O valor da confiança nos serviços de saúde

Seus sistemas, dados e pacientes estão seguros contra ameaças cibernéticas?

pwc

O uso de dados traz benefícios para o setor de saúde

Mas também gera maior exposição a riscos cibernéticos

48%

dos CISOs do setor dizem que seus orçamentos cibernéticos estão aumentando em 2021

Fonte: *Digital Trust Insights 2021,* PwC

85%

dos executivos do setor de saúde afirmam que garantir a cibersegurança e a privacidade é uma barreira para suas estratégias digitais

Fonte: PwC Health Research Institute, set/2019

Novas tecnologias e uso de dados têm o poder de melhorar os resultados do setor de saúde, transformar a qualidade dos serviços e reduzir custos. Mas à medida que a digitalização ganha impulso e inovações como telemedicina e dispositivos de monitoramento remoto se popularizam, cresce a vulnerabilidade a ataques cibernéticos.

O megavazamento que expôs dados de mais de 220 milhões de brasileiros revelado em janeiro de 2021 e o aumento exponencial de ataques *ransomware* em todo o mundo em 2020 mostram o grau de sofisticação crescente das ameaças e a velocidade com que elas se espalham em um ambiente interconectado.

As organizações de saúde começam a perceber que é necessário agir. A pesquisa *Global Digital Trust Insights 2021*, da PwC, apontou que 49% das empresas do setor que participaram do estudo estão incorporando questões de cibersegurança e privacidade em cada decisão ou plano de negócios.

Mais do que nunca, é preciso se preparar para combater cibercriminosos e se adequar a exigências regulatórias, como as da Lei Geral de Proteção de Dados (LGPD). Quem demorar a agir corre o risco de sofrer pesados prejuízos financeiros e de imagem, além da perda da confiança dos clientes e da sociedade.

Em sua jornada de transformação digital, as organizações de saúde devem se conscientizar da sua responsabilidade pela segurança e privacidade dos dados de seus consumidores. E tomar as medidas necessárias para criar estratégias de defesa, identificar e conter ataques, gerenciar com eficácia futuras violações e se manter em conformidade com as regulações vigentes.

A PwC tem uma equipe altamente especializada e dispõe dos recursos tecnológicos necessários para apoiar você nesse processo.

Foco na privacidade e na segurança dos dados de saúde

Tendências que preocupam

- Registros pessoais de saúde são negociados no mercado clandestino por valores quase 25 vezes maiores do que os pagos por dados financeiros.
- Pesquisa *Digital Trust Insights 2021* revela que os executivos do setor de saúde estão especialmente preocupados com o impacto de ataques via terceiros.
- Os orçamentos de segurança cibernética continuam muito limitados no setor, especialmente no serviço público.

- Sua organização tem um programa de privacidade que inspire confiança no público?
- Suas operações estão em conformidade com as regulamentações de privacidade de dados?
- Sua estrutura para detectar, responder, investigar e remediar ameaças ao longo de todo o ciclo de gerenciamento de incidentes é suficientemente robusta?

Pacientes mais dispostos a se conectar

A maioria das pessoas que experimentaram formas de atendimento virtual durante a pandemia se diz disposta a fazê-lo novamente no futuro, mesmo após o fim da pandemia de Covid-19.

83% **Chamada telefônica**

81% Aplicativo para celular

80% **E-mail**

78% **SMS**

Quanto mais as pessoas usam telemedicina, aplicativos de saúde e dispositivos de monitoramento remoto, maior é o número de pontos de entrada possíveis para os criminosos cibernéticos interessados em roubar dados de pacientes ou lançar ataques *ransomware*. As empresas do setor precisam aumentar seus esforços de segurança cibernética, cumprir as leis de privacidade e desenvolver recursos poderosos de segurança para os produtos ou serviços que oferecem aos pacientes.

Fonte: *Global Top Health Industry Issues 2021*, PwC

A PwC pode ajudar você a garantir a segurança e a privacidade dos dados e manter suas operações em conformidade com a legislação.

O que as empresas de saúde precisam fazer

Prioridade para o que é mais importante

Não é fácil proteger tudo. Identificar e localizar os ativos de informação críticos e confidenciais e aumentar a segurança em torno deles deve ser a prioridade.

Atenção ao básico

Manter as atualizações em dia é essencial. Sistemas desatualizados e sem correção podem abrir caminho fácil para os invasores.

Para proteger, é preciso conhecer as ameaças e tratar o risco

Aumente a visibilidade, monitore e detecte proativamente ameaças cibernéticas. Gerencie os riscos ao negócio. Conheça os principais riscos e tenha um plano de tratamento imediato.

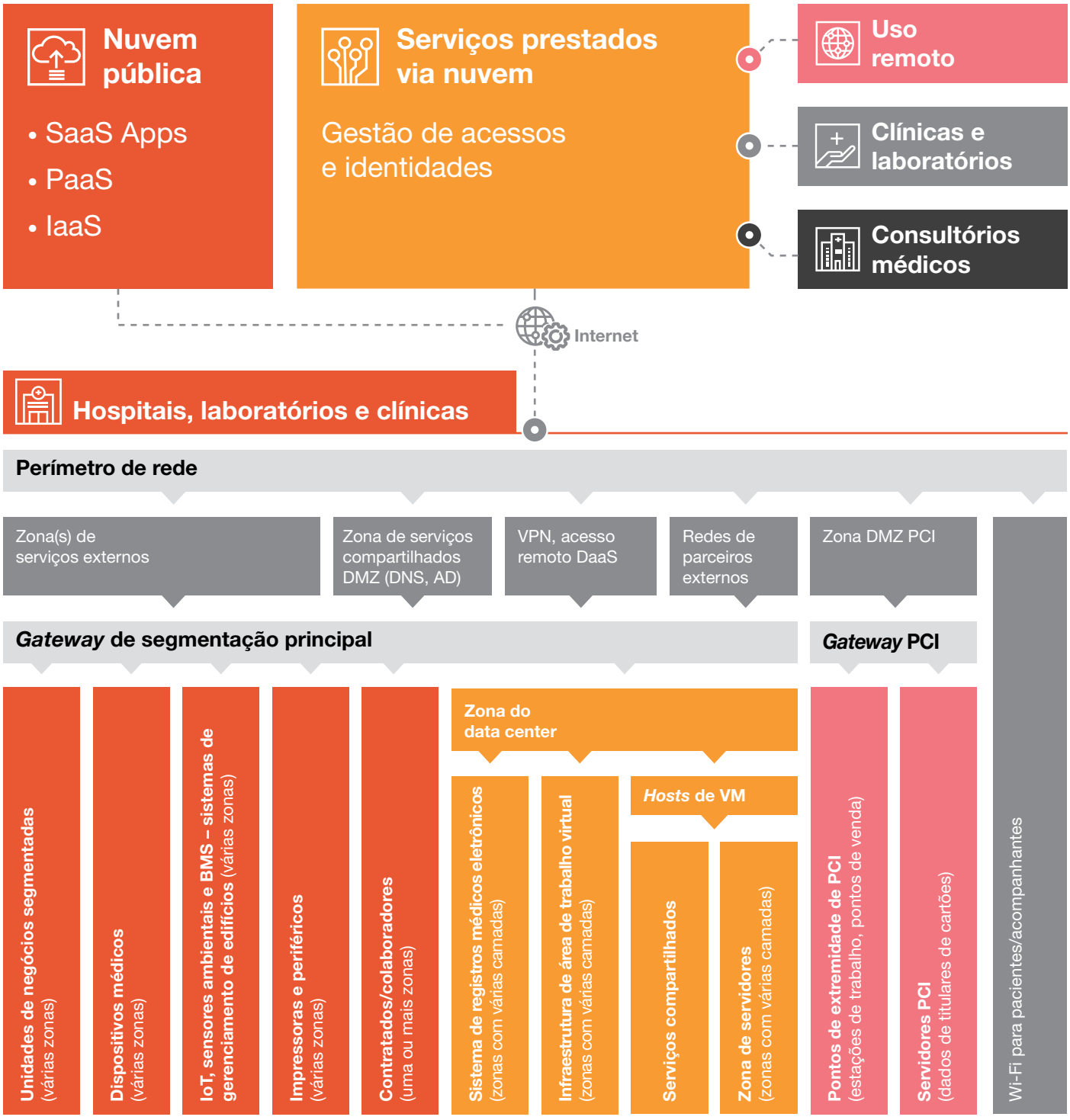
Não seja surpreendido pelo que pode evitar

Fazer simulações e testes regulares e usar os resultados para ajustar planos e políticas de resposta diminui a vulnerabilidade de sua organização.

Conscientização é fundamental

Manter as pessoas de sua organização cientes dos riscos, treiná-las em segurança cibernética e garantir que entendam suas responsabilidades faz toda a diferença.

Modelo de segmentação da rede hospitalar



A segmentação da rede com base em grupos de usuários, dispositivos ou tipos de dados (classificados por criticidade e risco) dificulta a ação de invasores e a disseminação de *malware*. Com base nessa compartimentação, fica mais fácil aplicar medidas de segurança com níveis de proteção diferentes para os vários grupos. Essa abordagem também reduz o esforço necessário para comprovar o *compliance* com regulamentações, restringindo a investigação às áreas nas quais estão armazenados os dados relevantes.

Nossa atuação

Oferecemos toda a gama de serviços cibernéticos e contamos com uma estrutura global que proporciona maior robustez a nossas análises de ameaças, feitas com base em insights, dados e pesquisas. Trabalhamos com uma equipe multidisciplinar pronta para apoiar o seu negócio em três frentes:

Construção de defesas

Sua estratégia cibernética de segurança requer uma abordagem que envolva todas as operações da organização. Podemos ajudar a:

- Desenvolver uma resposta estratégica mais ampla para lidar com os riscos cibernéticos.
- Fortalecer suas defesas.
- Testar sua infraestrutura.
- Transformar técnica e culturalmente a postura de sua organização em relação à segurança cibernética.

Identificação e resposta a ataques

As empresas do setor de saúde já estão sob ataque. Podemos ajudar a:

- Conduzir a gestão da crise cibernética e garantir a menor exposição dos negócios.
- Responder a incidentes e gerenciar a resposta para garantir que a perda de dados seja rapidamente contida e que os sistemas sejam restaurados no menor prazo.
- Realizar investigações após o incidente para entender a natureza da violação e saber como evitar ataques futuros.

Cenário legal e regulatório

Temos uma visão ampla do ambiente regulatório e conhecimento profundo do setor da saúde. Podemos ajudar a:

- Manter a conformidade com aspectos legais desde a concepção estratégica da segurança cibernética e da proteção de dados até o envolvimento em litígios pós-incidente.
- Apoiar o processo de adequação à LGPD, com avaliações de risco de operações e processos, reformulação da estratégia de governança e implementação de programas de privacidade de dados.

Cyber Control Center da PwC

Um dos diferenciais dos serviços de segurança cibernética da PwC é o nosso Cyber Control Center, que opera todos os dias de forma ininterrupta para monitorar a segurança da infraestrutura de tecnologia de nossos clientes, proteger seus ativos de informação e prevenir incidentes.

O Cyber Control Center tem uma solução de orquestração, automatização e resposta (SOAR) que nos permite responder a eventos de segurança com documentação mais robusta e de forma mais rápida e precisa, reduzindo o tempo gasto com triagem, análise e contenção.

Uma excelente prevenção permite impedir 99% dos ataques de forma automatizada em tempo real sem nenhum tipo de verificação manual. Com aprendizado de máquina e inteligência artificial, aumentamos a produtividade da operação de segurança focando nas ameaças que realmente importam. A automação é necessária para enriquecer informações de incidentes e rapidamente conter ataques reais. Casos de uso precisam ser automatizados e enriquecidos com informações variadas, como inteligência de ameaças, comportamentos do usuário e informações de *end point*.

Visibilidade e prevenção

- Inteligência de ameaças
- Modelagem de ameaças no contexto do negócio
- Mapeamento de *surface, deep* e *dark web*
- Alertas e *dashboard* em tempo real

PwC C3BR

Security Operations Center

- Detectar
- Analisar
- Conter
- Recuperar
- Enriquecer, orquestrar e automatizar

Além da remediação

- Recuperação dos ativos
- Otimizar o ambiente (*lockdown*, *threat hunting*)
- Melhorar indicadores da operação (*time-to-detect* e *time-to-remediate*)
- Engajar equipes forenses e de gestão de crises

Contatos

Eduardo Batista

Sócio e líder de *Cybersecurity*

eduardo.batista@pwc.com

Bruno Porto

Sócio e líder do setor de Saúde

bruno.porto@pwc.com

Rafael Cortes

Diretor, especialista em *Cybersecurity*

cortes.rafael@pwc.com

PwC Brasil @PwCBrasil PwC Brasil @PwCBrasil PwC Brasil @PwCBrasil

(DC0) Informação Pública
Versão: Junho 2021 | [F300]