ARTIGO

Cibersegurança para provedoras de serviços de saúde

Introdução

Para competir em um mercado que muda rapidamente, as organizações provedoras de serviços de saúde adotam novos dispositivos e aplicações para oferecer atendimento premium ao paciente e experiências de alto nível. Cada nova adição traz seus próprios benefícios para os pacientes e seu próprio conjunto de riscos de segurança para a organização.

Esse ambiente de TI complexo, combinado com o alto valor das PHI (informações de saúde protegidas), cria uma oportunidade irresistível para os cibercriminosos, que continuam a destruir sistemas. De acordo com um relatório do Departamento de saúde e serviços humanos dos EUA e pesquisa feita pela IBM, desde o início da pandemia, o setor de serviços de saúde registrou um aumento de 50% nos ataques cibernéticos, que foram os mais caros, com um custo médio de US$ 7,13 milhões por incidente. Esse relatório da IBM destacou que os ataques de ransomware foram a ameaça mais frequente, pois os agentes mal-intencionados visaram a necessidade de recuperação rápida dos sistemas de hospitais e de serviços de saúde, seguidos de roubo de dados e acesso ao servidor. Os provedores de serviços de saúde, em particular, são alvos atraentes de ransomware porque os EHRs (prontuários eletrônicos) podem chegar a US$ 1.000 na Dark Web, em comparação com aproximadamente US$ 110 para informações de cartão de crédito e mero US$ 1 para cada número de previdência social.

Com um número cada vez maior de ameaças contra seus sistemas, muitas organizações não estão adequadamente preparadas para mitigá-las. Pior ainda, algumas já sofreram infiltrações e não sabem disso. Os agentes de ameaça podem já estar exfiltrando dados ou aguardando o momento certo para atacar.

Agora é a hora de esclarecer a superfície de ataque da sua organização fazendo um inventário dos dispositivos e entendendo como eles se conectam à sua infraestrutura. Com um melhor conhecimento de onde existem vulnerabilidades, colocar em prática um plano sólido de mitigação impedirá ou minimizará o possível impacto dos ataques cibernéticos.

Como cobrir os maiores riscos de cibersegurança para sua organização

Ameaça nº 1: ataques de phishing

Phishing é um dos vetores de ataque cibernético mais comuns em todos os setores. De acordo com o Centro de coordenação de cibersegurança do setor de saúde, 2021 trouxe um aumento significativo nos ataques de phishing ao setor de serviços de saúde. Ao longo de 2020, a Akamai observou que os criminosos aproveitaram a COVID-19 e a promessa de assistência financeira ou o estresse das dificuldades financeiras para atingir pessoas em todo o mundo por meio de phishing.

O phishing tenta adquirir dados confidenciais por meio de e-mails ou páginas da Web fraudulentos. Quando bem-sucedido, faz com que um usuário insira suas credenciais de login por engano, dando aos autores de ataques uma porta aberta para a rede.

Isso aconteceu com aqueles que solicitaram auxílio desemprego em Nova Iorque. De acordo com um relatório de phishing de Steve Ragan, ex-editor da CSO Online e atual pesquisador de segurança da Akamai, houve vários kits de phishing que visaram programas de PUA (assistência ao desemprego pandêmico) no início de 2021. Esses são programas que tinham como objetivo ajudar aqueles que precisavam de ajuda durante os lockdowns da COVID-19 e que prestaram serviços essenciais para milhões de americanos.

Em uma reportagem na CBS News veiculada em todo o país, Ragan falou sobre um kit de phishing de desemprego direcionado a pessoas em Nova Iorque e sobre como os criminosos estavam coletando e vendendo informações pessoais comprometidas no golpe. Desde que a notícia foi transmitida, ele descobriu golpes de PUA direcionados a pessoas em Wisconsin, Indiana, Pensilvânia e Massachusetts.

Como interromper e mitigar ataques de phishing

Dependendo das configurações de permissão e das proteções de segurança existentes, obter acesso a uma única conta de usuário pode potencialmente fornecer aos criminosos acesso livre a partes críticas de sua rede, e eles podem, muitas vezes, expandir seu alcance uma vez dentro da rede de sua organização.

A microssegmentação limita o acesso dos agentes de ameaça apenas à parte da sua rede à qual eles inicialmente obtêm acesso, evitando que eles se movam lateralmente e tirando sua capacidade de causar mais danos em áreas adicionais. Ela limita o impacto de um comprometimento, impedindo que criminosos usem qualquer ponto de entrada para acessar a rede de sua organização de forma mais ampla.

Além da microssegmentação, a MFA (autenticação multifator) é uma das melhores linhas de defesa contra ataques de phishing. Ela fornece uma camada adicional de proteção, exigindo uma verificação de identidade adicional antes de permitir o acesso a uma conta, o que impede que credenciais comprometidas sejam exploradas.

A MFA, especialmente uma solução aprovada para FIDO2, garante a proteção contra os ataques mais recentes e requer que os usuários insiram um código exclusivo que seja gerado por meio de um texto ou app de autenticação no dispositivo móvel do usuário. Essa etapa adicional de login ajuda a impedir ataques de phishing, mesmo quando os criminosos têm credenciais de login precisas.

É fundamental educar sua equipe sobre as táticas de ataques de engenharia social, como phishing. A realidade é que o phishing é um dos problemas que não tem uma correção miraculosa, porque há realmente muitas partes móveis. É difícil prever o que os criminosos farão em seguida. Como os seres humanos ainda são um aspecto vital no phishing, eles continuarão a ser o elo mais fraco da cadeia.

Isso significa que tornar a segurança fácil é essencial. A Akamai oferece uma solução de MFA sem atritos e à prova de phishing para proteger até mesmo contra os cibercriminosos mais inteligentes.

Ameaça nº 2: software legado não suportado

O software desatualizado é outra preocupação de vulnerabilidade significativa. Cada nova atualização de segurança (patch) que não é instalada imediatamente cria backdoors abertos em sua rede. Isso acontece especialmente em dispositivos mais antigos que envelhecem sem suporte e não recebem mais atualizações.

Softwares não suportados podem ter vulnerabilidades de dia zero que as organizações podem hesitar em corrigir por conta própria. Criar um patch personalizado pode, às vezes, anular a garantia de um dispositivo, levando a reparos dispendiosos quando algo dá errado.

Embora os dispositivos médicos tenham um ciclo de vida longo, se não forem atualizados assiduamente com a versão mais recente do sistema operacional, ou estiverem executando um sistema operacional não suportado, os hackers podem explorar vulnerabilidades para roubar dados, infiltrar-se em uma rede hospitalar e interromper o atendimento. Na verdade, até 83% dos dispositivos de imagens médicas conectados à Internet, de máquinas de mamografia a aparelhos de ressonância magnética, são vulneráveis, conforme relatado pela Fortune.

Quanto mais antigo for um dispositivo, especialmente aqueles que estão além do ciclo de vida de manutenção, maior a probabilidade de que os criminosos saibam os pontos fracos que lhes permitem acessar a rede da sua organização por meio de um dispositivo de terceiros.

Por exemplo, o Windows 95 está fora de manutenção há anos e, ainda assim, muitos aparelhos de ressonância magnética (entre outros) ainda dependem desse sistema operacional, pois ele foi o último a permitir a escrita direta. Os desenvolvedores internos podem ser capazes de corrigir uma vulnerabilidade, mas seu patch pode anular a garantia do equipamento. A única opção segura é substituir totalmente o aparelho de ressonância magnética, mas isso é um custo proibitivo para muitas instalações.

Os administradores de rede tentam manter os sistemas sem suporte fora da rede, mas isso nem sempre é possível, especialmente quando os dispositivos são necessários para o atendimento ao paciente e precisam fornecer dados rapidamente aos médicos. O isolamento também falha quando há um mapa incompleto de todos os dispositivos conectados à rede, criando backdoors. É difícil proteger o que não se pode ver.

Como proteger dispositivos vulneráveis e não suportados

Para proteger esses dispositivos de fornecer acesso à rede da sua organização, é fundamental migrar para uma arquitetura ZTNA (Zero Trust Network Access). ZTNA é uma estrutura que trata todas as solicitações recebidas como uma ameaça potencial até que seja comprovadamente segura, interrompendo efetivamente os invasores antes que eles obtenham acesso ao dispositivo, mesmo que seu software esteja desatualizado.

Avançar para uma ZTNA marca uma mudança fundamental da abordagem de "castelo e fosso" dos anos passados para um modelo Zero Trust (verificar e depois confiar). Embora uma abordagem Zero Trust provavelmente não proteja totalmente contra ataques cibernéticos, ela limita os possíveis danos de catastróficos a gerenciáveis. A HealthITSecurity articula da melhor forma: "Se um invasor conseguir credenciais e manipular um dispositivo, é improvável que ele vá muito mais longe com uma arquitetura Zero Trust."

A Akamai oferece um plano robusto para ajudar os provedores a migrar para uma arquitetura Zero Trust, sem o tempo de inatividade e a flexibilidade dos fluxos de trabalho atuais. Comece agora com a ZTNA com este guia de esquema.

Ameaça nº 3: provedores que trabalham em casa e BYOD (Traga seu Próprio Dispositivo)

A continuidade do atendimento médico no século XXI é descentralizada. Os pacientes recebem atendimento do conforto de suas casas. Os provedores fornecem atendimento por meio de seus dispositivos móveis em vez de pessoalmente. Mas esse aumento na acessibilidade significa que os provedores estão observando os riscos de cibersegurança se agravarem drasticamente à medida que os membros da equipe oscilam entre acessar redes no local e em casa, e fazem login usando dispositivos não gerenciados.

Embora os membros da sua equipe pudessem fazer login ocasionalmente em seu sistema a partir da rede doméstica antes da pandemia, o aumento do volume de dispositivos pessoais que acessam a rede da sua organização inevitavelmente aumentou durante esse período. Se esses notebooks, tablets ou smartphones fossem infectados com malware, eles poderiam se tornar um ponto de entrada para um ataque de ransomware.

Por exemplo, se alguém de sua equipe for vítima de um ataque de phishing inserindo acidentalmente suas credenciais de login em uma página da Web falsa, os agentes mal-intencionados terão o mesmo acesso que o usuário tem, permitindo que criptografem arquivos, bloqueiem sua equipe e prejudiquem sua organização exigindo um resgate considerável para descriptografar os arquivos.

Como proteger a edge da sua rede

Monitorando de perto quem está acessando a rede da sua organização (onde está, qual é o endereço IP, qual dispositivo está usando etc.), você pode minimizar a probabilidade de ocorrer uma situação como essa e trabalhar para interromper um ataque antes que ele aconteça.

Se sua equipe usa dispositivos pessoais ou trabalha em casa, faça a si mesmo as seguintes perguntas:

- Temos uma abordagem ZTNA (Zero Trust Network Access) em vigor para maximizar a análise de solicitações recebidas e interromper um ataque antes que ele ocorra?
- Estabelecemos microssegmentação para limitar o acesso e evitar movimentos laterais caso um criminoso consiga entrar na rede da organização?
- Estamos usando uma estrutura SASE (Secure Access Service Edge) para proteger nossa rede e, ao mesmo tempo, minimizar a latência e manter uma experiência de usuário rápida e agradável?
- Nossa equipe está usando códigos de acesso, senhas fortes e exclusivas e MFA (autenticação multifator) para cada login de dispositivo e conta?

A Akamai ajuda a facilitar o gerenciamento de acesso à rede com nossas soluções remotas de segurança da força de trabalho.

Ameaça nº 4: mapeamento fraco do fluxo de dados

Com um pé no local e o outro na nuvem, pode ser quase impossível entender onde seus dados vivem e como eles fluem. Isso acontece por algumas razões diferentes.

Primeiro, volume. Pode ser difícil acompanhar o número de dispositivos e aplicações que estão sendo adicionados e removidos de sua rede diariamente, se não de hora em hora, já que fornecedores, prestadores de serviços e consultores parecem usar diferentes dispositivos, ferramentas e soluções.

Em segundo lugar, o sistema de rastreamento de hardware e software se tornou obsoleto e não é mais preciso ou confiável devido à rotatividade de membros da equipe, mudanças de processo ou prioridades concorrentes.

Independentemente do motivo, é importante visualizar a rede e os dispositivos conectados, pois não é possível proteger o que não se vê.

Como mapear o fluxo de seus dispositivos conectados

É fundamental ter uma ferramenta de visibilidade que possa criar um mapa de dispositivos conectados. Especialmente desde que um artigo de 2019 no HIPAA Journal citou que 82% das organizações de serviços de saúde tiveram um ataque cibernético em seus dispositivos conectados nos 12 meses anteriores.

A primeira etapa no mapeamento de seus dispositivos conectados é a escolha de uma solução que controle o fluxo de dados em toda a rede, informando de onde ele está vindo e para onde está indo, incluindo dispositivos que não estão conectados à sua rede. Isso permite que você tenha um diagrama de rede em tempo real de onde as informações estão fluindo e ajuda a descobrir dispositivos mal-intencionados que podem estar em sua rede. Ao colocar anéis de microssegmentação definidos por software em torno de sistemas principais, ativos e dados (como PHI), sua organização pode limitar o movimento lateral que os invasores têm dentro de sua rede. Obtenha a visibilidade de que você precisa com as ferramentas de microssegmentação da Akamai.

Ameaça nº 5: gerenciamento da complexidade de redes, apps e sistemas

Você sabe quais aplicações e softwares podem ler seus dados? Alguns softwares, como plataformas de mídia social, declaram claramente sua capacidade invasiva na declaração de privacidade ou termos de serviço. Outras, como os provedores de e-mail, são mais discretas, mas ainda representam um risco significativo (por exemplo, ter acesso às fotos de um dispositivo quando as fotos contêm PHI).

As aplicações também podem ter permissão para visualizar itens copiados para a área de transferência, incluindo identificadores de pacientes ou senhas. Se houver informações do paciente em um dispositivo, há a probabilidade de que um terceiro (ou invasor) as veja (e as registre).

Eduque sua equipe, visualize toda a sua rede, proteja sua edge

É fundamental que você eduque todos na organização do seu provedor sobre os riscos de usar dispositivos pessoais e o que é necessário para proteger as informações privadas dos pacientes.

Também é importante considerar a visão que sua organização tem de sua superfície de ataque e de possíveis vetores. Sua equipe de segurança está monitorando toda a rede em vários provedores de serviços em nuvem e data centers locais? Ou eles estão isolados em vários grupos focados em diferentes aspectos da infraestrutura da sua organização? É imprescindível manter uma visão holística de toda a rede da organização e de sua atividade, especialmente durante um ataque.

Semelhante à ameaça nº 4, suas melhores opções de defesa para proteger a edge da rede é uma arquitetura Zero Trust combinada com microssegmentação e MFA para logins de contas. Utilizar um provedor para proteger todos os sistemas, independentemente de quem os possui e se estão na nuvem ou no local, permite que você proteja sua rede sem prejudicar a experiência do usuário.

Qual é o impacto da falta de ação?

Os custos podem ocorrer de muitas formas. O mais óbvio é financeiro, com as empresas de saúde dos EUA registrando em média US$ 9,23 milhões em custos totais associados a uma única violação de dados, de acordo com o Relatório da IBM sobre o custo de uma violação de dados 2021. Outros custos são mais qualitativos, como a segurança e a confiança dos pacientes, que podem ter um impacto igual, se não maior, sobre as organizações de saúde.

Menor segurança do paciente

A segurança do paciente é o alvo mais significativo quando se trata de cibersegurança. Quando os sistemas de TI são forçados a desligar por causa de um ataque, o atendimento ao paciente é interrompido. Os tratamentos e consultas são adiados e podem resultar em desfechos adversos de saúde para os pacientes. Na verdade, uma ação judicial recente marcou a primeira alegação de morte de um paciente resultante diretamente de um ataque de ransomware.

Enquanto isso, os dispositivos médicos conectados usados para o monitoramento remoto do paciente (por exemplo, frequência cardíaca ou níveis de glicose) representam uma ameaça mais direta ao tratamento. Por exemplo, interromper as leituras de pressão arterial de um paciente pode fazer com que condições perigosas sejam despercebidas e não tratadas, causando potencialmente um evento sentinela.

Perda de confiança do paciente

A incapacidade de fornecer cuidados confiáveis e de proteger as informações do paciente leva a uma perda de confiança do paciente. Mais de 90% dos pacientes dizem que trocariam de provedor se suas informações privadas fossem comprometidas em uma violação de dados. O número real pode ser menor quando chegar a hora, mas faça as contas: Mesmo que apenas metade desses pacientes fosse embora, ou um décimo deles, qual impacto isso teria na população de pacientes? E quanto tempo você incorreria em perdas contínuas enquanto adquire gradualmente novos pacientes?

Perda de receitas

Em 38%, a perda de negócios é o maior fator de custo associado a uma violação de dados. Quando os principais sistemas de provedores ficam inativos (como EHRs, servidores de e-mail etc.), os negócios que chegam ficam paralisados. Isso significa que não há consultas, visitas, encontros e receita (sem mencionar o impacto que isso tem no atendimento ao paciente).

A Scripps Health, sediada em San Diego, sofreu um grande ataque cibernético em maio de 2020, que resultou em US$ 91,6 milhões de perda de receita, principalmente devido à redução do volume de atendimento do departamento de emergência e das cirurgias eletivas.

Mesmo que algumas partes da rede do sistema de saúde ainda estejam operacionais, não é possível ter certeza de que tudo está seguro até que você localize o vetor, corrija a vulnerabilidade e conclua a análise forense.

Aumento de sobrecarga

O recrutamento, a contratação e a retenção de cobiçados engenheiros de cibersegurança são caros, mas os custos reais vão muito além disso. A contratação de uma equipe de cibersegurança interna em sua organização pode deixar você com lacunas dispendiosas na cobertura.

Em termos gerais, quanto mais tempo for necessário para a sua organização identificar e exfiltrar um invasor da sua rede, maiores serão os custos. Um relatório do Ponemon Institute afirma que a detecção de um ataque cibernético nos primeiros 200 dias pode permitir uma economia de mais de US$ 1,26 milhão a uma organização. Infelizmente, de acordo com o mesmo relatório, o ataque médio leva 287 dias para ser identificado e contido. *287 dias!* Isso significa que os agentes de ameaça estão frequentemente dentro da infraestrutura de rede por mais de nove meses, traçando e planejando seu ataque para causar danos máximos à reputação e aos resultados do seu hospital.

É essencial quantificar o tempo que sua equipe de segurança precisa para identificar e tomar medidas contra um ataque. A consolidação de fornecedores de segurança para aqueles que oferecem serviços gerenciados e suporte de engenharia para aumentos repentinos de equipe pode representar uma economia significativa de custos.

Multas regulatórias

Com tantas informações pessoais valiosas sob sua responsabilidade, uma violação de dados pode levar a multas pesadas de órgãos reguladores. Em 30 de novembro de 2021, o gabinete de direitos civis (Office of Civil Rights) do Departamento de Saúde e Serviços Humanos dos Estados Unidos (Department of Health and Human Services) estabeleceu ou impôs penalidades contra 106 entidades cobertas pela HIPAA, totalizando mais de US$ 131 milhões. Isso representa uma média de mais de US$ 1,2 milhão por penalidade (além dos custos adicionais mencionados aqui).

Como preparar melhor sua organização de serviços de saúde para um ataque cibernético

As atuais ciberameaças exigem que as organizações provedoras tenham segurança líder do setor. Seus pacientes e seus negócios dependem disso; o custo da inércia é muito alto.

Restrições financeiras, prioridades concorrentes ou incerteza dos riscos podem levar você a assumir riscos em excesso. Mas seus esforços de segurança devem ser minuciosos, estratégicos, vigilantes e ágeis.

Um ecossistema adequadamente protegido hoje não está necessariamente protegido amanhã. As ameaças evoluem rapidamente. Um dia (ou menos) pode ser tudo o que é necessário para que os invasores explorem uma nova vulnerabilidade.

Os provedores que buscam reduzir essa superfície de ameaça e seguir o conselho da abordagem de backup descrita no comunicado federal (salvando três cópias em pelo menos dois formatos diferentes, com uma offline) estão cada vez mais adotando uma abordagem híbrida. O armazenamento de dados local fornece maior controle sobre a segurança, mas pode ser caro e difícil de expandir rapidamente, especialmente com o aumento exponencial dos dados de saúde e a transformação digital na assistência médica, ambos impulsionados pela pandemia. O armazenamento de dados em nuvem pública é mais econômico, mas as organizações correm o risco de interrupções e de falta de transparência na forma como os dados são protegidos.

Uma abordagem híbrida permite que dados confidenciais sejam mantidos no local, enquanto dados menos confidenciais são armazenados na nuvem. Mesmo isso não é perfeito, pois a segurança deve ser colocada em vigor para proteger a transferência de dados entre os dois tipos de armazenamento e garantir que o acesso seja limitado àqueles que estão autorizados a fazer as transferências e visualizar os dados. Avançar para os sete principais requisitos para implementar uma arquitetura ZTNA ajuda as instituições a proteger seus dados por meio da concessão aos usuários de acesso apenas às aplicações de que precisam para sua função, com segurança adicional oferecida pela MFA.

A Akamai está aqui para ajudar você a se preparar para quando, e não se, um ataque ocorrer. Vamos trabalhar juntos para criar uma visão coesa da sua rede para identificar rapidamente um ataque e mitigar os danos de forma eficiente. Nossa empresa foi criada para proteger as redes contra ataques distribuídos de negação de serviço e ransomware para oferecer experiências da Web seguras e perfeitas (incluindo aplicações e APIs).

Fortalecemos a edge de sua rede para limitar suas chances de violação e para reduzir o raio de ataque quando uma violação ocorre. E nós fazemos isso mantendo a flexibilidade para o acesso dos usuários, para que sua organização possa se concentrar em fornecer resultados de saúde ideais em meio a demandas operacionais e de cuidados em constante mudança.

Nunca foi tão importante proteger as informações de seus pacientes contra a crescente sofisticação dos cibercriminosos e superfícies de ataque baseadas em nuvem em expansão. Organizações e entidades governamentais centradas no paciente confiam na plataforma de edge da Akamai para manter suas experiências digitais mais próximas dos pacientes e as ameaças mais distantes.

Confie na Akamai, a parceira que transformará a cibersegurança de um fardo perpétuo em uma força competitiva.

Entre em contato conosco para saber mais ou ligue para +1-877-425-2624.