Cibersegurança para redes de saúde na era da Transformação Digital

Inclui entrevista especial com Silvia Piai,
Diretora de Pesquisa do IDC Health Insights

IDC ANALYZE THE FUTURE

Folheto

Alcatel·Lucent Enterprise

Sumário executivo

Não é de hoje que a cibersegurança é uma prioridade para as organizações de saúde. No entanto, as exigências da cibersegurança estão mudando devido à transformação digital que está ocorrendo. A transformação digital significa que as organizações de saúde usam mais dispositivos conectados e móveis em suas redes, enquanto clínicos, parceiros e médicos acessam cada vez mais aplicativos e dados externos à rede. À medida que a mudança se acelera, os velhos métodos de segurança de rede já não conseguem acompanhar o ritmo.

Neste documento, Silvia Piai, diretora de pesquisa do International Data Corporation (IDC), compartilha percepções sobre as forças que estão mudando os requisitos de segurança cibernética na saúde, e recomenda estratégias que as organizações de saúde podem adotar e tecnologias que podem implantar para manter os dados e sistemas seguros na era da transformação digital. A Alcatel-Lucent Enterprise vai mostrar como sua solução Rede de Era Digital (DAN) atende às demandas de uma empresa transformada digitalmente. Com uma abordagem multifacetada à cibersegurança, a DAN mantém a confiança com acesso seguro e baseado em políticas aos dispositivos médicos conectados, dados de pacientes e aplicativos de software em todo o ecossistema de saúde.

A segurança cibernética na área da saúde atual

As organizações de saúde investiram **US$ 5,5 bilhões globalmente** em cibersegurança em 2019.

Em pesquisa do IDC, organizações de saúde relatam que a cibersegurança é uma prioridade máxima.[1] Isso não é surpreendente. A saúde tem sido, e continua sendo, uma das indústrias mais visadas pelos hackers. E o problema não para de crescer. Em 2018, o setor de saúde viu 15 milhões de registros de pacientes comprometidos em 503 violações, três vezes a quantidade observada em 2017, segundo o Protenus Breach Barometer.[2]

As violações ocorrem porque os dados de saúde são extremamente valiosos. Os registros individuais dos pacientes contêm tudo: incluindo nome, endereços atuais e anteriores, histórico de trabalho, nomes e idades dos parentes de um indivíduo e informações financeiras, como cartões de crédito e números bancários.[3]

Não só as violações da cibersegurança resultam em dados roubados, como também podem levar a interrupções operacionais, danos à reputação do hospital e multas por violações de regulamentos como a Lei de Portabilidade e Responsabilidade de Seguro de Saúde (HIPAA) dos Estados Unidos e o Regulamento Geral de Proteção de Dados (RGPD). Uma situação ainda pior é o potencial para os pacientes serem prejudicados. Por exemplo: uma bomba pode fornecer a quantidade errada de insulina. Ou a informação não pode ser entregue à equipe médica, durante o tratamento do paciente, deixando o médico desinformado sobre alergias ou outros medicamentos que o paciente está tomando.

O IDC estima que as organizações de saúde investiram US$ 5,5 bilhões globalmente em cibersegurança em 2019 para mitigar esses riscos. De hoje até 2022, o IDC projeta um crescimento anual composto de 8,7% nos gastos com cibersegurança na saúde, o que é semelhante ao montante gasto por outros setores.[4]

Apesar destes investimentos, continuam a existir lacunas de longa data na cibersegurança dos cuidados de saúde. Embora muitas organizações digam que a cibersegurança é uma prioridade, muitas vezes ela continua a ser uma preocupação posterior na prática diária. Afinal, hospitais e clínicas estão no negócio de curar pessoas, não de cibersegurança. Os médicos, além disso, podem resistir ativamente aos esforços para reforçar a cibersegurança se ela impedir o fluxo do trabalho clínico. Por exemplo, se médicos, enfermeiras e clínicos tiverem que perder muito tempo fazendo login e autenticação para acesso aos registros médicos eletrônicos ou ao sistema de registros de saúde (EMR/EHR), eles procurarão atalhos para economizar esse tempo precioso. Além disso, muitos clínicos simplesmente não possuem conhecimento suficiente das ameaças e impactos na cibersegurança.

1 Por exemplo: Prioridades, Estratégias e Investimentos: Superando os desafios do DX nos cuidados de saúde europeus https://www.idc.com/getdoc.jsp?containerId=EMEA44355219

2 https://healthitsecurity.com/news/the-10-biggest-healthcare-data-breaches-of-2019-so-far

3 https://www.forbes.com/sites/mariyayao/2017/04/14/your-electronic-medical-records-can-be-worth-1000-to-hackers/#2bb1f96b50cf

4 Guia IDC Semestral Mundial de Gastos com Segurança https://www.idc.com/getdoc.jsp?containerId=IDC_P33461

Ameaças à cibersegurança

Ao mesmo tempo, a natureza das ameaças de cibersegurança está mudando. Os hackers estão usando inteligência artificial (IA) e o machine learning (ML) para criar ataques mais sofisticados e automatizados. Novas técnicas de engenharia social permitem ao criminoso conectar poucas informações encontradas nas mídias sociais para criar perfis muito bons de indivíduos ou dos dados mantidos pelas organizações de saúde.

A transformação digital no setor de saúde está mudando ainda mais os requisitos de cibersegurança, resultando em maior complexidade, maior uso de dispositivos conectados, desaparecimento dos limites, e tudo isso a um ritmo acelerado.

Maior complexidade

As organizações de saúde estão adotando novas tecnologias, incluindo nuvem, mobile, IoT, Big Data, e análises avançadas. Estas novas soluções trazem um novo nível de complexidade que requer uma nova forma de olhar para a segurança.

Aumento do uso de dispositivos conectados

Até 2022, 97% dos enfermeiros, 98% dos médicos, 96% dos farmacêuticos e 94% dos enfermeiros da emergência estarão utilizando dispositivos móveis.[5] Como as organizações de saúde e os pacientes usam cada vez mais aparelhos móveis, IoT e dispositivos de saúde domiciliar como Fitbits, novas vulnerabilidades têm surgido.

Por exemplo, a primeira geração de dispositivos médicos conectados não necessitava de senhas. Por causa destes dispositivos conectados à rede, os hackers poderiam usá-los como um canal para a rede. Hoje em dia, a FDA e equivalentes europeus exigem recursos de segurança como senhas codificadas. No entanto as violações

Até 2022, 97% dos enfermeiros, 98% dos médicos, 96% dos farmacêuticos e 94% dos enfermeiros da emergência estarão usando dispositivos móveis.[2]

5 https://www.aiin.healthcare/topics/connected-care/over-90-nurses-physicians-will-use-mobile-devices-2022

permanecem inevitáveis e, quando elas ocorrem, os hackers ainda podem ganhar acesso a toda a rede. A pesquisa do IDC mostra que apenas 6% dos prestadores de serviços de saúde europeus têm uma estratégia de segurança de dispositivos médicos integrada em sua arquitetura de segurança empresarial e, preocupantemente, 16% ainda não começaram a avaliar as ameaças potenciais aos dispositivos médicos em rede.[6] De fato, palestrantes na Quinta Conferência sobre Segurança da Saúde Eletrônica da Agência Europeia de Segurança de Redes e Informações (ENISA) estimaram que houve um aumento de 600% nos ataques a dispositivos IoT, especificamente dispositivos médicos.[7]

Apenas 6% dos prestadores de cuidados de saúde europeus têm uma estratégia de segurança para os dispositivos médicos conectados.

As fronteiras estão desaparecendo

A maioria das organizações tem, há muito tempo, demarcado claramente o limite entre usuários e recursos dentro e fora da rede.

Contudo, à medida que as organizações de saúde abraçam a transformação digital, tornam-se mais abertas a trocas com o ecossistema mais amplo, incluindo pacientes, parceiros, pagadores, autoridades governamentais de saúde e outros provedores em um ambiente integrado de cuidados colaborativos. Os usuários já não acessam simplesmente os recursos de dentro do perímetro da rede - eles podem estar em qualquer lugar. Os cirurgiões podem trocar informações com os médicos do atendimento primário, em uma rede diferente. Os hospitais podem monitorar os pacientes remotamente, após a alta do hospital. Os médicos podem usar dados dos dispositivos pessoais de saúde dos pacientes, para ajudar no diagnóstico e cuidados.

Os recursos de TI também já não estão confinados ao perímetro da rede. Eles estão no local, na nuvem, e conectados através de APIs. As organizações de saúde precisam de formas modernas de proteger os recursos quando o perímetro já não existe.

Acelerando a taxa de mudança

Em um mundo transformado digitalmente, tudo se move mais rápido. As ferramentas de segurança devem lidar com esta velocidade.

6 Segurança da IoT nos Cuidados de Saúde Europeus https://www.idc.com/getdoc.jsp?containerId=EUR145549919

7 https://www.enisa.europa.eu/events/5th-ehealth-security-conference

Entrevista com Silvia Piai, Diretora de Pesquisa do IDC Health Insights

A Alcatel-Lucent Enterprise recentemente teve a oportunidade de conversar com Silvia Piai, Diretora de Pesquisa do IDC Health Insights, para obter as opiniões e recomendações do IDC sobre segurança cibernética na indústria da saúde.

IDC ANALYZE THE FUTURE

Recomendações do IDC para melhorar a cibersegurança nos cuidados de saúde

Apesar dos desafios emergentes, a abordagem da indústria da saúde à segurança continua a ser tradicional. As organizações de saúde muitas vezes implementam a segurança simplesmente para cumprir com requisitos básicos de conformidade, e não consideram as mudanças devidas à transformação digital, que impactam os requisitos de segurança.

O IDC recomenda que as organizações de saúde adotem uma abordagem holística da segurança das redes, que inclua estratégia, tecnologia, pessoas (por exemplo, formação) e processos (por exemplo, como a segurança está embutida nos fluxos de trabalho). Neste documento, vamos analisar a Estratégia e a Tecnologia.

Estratégia

Em vez de implementar a cibersegurança mínima para alcançar a conformidade, as organizações de saúde devem aproveitar a oportunidade para desenvolver um plano estratégico de segurança que gerencie o risco de forma que atenda às demandas do contexto atual de transformação digital. Elas devem:

- **Pensar na conformidade regulamentar como um ponto de partida.** Enquanto muitas organizações começam por fazer o mínimo necessário para cumprir o RGPD, ou outras regulamentações equivalentes fora da Europa, as organizações de saúde devem pensar na conformidade regulamentar como um ponto de partida para repensar a forma como estão gerenciando e governando os dados dentro das suas organizações e com os seus parceiros.
- **Entenda que a segurança impulsiona o valor do negócio**, assegurando a continuidade dos negócios. As organizações de saúde devem evitar a perda de receita (e reduzir as preocupações com a segurança dos pacientes) que resultam dos ciberataques que derrubam os sistemas de TI. Alinhe a segurança com os objetivos mais amplos da sua empresa, e faça dela uma parte das suas atividades diárias.

Siga uma abordagem de segurança por projeto: O risco anda de mãos dadas com os fluxos de trabalho dos negócios, que estão em constante evolução juntamente com as tecnologias. As organizações de saúde devem incorporar a segurança nos fluxos de trabalho desde o início. A segurança deve ser um valor central do negócio, e complementar todas as decisões empresariais das organizações de saúde.

- **Trabalhar com o ecossistema.** As organizações de saúde já não têm um perímetro claro a defender, uma vez que integram cuidados de outras organizações para os seus pacientes e parceiros. Elas precisam trabalhar com o ecossistema para manter a segurança cibernética.

Tecnologia

A criação de um ecossistema conectado e seguro torna-se primordial à medida que as organizações de saúde transformam digitalmente as suas operações. Este ecossistema requer uma abordagem estratificada que coloca os quatro pontos centrais da gestão de segurança -identidade, gestão de vulnerabilidades, gestão de ameaças e gestão da confiança - numa nova dimensão que permite escalabilidade, velocidade, inteligência e automação. Esta abordagem deve alinhar-se com o ambiente digital empresarial mais amplo e com os resultados que a organização pretende alcançar.

Os principais aspectos da tecnologia de segurança de rede em camadas devem incluir:

- **Segurança de endpoint**- para gerenciar vulnerabilidades de dispositivos individuais.
- **Gerenciamento de identidade** - para autenticar usuários e controlar o acesso. A solução deve fornecer recursos de autenticação do usuário e políticas de segurança de granulação fina, que concedam aos usuários o nível de acesso correto, apenas às informações de que precisam.

- **Troca segura de dados** - o uso de protocolos de criptografia e troca segura de arquivos deve proteger os dados em movimento.
- **Conteinerização** - para evitar que as ameaças pulem de um sistema para o outro, uma vez que uma ameaça tenha acesso à rede a solução deve utilizar a conteinerização e a segmentação da rede para isolar os sistemas individuais.
- **Gestão de confiança** - as organizações de saúde precisam de uma abordagem de gestão de risco que considere o fato de usuários e recursos poderem estar fora do perímetro da rede. Uma forma de estabelecer confiança em tal ambiente é compreender o que constitui um comportamento normal e anormal na rede. Ferramentas de Inteligência Artificial (IA) capacitadas para a gestão de identidade e autorização permitem estabelecer uma linha de base normal para o comportamento na rede. Estas ferramentas podem avaliar cada usuário e dispositivo e sua aplicação, segurança e requisitos de qualidade de serviço para estabelecer um comportamento normal de referência. Depois disso, a IA pode identificar rapidamente quaisquer eventos ou ações incomuns, tais como um sistema de vigilância que entre em contato com um EMR ou EHR, e análises que ajudam a determinar porque algo mudou.
- **Uma Arquitetura definida por Software** - uma solução de gerenciamento de rede automatizada pode fornecer a velocidade necessária para acompanhar a transformação digital.

A solução da Alcatel-Lucent Enterprise

A Rede da Era Digital (DAN) da Alcatel-Lucent Enterprise para o setor de saúde é uma abordagem multifacetada à cibersegurança das redes de saúde, que fornece segurança em profundidade para dispositivos e aplicativos médicos conectados através de várias camadas de segurança.

Conectividade flexível com uma rede definida por serviço

Nossa abordagem começa com uma Rede Definida por Serviço flexível, que torna rápido e fácil configurar políticas de rede e segurança cibernética para o vasto número de usuários conectados, dispositivos e aplicativos que alimentam a transformação digital.

No passado, a TI era uma operação de problema/correção. A TI instalaria novos equipamentos, colocaria em funcionamento e gerenciaria a rede usando processos manuais tediosos. A DAN é uma rede inteligente e automatizada que facilita a conexão de usuários e dispositivos às suas aplicações específicas, de forma segura. Projetada usando a tecnologia Alcatel-Lucent Enterprise Intelligent Fabric (iFab), a DAN inclui nossa intelligent fabric combinada ao padrão da indústria Shortest Path Bridging (SPB). Juntas, estas tecnologias simplificam a criação e configuração de redes, ao mesmo tempo que permitem o roteamento multicaminhos e a agregação de links para combinar múltiplas conexões de rede em paralelo e, assim, aumentar o rendimento e fornecer redundância.

Com a abordagem da ALE, a TI define os serviços de rede, arquitetura, políticas de acesso e contêineres, e a rede se constrói automaticamente. Uma vez que a rede é arquitetada, se algo é movido, alterado ou adicionado, a rede faz os ajustes necessários de forma automática e indetectável. Por exemplo, se um switch estiver fora de serviço, a rede irá se redirecionar automaticamente em torno desse switch.

Utilizando uma rede definida por serviço, as organizações de saúde beneficiam-se de automação, que reduz os erros de configuração manual e ajuda a acompanhar a taxa de mudança acelerada dentro das suas organizações. Como a automação elimina o trabalho manual, a TI se torna mais um motor de negócios.

Controle de acesso abrangente, com políticas inteligentes e automatizadas

Organizações de saúde podem usar a DAN para definir as regras e as políticas de acesso dos usuários, que gerenciam quais aplicativos e dispositivos os usuários podem acessar - e seguir os usuários onde eles forem. Por exemplo, podem estabelecer políticas que permitem:

- Aos médicos, acesso a todos os sistemas exceto aos sistemas financeiros
- Aos pacientes, acesso aos serviços de Internet
- Às empresas de saúde ou outros parceiros, uma política para sub-contratados

A ALE também oferece serviços baseados em localização, tais como navegação em ambientes fechados, rastreamento de ativos e pessoas que permitem às organizações de saúde estabelecer políticas que levam em conta a localização do usuário.

Os recursos de gerenciamento unificado de políticas aplicam as políticas automaticamente toda vez que um usuário se conecta, garantindo que os usuários tenham apenas os privilégios de acesso permitidos. Quando os usuários entram na rede com um PC/notebook/aparelho móvel e suas credenciais são validadas, eles não precisam continuar se autenticando. Permanecem conectados enquanto o dispositivo estiver ligado e o sistema aplicar automaticamente a política para esse usuário.

As políticas garantem que todos os usuários, dentro ou fora da organização, tenham acesso apenas às áreas permitidas e que esses controles de acesso sejam aplicados de forma consistente. Elas também descomplicam os fluxos do trabalho hospitalar, enquanto reforçam a segurança cibernética. Os médicos responsáveis por cuidar do paciente podem acessar rapidamente os sistemas e informações de que precisam, sem procedimentos onerosos de login de segurança.

Reduzida vulnerabilidade com a segmentação e a conteinerização

As organizações de saúde utilizam muitos dispositivos IoT, incluindo máquinas de RM, monitores de pacientes, bombas de infusão, robôs de distribuição de medicamentos, bem como câmaras de vídeo, sistemas de climatização, sistemas de sprinkler, sistemas de detecção de intrusão, e muitos outros. A solução DAN da ALE permite que as organizações de saúde façam a conteinerização de cada dispositivo, criando um segmento de rede virtual para evitar que qualquer dispositivo se torne um vetor de ataque. A conteinerização dentro da DAN faz múltiplas redes virtuais a partir de uma única rede física, que é gerida por um único sistema de gestão.

A implementação da conteinerização é simples para a TI. A solução DAN descobre

automaticamente cada dispositivo na rede. Quando um dispositivo é conectado à rede, o sistema de gerenciamento de rede Alcatel-Lucent OmniVista® 2500, disponível localmente ou na nuvem, tenta identificar esse dispositivo. Se o sistema de gerenciamento não tiver o dispositivo em seu banco de dados, ele consultará um banco de dados na nuvem que contém mais de 17 milhões de dispositivos.

Uma vez identificado o dispositivo, o sistema irá classificá-lo, por exemplo, como uma câmera de segurança. Se esse dispositivo estiver na lista de fornecedores aprovados para câmeras de segurança, ele será adicionado à rede. Se não, então ele não será conectado. A solução é então configurada num ambiente (contêiner) virtual para o dispositivo, separando-o do resto da rede. Se alguém invadir qualquer dispositivo da rede, esse hacker não poderá usar esse dispositivo para acessar o resto da rede.

Melhoria da confiança graças à Inteligência Artificial

Uma vez conectados, os dispositivos devem ser monitorados continuamente para identificar quaisquer ameaças e manter a confiança. A análise e a visibilidade da aplicação da ALE permitem aos administradores ver o que se passa na rede, por dispositivo. A análise identifica padrões para o comportamento normal e esperado da rede, bem como quaisquer padrões incomuns quando eles ocorrem. Podemos observar o comportamento dos aplicativos na borda da rede para decidir se devemos conectar a uma aplicação, bem como o comportamento incomum em aplicações autorizadas, como uma câmera de vídeo que está produzindo mais dados do que deveria.

Se uma anomalia ou comportamento incomum ocorrer no dispositivo, a análise mostrará esses dados para que o gerente de segurança da rede possa intervir. Hoje, a investigação deve ser feita manualmente, mas a ALE está trabalhando na automatização da resposta usando AI e ML.

Os recursos de IA também suportam serviços para pacientes remotos. A ALE está desenvolvendo equipamentos que permitem aos hospitais monitorar remotamente os pacientes em suas casas, enquanto eles se recuperam de uma enfermidade ou cirurgia. O equipamento precisa transmitir com segurança os dados do dispositivo para o hospital. A IA pode monitorar a atividade de dispositivos IoT remotos para

garantir que seu comportamento seja consistente com o comportamento esperado. Além disso, os pacientes estão usando cada vez mais aplicativos para monitorar sua saúde. Se um médico puder monitorar um Apple Watch® ou outro dispositivo de monitoramento usado por um paciente, ele pode melhorar o engajamento com o paciente e fazer melhores diagnósticos. Com a ALE AI, as organizações de saúde terão mais visibilidade se uma aplicação ou atividade dentro dela pode ser confiável.

Um equipamento de rede seguro reduz as vulnerabilidades

As organizações de saúde de hoje estão cientes da necessidade de proteger os dispositivos IoT na rede. Mas elas podem falhar em considerar dispositivos que formam a base da rede, tais como switches e pontos de acesso (APs).

A ALE emprega muitas tecnologias para reduzir a ameaça dos dispositivos. Nossas soluções:

- Fortalecem o sistema operacional para fornecer código seguro e diversificado
- Enviam o software do sistema operacional para verificação e validação por terceiros para garantir que não tenha pontos de entrada ou backdoors fáceis
- Garantem que, toda vez que um switch seja inicializado, a memória seja compilada e ativada de uma maneira diferente. Embora os switches funcionem de forma idêntica, não há dois deles com a mesma configuração de memória internamente. Se alguém fosse violar um dos nossos switches, não poderia acessar outro switch da mesma maneira.
- Proporcionam proteção integrada contra negação de serviço (DoS). Nossa CPU pode detectar quantidades incomuns de tráfego na rede e desligar automaticamente a CPU, se necessário.
- Completar múltiplas certificações de segurança, como JDIC e FIPS
- Realizar atualizações contínuas de software.

Conexões seguras para o tráfego de entrada e saída

Para o tráfego de entrada, nossos recursos de VPN fornecem uma conexão criptografada à rede local, enquanto o tráfego de ponta a ponta é protegido usando a criptografia MACsec (também conhecida como IEEE 802.1AE) para proteger a informação enquanto ela atravessa a rede.

Relatórios

Os relatórios da ALE permitem que usuários diferentes tenham acesso a informações sobre o status, saúde e desempenho da rede, como as aplicações estão sendo executadas e a satisfação do usuário. Por exemplo, a TI pode ver dados sobre o desempenho e as operações da rede. As unidades de negócios podem garantir que equipamentos como sistemas de imagem (ressonância magnética, raio-X) estejam transmitindo dados para servidores e tablets sem problemas. Os CXOs podem determinar se a rede está fornecendo serviços que permitem aos médicos passar mais tempo com os paciente, e se eles estão tirando o máximo proveito da rede.

Conclusão

A transformação digital mudou profundamente os requisitos de segurança cibernética dos hospitais. Conforme o número de dispositivos conectados aumenta, o perímetro da rede desaparece e as mudanças continuam aceleradas. A solução Alcatel-Lucent Enterprise Digital Age Networking para a Saúde mantém seus ativos de TI e os dados dos pacientes seguros na era atual da Transformação Digital. Através dessa solução, você pode gerenciar de perto o acesso do usuário, reduzir vulnerabilidades criadas pelo IoT, dispositivos móveis e de rede, evitar que a violação inevitável forneça um vetor de ataque e se comunique em todo o ecossistema de saúde a partir de uma posição de confiança.

Alcatel-Lucent Enterprise

Somos a ALE. Podemos ajudar você a conectar seus pacientes, sua equipe e seu ecossistema de saúde. Proporcionando uma tecnologia que funciona em todas as suas instalações e além delas.

www.al-enterprise.com/en/industries/healthcare

DID20021001PTBR (maio de 2021)

Alcatel·Lucent
Enterprise