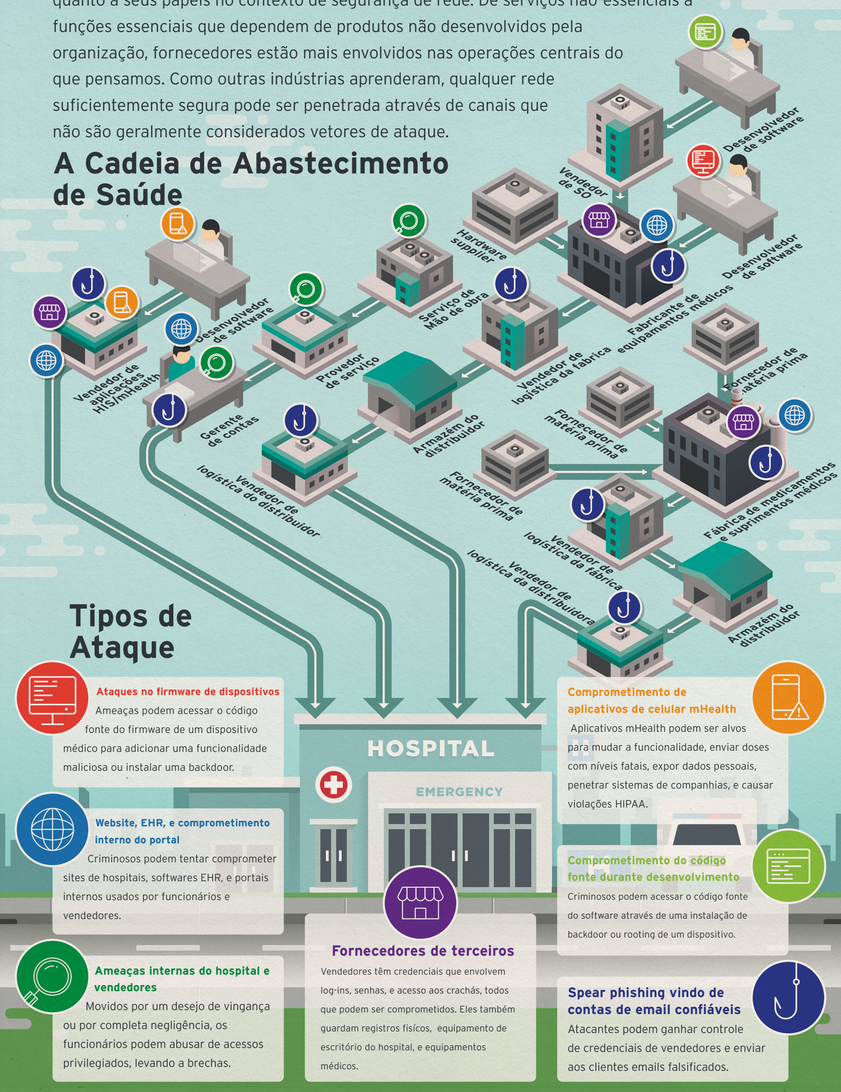
EM QUEM VOCÊ CONFIA?

Desafios de Cadeia de Abastecimento em Hospitais Conectados

Fornecedores terceirizados e prestadores de serviço são muitas vezes negligenciados quanto a seus papeis no contexto de segurança de rede. De serviços não-essenciais à funções essenciais que dependem de produtos não desenvolvidos pela organização, fornecedores estão mais envolvidos nas operações centrais do que pensamos. Como outras indústrias aprenderam, qualquer rede suficientemente segura pode ser penetrada através de canais que não são geralmente considerados vetores de ataque.

A Cadeia de Abastecimento de Saúde



Tipos de Ataque

Ataques no firmware de dispositivos
Ameaças podem acessar o código fonte do firmware de um dispositivo médico para adicionar uma funcionalidade maliciosa ou instalar uma backdoor.

Website, EHR, e comprometimento interno do portal
Criminosos podem tentar comprometer sites de hospitais, softwares EHR, e portais internos usados por funcionários e vendedores.

Ameaças internas do hospital e vendedores
Movidos por um desejo de vingança ou por completa negligência, os funcionários podem abusar de acessos privilegiados, levando a brechas.

Fornecedores de terceiros
Vendedores têm credenciais que envolvem log-ins, senhas, e acesso aos crachás, todos que podem ser comprometidos. Eles também guardam registros fisícos, equipamento de escritório do hospital, e equipamentos médicos.

Comprometimento de aplicativos de celular mHealth
Aplicativos mHealth podem ser alvos para mudar a funcionalidade, enviar doses com níveis fatais, expor dados pessoais, penetrar sistemas de companhias, e causar violações HIPAA.

Comprometimento do código fonte durante desenvolvimento
Criminosos podem acessar o código fonte do software através de uma instalação de backdoor ou rooting de um dispositivo.

Spear phishing vindo de contas de email confiáveis
Atacantes podem ganhar controle de credenciais de vendedores e enviar aos clientes emails falsificados.

O que está em risco?

Saúde do paciente

- Sistemas usados para diagnósticos, monitoramento e tratamento
- Dispositivos médicos
- Equipamentos médicos
- Sistema de informação hospitalar

Privacidade de dados

- Informações pessoais do paciente como registros médicos e informações de seguro
- Informações de funcionarios
- Pesquisas e dados de novos medicamentos
- Folha de pagamento
- Propiedade intelectual

Operações hospitalares

- Dados de agendamentos
- Paginação hospitalar
- Controle de operações
- Sistema de suporte de tubos pneumaticos
- Sistema de inventário
- Administração

Porque organizações de saúde precisam se preocupar com ataques?

- Dano à reputação
- Penalidades ou multas (HIPAA, GDPR, LGPD)
- Esforços de remediação Técnicos e não técnicos
- Perdas financeiras
- Perda de vantagem competitiva
- Problemas legais

O que as organizações de saúde podem fazer?

- Realizar assessments de vulnerabilidades nos novos dispositivos médicos
- Programas de Bring your own device (BYOD) devem incluir autenticação utilizando Network Access Control (NAC) antes de permitir o acesso à rede
- Compre dispositivos médicos de fabricantes que passam por avaliações rigorosas de segurança de seus produtos durante o projeto e a fabricação
- Crie um plano para aplicação de patches e atualização de códigos ou firmware para os dispositivos implantados nos pacientes e nos equipamentos médicos do hospital
- Realize avaliações de risco de todos os fornecedores e vendedores da cadeia de abastecimento e faça verificações de antecedentes sobre os funcionários que têm acesso a dispositivos médicos
- Faça scan de vulnerabilidades e teste de penetração na rede do hospital e nas aplicações para garantir certo nível de segurança em relação à ataques

As recomendações acima da cadeia de abastecimento devem derivar de uma estratégia geral de segurança que permita que uma organização previna e detecte ameaças de segurança cibernética.

Created by TrendLabs,
The Global Technical Support and R&D Center of TREND MICRO

TREND MICRO