais para o cliente, mas podem estar fora do controle do fabricante.

Os fabricantes geralmente fornecem funcionalidades de rede adicionais em seus produtos além do conjunto mínimo necessário para operar corretamente. Por exemplo, um produto pode ter um servidor da Web incorporado para fornecer informações de diagnóstico. O servidor web não faz parte da funcionalidade principal do produto, mas oferece um benefício ao cliente ao operar e manter o produto. Os fabricantes precisam garantir que os clientes estejam cientes da funcionalidade adicional que pode ser acessada pela rede para permitir que eles avaliem os riscos e benefícios dessa funcionalidade.

Monitoramento de Dispositivos e Sistemas

Os clientes são os responsáveis por monitorar os dispositivos e sistemas em sua rede. Os fabricantes devem fornecer aos clientes a capacidade de monitorar seus dispositivos, de preferência usando alguma tecnologia de monitoramento centralizado.

Além de simplesmente monitorar os dispositivos e sistemas em sua rede em busca de possíveis incidentes ou anomalias de segurança, os clientes podem esperar que os produtos dos fabricantes sejam capazes de relatar informações de identificação. Isso permite que os clientes façam um inventário preciso de seus dispositivos e sistemas. Ser capaz de coletar centralmente essas informações pode tornar desnecessário tocar em cada dispositivo ou sistema.

Coletar e analisar as informações desses dispositivos fornece uma indicação precoce de um evento atípico.

Um mecanismo que os fabricantes podem utilizar para fornecer informações de segurança do dispositivo aos clientes é o Software Bill of Materials (SBOM). O SBOM é uma lista mantida de componentes de software utilizados em um dispositivo ou sistema e pode auxiliar na detecção de possíveis ameaças à segurança, identificando o componente de software em risco. Um SBOM típico contém informações do

RESTRITO

componente, como fornecedor do componente, nome do componente e versão do componente. O SBOM deve ser atualizado à medida que os componentes de software são atualizados ou alterados.

Identificação de ameaças e análise de suas implicações

Um sistema de monitoramento eficaz servirá para aumentar a segurança integrada do dispositivo ou sistema correspondente.

Documentos de referência

a. IEC 62443-3-3:2013 Redes de comunicação industrial—Rede e segurança do sistema—Parte 33: Requisitos de segurança do sistema e níveis de segurança
    1. FR 6 Resposta oportuna a eventos
b. NIST SP 800-53 Rev 5 Controles de segurança e privacidade para sistemas de informação e organizações
    1. AU-2 Eventos de Auditoria
    2. AU-3 Conteúdo dos Registros de Auditoria
    3. AU-7 Redução de Auditoria e Geração de Relatórios
    4. AU-8 Carimbos de data e hora
    5. CA-7 Monitoramento Contínuo
    6. SI-4 Monitoramento do Sistema
c. ISO/IEC 27001:2013 Tecnologia da informação — Técnicas de segurança — Sistemas de gerenciamento de segurança da informação — Requisitos
    1. 5.2, 5.3, 7.5.1, 7.5.2, 7.5.3, 9.1, 9.2, A.12.4.1, A.12.4.4, A.18.2.2, A.18.2.3
d. NIST SP 800-82 Rev 2 Guia para Segurança de Sistemas de Controle Industrial (ICS) (maio de 2015)
e. IETF RFC 5424: O protocolo Syslog
f. FDA Conteúdo das submissões de pré-mercado para gerenciamento de segurança cibernética em dispositivos médicos
g. FDA Gerenciamento pós-mercado de segurança cibernética em dispositivos médicos

Recomendação dos fabricantes

Os clientes podem querer manter um inventário de todos os dispositivos em sua rede, identificando itens como fornecedor, número do modelo, número de série e revisão do firmware. Os fabricantes podem fornecer algumas dessas informações a seus clientes fornecendo, por exemplo, um SBOM com seu dispositivo. Os fabricantes devem educar seus clientes sobre como recuperar essas informações, especialmente se estiverem disponíveis por meio de um servidor central. Isso ajudará o cliente a gerar e manter automaticamente uma lista de ativos precisa, uma parte essencial do monitoramento e detecção de incidentes.

Os fabricantes que constroem produtos com a capacidade de monitorá-los de outro local (como um sistema de monitoramento central) devem descrever os eventos e alertas que o produto pode gerar. Os

RESTRITO

protocolos usados para comunicar alertas e eventos devem ser capazes de atribuir diferentes níveis, prioridades ou identificadores. Os fabricantes devem fornecer contexto em torno desses alertas e eventos para seus clientes, como alertas de proteção de endpoint, tentativas de saída de firewall bloqueadas e adição de novos usuários de administração. Eles devem explicar a diferença entre eventos informativos e avisos para que os clientes possam entendê-los e utilizá-los em seu gerenciamento de alarmes e planos de resposta a incidentes.

Os clientes muitas vezes são desafiados a integrar dispositivos em seu ambiente de monitoramento, sem uma compreensão clara dos tipos de eventos, alarmes e estatísticas que um determinado dispositivo ou componente pode gerar. Os fabricantes podem facilitar a integração de seus produtos em um ambiente de monitoramento do cliente documentando os eventos, alarmes e estatísticas que o produto gera e explicando a importância relativa das informações. Uma explicação clara das informações, seu significado e implicações para um cliente, e uma ação recomendada para o cliente quando um determinado evento ocorre, podem ser usados pelos clientes para estarem mais preparados e informados. A documentação clara e concisa de eventos e estatísticas aumentará a chance de o cliente obter a resposta desejada. Sempre que possível; os eventos e alarmes também devem incluir recomendações textuais sucintas sobre as ações que um cliente deve tomar em resposta ao evento.

Os dispositivos na rede devem ser monitorados para determinar como eles normalmente interagem. Uma ferramenta de gerenciamento de informações e eventos de segurança (SIEM) pode fornecer muitos recursos e serviços para que os clientes forneçam com eficiência uma visão holística, não apenas de uma infraestrutura de rede específica, mas também de seu fluxo de trabalho, conformidade e gerenciamento de logs. Em sua essência, um SIEM fornece coleta de eventos e logs, exibições centradas em camadas, normalização, correlação, adaptabilidade, relatórios e alertas e gerenciamento de logs. Os clientes podem não ter o conhecimento necessário para implantar e gerenciar um SIEM por conta própria. Nesse caso, os provedores de serviços de segurança gerenciados (MSSP) geralmente podem fornecer soluções prontas para uso.

Gerenciamento de usuários

Os fabricantes devem fornecer recursos de gerenciamento de usuários a seus clientes para que eles possam controlar de forma inteligente o acesso à sua rede de computadores. O gerenciamento de usuários geralmente abrange as quatro áreas a seguir:

a. **Administração-** Os usuários designados como administradores devem ter recursos para criar, modificar e excluir contas no sistema. Isso pode ser gerenciado centralmente ou localmente.

b. **Autenticação-** Deve haver um processo para verificar a identidade de um usuário. Com base no grau de risco aceitável, isso pode ser multifatorial.

c. **Autorização-** A capacidade deve ser fornecida para gerenciar privilégios de usuário, por exemplo, controle de acesso baseado em função.

d. **Auditoria—** Deve haver uma maneira de monitorar as ações realizadas e os recursos consumidos por um usuário ou processo e armazenar esses dados em um log de auditoria.

Identificação de ameaças e análise de suas implicações

Talvez uma das ameaças mais comuns seja o fato de os fabricantes não imporem uma alteração obrigatória de senha padrão durante a configuração inicial de um produto. Embora as senhas padrão sejam muito úteis para fabricantes e clientes ao permitir a configuração rápida de um dispositivo a partir de seu estado original, surgem problemas quando as senhas padrão não são alteradas pelo cliente, os

RESTRITO

fabricantes não fornecem um mecanismo fácil para alterá-las ou senhas codificadas estão incluídas no produto.

Quando um cliente devolve um dispositivo para manutenção e atribui a ele uma senha exclusiva, pode ser difícil para um fabricante recuperar o desempenho do produto e os logs de atividades necessários para o processo de reparo.

Documentos de referência

a. IEC 62443-2-1:2010 Redes de comunicação industrial—Segurança de rede e sistema—Parte 21: Estabelecendo um programa de segurança de sistema de controle e automação industrial
    1. A.3.3.5 Elemento: Controle de Acesso: Administração de Conta
    2. A.3.3.6 Elemento: Controle de Acesso: Autenticação
    3. A.3.3.7 Elemento: Controle de Acesso: Autorização
b. IEC 62443-3-3:2013 Redes de comunicação industrial—Rede e segurança do sistema—Parte 33: Requisitos de segurança do sistema e níveis de segurança
    1. Suporte de funções essenciais
    2. FR 1 Identificação e controle de autenticação
    3. FR 2 Controle do uso
c. NIST SP 800-53 Rev 5 Controles de segurança e privacidade para sistemas de informação e organizações
    1. AC Access Control Family
    2. AU-14 Auditoria da Sessão
    3. IA Identification and Authentication Family
d. ISO/IEC 27001:2013 Tecnologia da informação — Técnicas de segurança — Sistemas de gerenciamento de segurança da informação — Requisitos
    1. 5.2, 5.3, 7.5.1, 7.5.2, 7.5.3, A.5.1.1, A.5.1.2, A.6.1.1, A.6.2.1, A.6.1.2, A.6.2. 1, A.6.2.2, A.9.1.2, A.9.2.1, A.9.2.2, A.9.2.3, A.9.2.4, A.9.2.5, A.9.2.6, A.9.3.1, A.9.4.1, A.9.4.2, A.9.4.3, A.9.4.4, A.9.4.5, A.11.1.5, A.11.2.6, A. 11.2.8, A.11.2.9, A.12.1.1, A.12.4.1, A.13.1.1, A.13.1.3, A.13.2.1, A.14.1.2, A.14.1. 3, A.18.1.1, A.18.1.3, A.18.1.5, A.18.2.2
e. NIST SP 800-82 Rev 2 Guia para Segurança de Sistemas de Controle Industrial (ICS) (maio de 2015)

Recomendação do fabricante

Embora os produtos dos fabricantes possam oferecer a capacidade de gerenciar usuários, cabe aos clientes implementar esses recursos adequadamente para manter a segurança desses produtos. Os fabricantes devem fazer recomendações a seus clientes sobre estratégias de implementação e aconselhá-los sobre o gerenciamento de usuários.

Os fabricantes podem ajudar seus clientes a implementar o gerenciamento de usuários fornecendo casos de uso que envolvem todo o ciclo de vida de um usuário. Isso permitiria ao fabricante fornecer

RESTRITO

recomendações sobre a integração do processo de contratação com a capacidade de criar e gerenciar usuários com seu produto. Também poderia discutir a modificação da função de um usuário com base em uma mudança de função e, eventualmente, desabilitar e excluir contas de usuário devido à troca de função. Também permitiria ao fabricante destacar e distinguir sua funcionalidade, como fornecer maior granularidade no gerenciamento de funções do usuário ou distinções entre terceiros e/ou contratados de operadores e engenheiros normais.

Uma recomendação de segurança comum para os clientes é que eles auditem suas contas de usuário regularmente. Se um fabricante implementou o recurso de auditoria de contas de usuário em seus produtos, ele deve informar seus clientes sobre como usar esse recurso de auditoria. Isso aumentará muito a capacidade do cliente de monitorar suas contas de usuário com menor tempo gasto na coleta de dados.

Os dispositivos da Internet das Coisas (IoT) proliferaram e alguns representaram uma ameaça à Internet em geral. Isso ocorre devido ao grande número de dispositivos IoT e porque alguns fabricantes desses produtos não adotaram medidas de segurança cibernética apropriadas para protegê-los. Como resultado, os produtos IoT foram comprometidos e usados para fins maliciosos. Uma maneira típica pela qual os dispositivos foram comprometidos é por meio de senhas padrão, que os clientes geralmente não alteram e nem sabem que existem.

As senhas padrão são normalmente usadas para realizar o comissionamento inicial do dispositivo porque os padrões conhecidos simplificam o processo. Recomenda-se que os fabricantes exijam que as senhas padrão sejam alteradas antes que o dispositivo se torne capaz de se comunicar operacionalmente. Os requisitos de complexidade de senha variam de acordo com o setor. Os fabricantes são incentivados a evitar que o usuário use senhas fracas em conformidade com esses padrões de complexidade de senha. Normalmente, um dispositivo terá uma ou mais contas e/ou senhas armazenadas localmente para executar várias funções quando a autenticação e autorização do usuário remoto central não estiver disponível ou habilitada.

Inevitavelmente, as senhas para autenticação local serão perdidas ou esquecidas. A seguir estão as melhores práticas recomendadas para a recuperação de um dispositivo nestas condições:

a. Sempre que possível, autentique centralmente (por exemplo, via RADIUS, LDAP ou Active Directory) um usuário como administrador de segurança privilegiado do dispositivo. Além disso, permita que o usuário privilegiado redefina as senhas de contas locais para um novo valor.

b. Quando a autenticação central não for possível, os fabricantes devem fornecer algum mecanismo que não seja baseado em rede, por exemplo, um botão de reinicialização ou uma sequência de ativação especial, para redefinir um dispositivo para sua configuração e/ou senha padrão, permitindo que os clientes restaurem o acesso ao dispositivo. Os fabricantes devem documentar claramente os mecanismos de redefinição para que os clientes entendam o estado operacional do dispositivo antes, durante e após o processo de redefinição.

    1. O usuário deve ser solicitado a alterar a senha padrão como parte do processo de redefinição de senha da mesma forma que é necessário para o comissionamento inicial do dispositivo.

    2. Quando um dispositivo é redefinido, ele deve comunicar a operação de redefinição a um serviço ou sistema de registro.

    3. A operação segura do dispositivo deve continuar enquanto o usuário estiver redefinindo a senha.

RESTRITO

4. O sistema deve excluir todas as informações confidenciais do cliente armazenadas no dispositivo após a redefinição de senha. O sistema deve limpar com segurança as chaves de criptografia, certificados e endereços IP ou nomes DNS armazenados no dispositivo para evitar a divulgação de informações privadas do cliente.
5. Os fabricantes devem fornecer um meio de fazer backup da configuração e das configurações de um dispositivo e permitir a restauração da configuração e das configurações após a redefinição de senha para trazer um dispositivo de volta ao estado totalmente operacional com o mínimo de tempo de inatividade.

Os fabricantes às vezes ignoram a manutenção de devolução do produto. Os dispositivos que são protegidos corretamente e protegidos por senha com senhas do cliente devem impedir o acesso às informações necessárias aos fabricantes para diagnosticar problemas. Recomendamos a seguir as melhores práticas:

a. Os fabricantes devem documentar sua política de privacidade de dados de clientes em relação às informações que podem recuperar de um dispositivo devolvido.
b. O mecanismo usado pelo fabricante para recuperar informações de diagnóstico, logs e definições de configuração do dispositivo não deve incluir a recuperação de informações pessoais, incluindo chaves simétricas e assimétricas, certificados, senhas etc.
c. Quando um dispositivo é acessado pelo fabricante para manutenção, o dispositivo deve apagar todos os dados confidenciais do cliente, mas preservar e permitir que o fabricante acesse os dados de diagnóstico.
d. Um dispositivo acessado por um fabricante deve ser totalmente redefinido antes de retornar ao serviço.
e. O método utilizado pelo fabricante para obter acesso às informações de diagnóstico deve exigir acesso físico ao dispositivo e pode ser uma variação do processo utilizado pelos clientes para recuperar senhas perdidas ou esquecidas.

Fortalecimento dos dispositivos

Este princípio aborda as técnicas que os fabricantes oferecem aos seus clientes para fortalecer os dispositivos com base nos requisitos de um mercado específico.

Identificação de ameaças e análise de suas implicações

À medida que os fabricantes de equipamentos oferecem a seus clientes defesas de rede mais eficazes, os invasores identificam métodos alternativos para entrar no ambiente de rede protegido e confiável. Uma vez dentro, esses ataques podem explorar vulnerabilidades ou comprometer o ambiente usando vários vetores, como web, e-mail e arquivos maliciosos.

Deve-se considerar as trocas de manutenção e funcionalidade ao proteger um dispositivo. Por exemplo, fechar portas de rede ou desabilitar funcionalidades em um sistema operacional pode tornar mais difícil para um administrador de rede cumprir suas responsabilidades.

Para muitos dispositivos médicos, é proibido fortalecer um dispositivo após sua implantação sem o envolvimento explícito do fabricante.

RESTRITO

Documentos de referência

a. NEMA CPSP 1-2015 Melhores Práticas da Cadeia de Suprimentos

b. NEMA/MITA CSP 1-2016 Cibersegurança para imagens médicas

c. IEC 62443-3-3:2013 Redes de comunicação industrial—Rede e segurança do sistema—Parte 33: Requisitos de segurança do sistema e níveis de segurança

    1. SR 3.5 Validação de entrada
    2. SR 3.6 Saída determinística
    3. SR 3.7 Tratamento de erros
    4. SR 4.3 Uso de criptografia

d. NIST SP 800-53 Rev 5 Controles de segurança e privacidade para sistemas de informação e organizações

    1. SC-27 Aplicativos independentes de plataforma
    2. SC-41 Acesso à porta e ao dispositivo de E/S

e. ISO/IEC 27001:2013

    1. 5.2, 5.3, 7.5.1, 7.5.2, 7.5.3, A.9.1.1, A.9.2.1, A.9.2.2, A.9.2.3, A.9.2.6, A.12.1. 1, A.12.2.1, A.12.5.1, A.12.6.2, A.13.1.1, A.13.1.2, A.13.1.3, A.14.1.1,

f. NIST SP 800-82 Rev 2 Guia para Segurança de Sistemas de Controle Industrial (ICS) (maio de 2015)

Recomendações do fabricante

Os fabricantes devem fornecer a seus clientes dispositivos que sejam seguros por padrão e oferecer procedimentos para proteger seus dispositivos se fornecerem esse recurso. Os procedimentos de proteção também devem permitir que algumas funções sejam reforçadas, enquanto outras permanecem abertas para acomodar diferentes ambientes de clientes.

Os fabricantes também precisam fornecer algumas das compensações de risco para seus clientes ao fortalecer seus produtos. Na maioria dos casos, a proteção envolve a desativação de determinadas funções do produto ou a instalação da proteção de endpoint. Se um cliente optar por implementar o procedimento de proteção, ele deve ser informado sobre o impacto na funcionalidade e os riscos se não for configurado corretamente. Isso ajudará o cliente a tomar uma decisão baseada em risco sobre implementar ou não o procedimento de fortalecimento.

Existem alguns casos em que um fabricante pode não ter permissão para proteger um dispositivo após sua instalação. Nesses casos, os fabricantes podem decidir oferecer controles de mitigação (também conhecidos como contramedidas de compensação), como desabilitar um serviço vulnerável ou desabilitar portas no próprio dispositivo. Os fabricantes também podem fornecer uma lista de softwares de proteção de endpoints recomendados e validados com detalhes exatos sobre como configurá-los para o dispositivo.

Finalmente, os fabricantes devem alertar seus clientes sobre quaisquer implicações de segurança e garantia caso um cliente fortaleça um de seus dispositivos. Ao tempo em que desabilitar uma porta USB de uma placa-mãe a deixe inoperante, pode também torná-la impossível de reparar.

RESTRITO

Atualização de dispositivos

Esse princípio se concentra nos procedimentos que os fabricantes fornecem a seus clientes para atualizar os dispositivos implantados após a descoberta de novas vulnerabilidades ou quando os requisitos de segurança e as necessidades de seu ambiente operacional forem alterados.

Atualizar dispositivos e sistemas sempre que possível é uma etapa importante para acompanhar as recentes melhorias de funcionalidade e segurança.

Documentos de referência

a. HIMSS/NEMA HN_1_2019 Declaração de divulgação do fabricante sobre segurança de dispositivos médicos

b. NEMA CPSP 1-2015 Melhores Práticas da Cadeia de Suprimentos

c. NEMA/MITA CSP 1-2016 Cibersegurança para imagens médicas

d. IEC 62443-2-1:2010 Redes de comunicação industrial—Rede e segurança do sistema—Parte 2-1: Estabelecimento de um programa de segurança do sistema de automação e controle industrial

1. A.3.4.2.5.1 Patching de Dispositivos IACS
2. A.3.4.3 Elemento: Desenvolvimento e manutenção do sistema

e. IEC TR 62443-2-3:2015 Segurança para automação industrial e sistemas de controle—Parte 2-3: Gerenciamento de patches no ambiente IACS

f. NIST SP 800-53 Rev 5 Controles de segurança e privacidade para sistemas de informação e organizações

1. MA Maintenance Family

g. ISO/IEC 27001:2013 Tecnologia da informação — Técnicas de segurança — Sistemas de gerenciamento de segurança da informação — Requisitos

1. 5.2, 5.3, 7.5.1, 7.5.2, 7.5.3, A.5.1.1, A.5.1.2, A.6.1.1, A.11.2.4, A.11.2.5, A.12.1. 1, A.18.1.1, A.18.2.2

h. NIST SP 800-82 Rev 2 Guia para Segurança de Sistemas de Controle Industrial (ICS) (maio de 2015)

eu. NIST SP 1800-24 (2020) Protegendo o sistema de comunicação e arquivamento de imagens (PACS)—Cibersegurança para o setor de saúde

Recomendações aos clientes

A atualização de dispositivos e sistemas é uma contramedida comum discutida em quase todos os padrões, diretrizes e recomendações de segurança. Dependendo do nível de transferência de risco e dos contratos de serviço existentes, a responsabilidade pelas atualizações pode ser do cliente ou do fabricante. Há também riscos associados à instalação de atualizações não validadas pelo cliente (por exemplo, quando uma atualização de terceiros é transmitida ou recebida automaticamente).

Quando os clientes participam da instalação de atualizações de segurança, eles devem estar cientes dos processos de atualização que determinam:

- Aplicabilidade: Qual atualização deve ser implantada em qual dispositivo?
- Preparação: Como a atualização deve ser instalada e os dados do aplicativo devem ser arquivados?

RESTRITO

- Agendamento: Quando a atualização deve ser instalada e quem deve realizar a atualização?

Aplicabilidade: Os processos de atualização devem ser baseados em uma revisão do inventário de ativos existente de um cliente e conter itens como dispositivos elétricos programáveis, gateways de comunicação, sensores inteligentes e equipamentos de teste. Esse inventário de ativos também deve identificar dispositivos que podem ser atualizados independentemente e dispositivos que dependem de atualizações validadas do fabricante.

Preparação: Como a segurança cibernética é uma responsabilidade compartilhada entre diferentes atores (fabricantes, operadores etc.), é importante que existam mecanismos eficientes para garantir que os patches sejam disponibilizados após a detecção de uma vulnerabilidade. Antes que os clientes atualizem o sistema operacional ou alterem outro software nos servidores ou hardware implantados pelo cliente, o cliente deve coordenar com o fabricante para garantir que o software aplicativo e os bancos de dados do fabricante tenham sido testados e sejam compatíveis com a atualização proposta pelo cliente. Alguns fabricantes podem oferecer um serviço de Contrato de Manutenção de Software, que inclui serviços de teste e verificação. O arquivamento de dados de aplicativos – especialmente informações de saúde privadas – pode fazer parte de planos abrangentes de atualização.

Cronograma: os fabricantes geralmente fornecem a capacidade de atualizar seus dispositivos, mas os clientes nem sempre implementam as atualizações em tempo hábil. Os clientes, em muitos casos, avaliarão os riscos associados de software desatualizado em relação ao tempo perdido, receita perdida e tempo de inatividade potencial para implementar a atualização ou a possibilidade de a atualização causar uma falha.

Recomendações aos fabricantes

Os fabricantes precisam fornecer informações aos seus clientes sobre como aplicar as atualizações em diferentes momentos: durante a operação, paradas planejadas, desligamentos etc.Os fabricantes que fornecem atualizações para seus clientes precisam informar seus clientes sobre a prioridade de implementação da atualização. Essa prioridade nem sempre deve ser crítica. Os fabricantes devem fornecer algum contexto para a atualização e outras medidas da prioridade do seu ponto de vista. Isso é especialmente verdadeiro quando um fabricante incorpora bibliotecas ou softwares de terceiros que requerem atualização. Os fabricantes geralmente precisam revisar a atualização de seu fornecedor terceirizado, avaliar a prioridade fornecida por esse fornecedor no contexto de seu dispositivo e, em seguida, traduzi-la em uma prioridade que reflita com precisão qualquer novo risco apresentado pelo dispositivo.

O compartilhamento de custos dependerá dos requisitos legais de diferentes jurisdições, disposições de garantia e acordos contratuais entre fabricantes e operadores. Cada fabricante pode ter sistemas diferentes para estabelecer e custear a manutenção.

Em geral, se um patch mitigar um impacto potencial na segurança ou no desempenho, o patch deve ser disponibilizado pelo fabricante e em tempo hábil. Outros aspectos devem ser abordados nos contratos de serviços entre fabricantes e operadoras. As provisões podem incluir:

- Serviços de gerenciamento de patches (por exemplo, instalação de patches em um sistema para o cliente);
- Disponibilidade e custo de manutenção remota;
- Tempo e frequência da validação do patch (incluindo disponibilidade e custos do serviço acelerado).

Os fabricantes também devem abordar os dispositivos e sistemas legados que foram deixados no mercado conforme sua capacidade. Às vezes, esses dispositivos são muito antigos para receber patches para novas vulnerabilidades devido às arquiteturas de software ou hardware, como o fim do suporte a componentes de terceiros. Os fabricantes devem monitorar os planos de suporte de fornecedores terceirizados e fornecer informações apropriadas aos clientes.

RESTRITO

Além disso, os fabricantes devem fornecer quaisquer planos para encerrar o suporte para o dispositivo ou componentes do dispositivo em tempo hábil. O plano deve incluir o cronograma para o final do suporte, incluindo opções como informações de atualização ou substituição. Além disso, o plano pode incluir informações técnicas adicionais para o uso contínuo dos dispositivos e sistemas, como a proteção dos dispositivos, mesmo que possa apresentar algumas das compensações de risco descritas na seção 5.

Os fabricantes também devem comunicar que as vulnerabilidades de componentes de terceiros não são necessariamente exploráveis no contexto de um dispositivo específico e que uma nova vulnerabilidade não constitui necessariamente um risco à segurança ou ao desempenho do dispositivo médico. Por meio de sua análise de risco atualizada, os fabricantes estão na melhor posição para avaliar o risco residual e informar seus clientes adequadamente.

Caso as vulnerabilidades em componentes de terceiros sejam relevantes, mas não haja patches disponíveis, os fabricantes de dispositivos devem informar seus clientes sobre mitigações técnicas ou organizacionais.

Fornecimento de um plano de recuperação/ escalonamento de processo

Esse princípio se concentra em fornecer um plano de recuperação e um escalonamento de processo que os clientes devem usar para se recuperar rapidamente de um dispositivo com defeito ou que não funcione, que pode ser causado por um ataque mal-intencionado ou um incidente na rede.

Identificação de ameaças e análise de suas implicações

A ausência de um plano de recuperação e escalonamento de processo pode interromper as operações de negócios, segurança da informação, sistemas de TI, funcionários, clientes, fornecedores upstream e outras funções vitais.

Documentos de referência

a. NEMA CPSP 1-2015 Melhores Práticas da Cadeia de Suprimentos

b. IEC 62443-2-1:2010 Redes de comunicação industrial—Segurança de rede e sistema—Parte 21: Estabelecendo um programa de segurança de sistema de controle e automação industrial

    1. A.3.4.5 Elemento: Planejamento e resposta a incidentes

c. IEC 62443-3-3:2013 Redes de comunicação industrial—Rede e segurança do sistema—Parte 33: Requisitos de segurança do sistema e níveis de segurança

    1. SR 7.3 Backup do sistema de controle

d. NIST SP 800-53 Rev 5 Controles de segurança e privacidade para sistemas de informação e organizações

    1. IR Incident Response Family

e. ISO/IEC 27001:2013 Tecnologia da informação — Técnicas de segurança — Sistemas de gerenciamento de segurança da informação — Requisitos

    1. 5.2, 5.3, 7.5.1, 7.5.2, 7.5.3, A.5.1.1, A.5.1.2, A.6.1.1, A.6.1.3, A.7.2.2, A.12.1. 1, A.16.1.1, A.16.1.2, A.16.1.4, A.16.1.5, A.16.1.6, A.18.1.1, A.18.2.2

RESTRITO

f. NIST SP 800-82 Rev 2 Guia para Segurança de Sistemas de Controle Industrial (ICS) (maio de 2015)

g. ISO/IEC 29147:2014: Tecnologia da Informação—Técnicas de Segurança—Divulgação de Vulnerabilidade

h. ISO/IEC 30111:2013: Tecnologia da Informação—Técnicas de Segurança—Processos de Tratamento de Vulnerabilidades

i. NIST Estrutura de segurança cibernética V1.1

Recomendação dos fabricantes

Gerenciar e responder a incidentes e cenários de desastres fica a cargo dos clientes. Os clientes precisam ter planos de resposta a incidentes, planos de recuperação de desastres e planos de continuidade de negócios projetados adequadamente e executá-los de forma adequada. Os fabricantes podem oferecer a capacidade, por exemplo, de backup e recuperação e incorporar a funcionalidade de monitoramento e alerta em seus produtos com sistemas de monitoramento centralizados, mas os clientes são responsáveis por implementar esses recursos e procedimentos.

Os fabricantes devem oferecer a seus clientes informações sobre como receber suporte técnico caso um cliente precise de assistência em um incidente ou cenário de desastre. Essas informações podem ser especificadas como parte de um acordo de nível de serviço (SLA), mas devem ser claramente indicadas como o cliente deve entrar em contato com o fabricante para obter suporte. Essas informações devem descrever as informações que o fabricante pode solicitar ao cliente para que ele possa ajudá-lo a responder ao incidente.

Os fabricantes também devem oferecer um mecanismo para que clientes e pesquisadores forneçam feedback e relatórios de vulnerabilidade sobre seus produtos. Não é incomum que os clientes descubram vulnerabilidades em produtos que precisam ser corrigidas. Os fabricantes devem ter um mecanismo para que os clientes enviem relatórios de vulnerabilidade com segurança e os clientes devem receber informações sobre como o envio dessas informações pode ser realizado. Da mesma forma, pesquisadores de segurança podem encontrar vulnerabilidades em produtos. Os fabricantes devem oferecer um mecanismo, possivelmente o mesmo que para os clientes, para que outras partes interessadas relatem vulnerabilidades em produtos. Quando os fabricantes ficam sabendo de uma vulnerabilidade, eles devem trabalhar com o cliente e/ou pesquisador para divulgar com responsabilidade essas informações a todos os seus clientes. Os fabricantes devem identificar, avaliar e compartilhar informações de vulnerabilidade, independentemente de onde essas informações venham. Os fabricantes devem usar linguagem simples, em um nível de leitura apropriado para o usuário pretendido, para comunicar informações acionáveis sobre vulnerabilidades e ameaças de segurança cibernética do produto. Pode ser benéfico para o usuário incluir informações sobre os benefícios e riscos associados à implantação de uma atualização ou controles de compensação necessários até que a atualização esteja disponível. Embora isso não elimine a possibilidade de um indivíduo liberar dados de vulnerabilidade sobre o produto do fabricante sem divulgação responsável, reduz a probabilidade de isso acontecer se for tratado com responsabilidade pelo fabricante.

§

RESTRITO