RESUMO EXECUTIVO

Os Desafios Transformadores e a Complexidade da Cibersegurança para os Serviços de Saúde

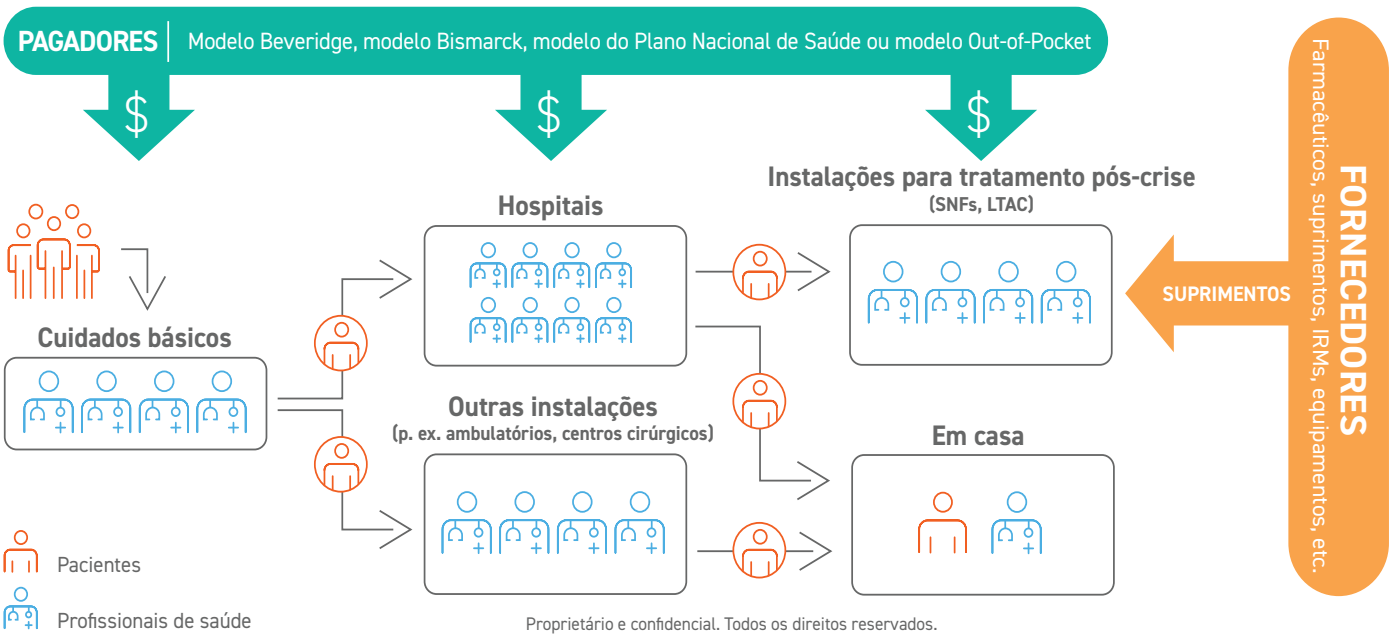
As quatro questões críticas de segurança cibernética que afetam os serviços de saúde atualmente.

Resumo

Desde o surgimento da Covid-19, as organizações de serviços de saúde (*Healthcare Delivery Organizations* – HDO) têm alternado e expandido sua projeção tecnológica. Esse crescimento tem sido uma reação ao rápido surgimento de serviços de saúde on-line, o fluxo de profissionais trabalhando remotamente, mudanças para gestão de dados e operações comerciais em nuvens, e a proliferação de dispositivos de monitoramento de pacientes conectados a redes. Embora essa tecnologia tenha permitido a esses profissionais prestar serviços de qualidade presencialmente, virtualmente ou em domicílio, onde quer que estejam, ela também criou - ou aumentou - o número de desafios de segurança cibernética. Este resumo examina os desafios transformadores e as complexidades da segurança cibernética no setor da saúde, que são compartilhados em todo o setor de serviços de saúde globalmente.

Introdução

Os interesses em serviços de saúde são expressivos, com novas tecnologias e aplicações médicas que afetam o bem-estar e a segurança de pacientes durante toda a sua jornada de tratamento e cuidados.



Os efeitos em cascata de ataques cibernéticos bem-sucedidos sobre a infraestrutura e os registros eletrônicos essenciais dos serviços de saúde (RES) podem afetar o tratamento dos pacientes de formas assustadoras:

- Os pacientes não terão o tratamento necessário se os serviços de saúde ficarem off-line devido a um ataque de ransomware ou DDoS.
- Cirurgiões adiam cirurgias porque as informações necessárias para realizar uma cirurgia que pode salvar uma vida se torna inacessível.
- Falhas em procedimentos de diagnóstico e exames laboratoriais resultam em atrasos no tratamento médico.
- A evasão nas unidades de pronto-socorro (PS) fazem com que as ambulâncias desviem sua rota para instalações clínicas a quilômetros de distância, causando resultados degradados e irreversíveis.

As PHI são mais importantes na *dark web*

Hospitais e outras HDO continuam sendo um dos alvos mais visados para ataques cibernéticos internos e externos, uma vez que as informações de saúde protegidas (*Protected Health Information* – PHI) têm alta demanda na *dark web*. Consequentemente, as PHI muitas vezes podem ser vendidas a preços mais altos do que outras informações de identificação pessoal (*Personal Identifiable Information* - PII).

Por exemplo, números de cartões de crédito roubados são desativados e substituídos assim que houver suspeita de gastos indevidos, o que reduz seu valor no mercado. Ao contrário, prontuários médicos têm uma valorização mais alta, pois são conjuntos de dados imutáveis que não podem ser alterados ou apagados facilmente. Desta forma, os criminosos cibernéticos podem se beneficiar continuamente, enquanto os pacientes afetados sofrem as consequências financeiras e emocionais e são obrigados a se empenhar em reparar os danos de atividades fraudulentas. Alguns exemplos são a compra de receitas médicas, o recebimento de tratamentos, a apresentação de alegações médicas falsas, ou a obtenção de empréstimos pessoais ou cartões de crédito utilizando registros médicos roubados de pacientes.

Os problemas com ransomware persistem

Os responsáveis pelas ameaças continuam encontrando meios de explorar as fraquezas que os centros de operações de segurança (*Security Operating Centers* - SOC) ainda não trataram ou identificaram, uma vez que as abordagens avançadas dos invasores continuam superando os investimentos no fortalecimento dos controles de segurança. Por exemplo, os criminosos cibernéticos buscam ativamente vulnerabilidades não solucionadas, como o Log4j, como o principal vetor de ataques e lançamentos de ataques de ransomware. O resultado é que o ransomware é considerado a ameaça mais significativa para o setor de saúde.

Essa tendência provavelmente continuará durante o ano de 2022, pois 42%[1] das HDOs já sofreram ataques de ransomware nos últimos dois anos. Além disso, mais de 36%[2] desses incidentes ocorreram via terceiros, como no caso dos ataques a cadeias de suprimentos, amplamente divulgados, contra softwares de gestão de infraestruturas críticas vulneráveis.

As vulnerabilidades dos servidores de rede por trás da maior parte dos incidentes de violação de dados

O setor teve o pior ano em termos de violação de dados em 2021, quando um número recorde de violações de dados ocorreu e prontuários com PHI foram expostos. Por exemplo, a secretaria de direitos civis dos EUA (*Office for Civil Rights* - OCR), no âmbito do departamento de serviços humanos e de saúde (*Health and Human Services* - HHS) relatou que mais de 700 (Figura 1) entidades abrangidas foram violadas, resultando em roubos, perdas ou divulgação de mais de 42 milhões de prontuários pessoais com PHI (Figura 2). Incidentes[3] relatados recentemente revelam que as violações e vulnerabilidades já apresentam números preocupantes em 2022 (Figura 3).

Figura 1
Violação de dados nos serviços de saúde com 500 ou mais prontuários

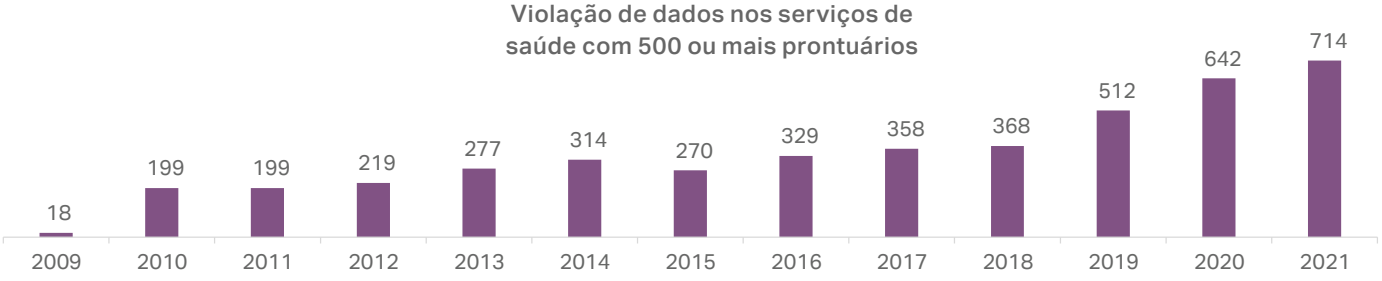
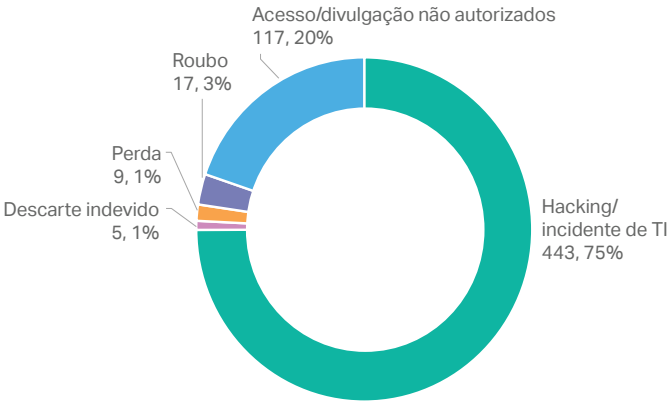


Figura 2

Departamento de Saúde e Secretaria de Serviços Humanos para Direitos Civis dos EUA, Violações de Dados Relatadas em 2021
Total: 5



Departamento de Saúde e Secretaria de Serviços Humanos para Direitos Civis dos EUA, Pessoas Afetadas em 2021

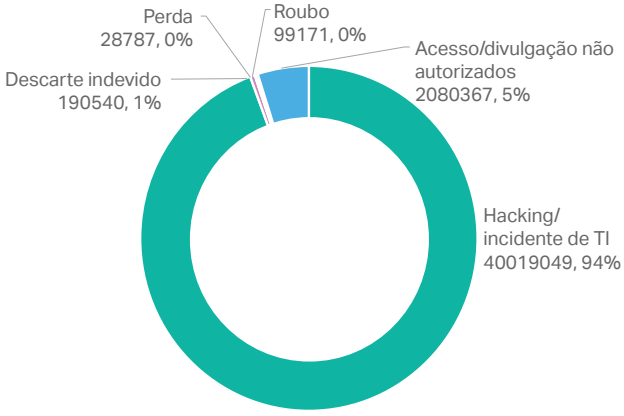
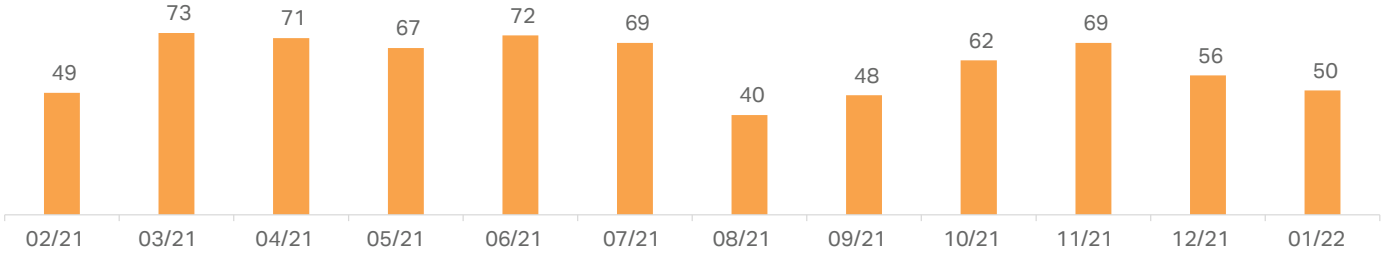
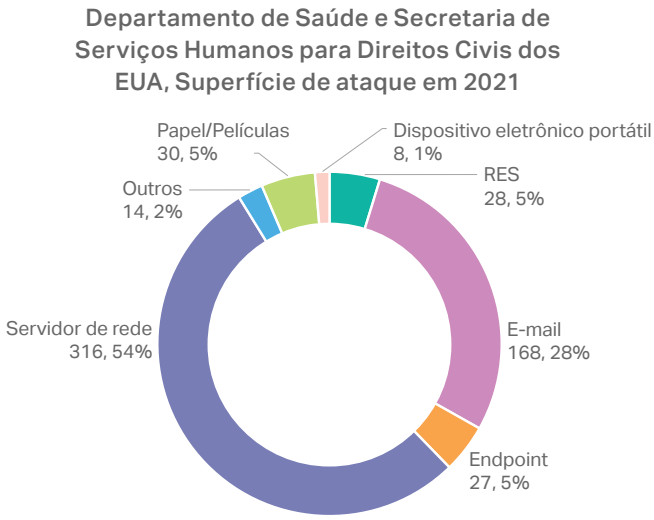


Figura 3
Violações de dados nos serviços de saúde nos últimos 12 meses nos EUA



As dez principais violações de dados de saúde relatadas em 2021 foram todas atribuídas a invasões bem-sucedidas de hackers, sendo sua gravidade medida pelo número de pessoas afetadas. 90% dessas violações ocorreram nos servidores de rede das instituições (Figura 4). Além disso, os servidores de rede e e-mail combinados representaram 80% dos vetores de ataque, impactando negativamente o tratamento de doenças agudas, o que pode levar a resultados desastrosos.

Figura 4



Quatro riscos críticos à segurança cibernética que desafiam o setor de saúde

Não obstante aos diversos benefícios que as tecnologias representam para o setor de saúde, a adoção de novos dispositivos que permitem a atuação de médicos e a interconexão entre diferentes sistemas de serviços de saúde acrescenta muitos riscos. As HDO enfrentam desafios significativos na área de segurança cibernética, compartilhados em todo o setor de serviços de saúde:

1. Manter a infraestrutura crítica coberta e continuamente disponível.
2. Proteger a privacidade dos pacientes contra riscos internos.
3. Preservar a integridade dos dados dos serviços de saúde.
4. Prevenir violações de dados originadas de ataques de ransomware e phishing.

Investimento insuficiente em segurança infraestrutural no contexto de expansão de infraestruturas críticas cria uma situação insustentável. As lacunas da segurança cibernética em áreas como gerenciamento de patches, gerenciamento de configurações, controles de acesso adequados, criptografia de dados e segurança do portal do paciente prejudicam a missão das HDOs de oferecer qualidade, tratamentos nos prazos previstos e proteção à privacidade dos pacientes. Qualquer colapso na proteção de PHI, conforme as leis e diretrizes de proteção de dados aplicáveis, representam riscos para os fornecedores, que ficam sujeitos a consequências severas. Alguns exemplos incluem a violação de dados, a interrupção de tratamentos, resultados insatisfatórios nos tratamentos, problemas de cobrança, prejuízos financeiros, custos de reparação de danos, despesas legais e com acordos, multas pesadas, perda de confiança, danos à reputação, etc.

Conclusão

Enquanto a pandemia persistir, as HDO continuam sobrecarregadas, com pessoal insuficiente e pressionadas pela tecnologia crescente na área de saúde e a transformação digital, para ser capaz de atender melhor seus pacientes. O pacote de soluções de segurança cibernética para o setor da saúde da SonicWall está disponível para facilitar a transição e fortalecer a segurança da infraestrutura de saúde, tornando os serviços mais eficientes, resilientes e seguros para os pacientes. Esse pacote de segurança integrado e com gestão centralizada consiste de edge, servidores, acesso, wireless, e-mails e endpoints, permitindo às HDO gerar resultados positivos na área da saúde, para todos os pacientes em sua jornada contínua pelos cuidados de saúde.

Leia o nosso artigo técnico *Boundless Cybersecurity for a Safer Healthcare Industry* (segurança cibernética ilimitada para um setor de saúde mais seguro) para saber como as soluções de segurança próprias para os serviços de saúde da SonicWall protegem a disponibilidade de infraestruturas críticas, a integridade dos registros eletrônicos de saúde e a confidencialidade e privacidade das informações pessoais de saúde.

1 Fonte: O impacto do ransomware nos serviços de saúde durante a COVID-19 e além, pelo Ponemon Institute.
2 Fonte: O impacto do ransomware nos serviços de saúde durante a COVID-19 e além, pelo Ponemon Institute.
3 Fonte: HIPAA Journal, January 2022 Healthcare Data Breach Report (Relatório de violação de dados no setor de saúde, janeiro de 2022), https://www.hipaajournal.com/january-2022-healthcare-data-breach-report/

Sobre a SonicWall

A SonicWall oferece segurança cibernética ilimitada na era hiperdistribuída e em uma realidade em que todos estão trabalhando remotamente, em dispositivos móveis e inseguros. A SonicWall preenche a lacuna comercial da segurança cibernética para hospitais, clínicas e prestadores de serviços em todo o mundo, conhecendo o desconhecido, oferecendo visibilidade em tempo real e permitindo uma economia revolucionária. Para obter mais informações, visite www.sonicwall.com/healthcare

SonicWall, Inc.
1033 McCarthy Boulevard | Milpitas, CA 95035
Consulte nosso site na internet para obter mais informações.
www.sonicwall.com

ExecBrief-HealthcareCybersecurity-A4-JK-6455