Diligent

10 PERGUNTAS

para avaliar a segurança de um portal para conselhos

Quando uma organização contrata um provedor de portal para conselhos, ela confia no provedor para proteger documentos confidenciais e oferecer um sistema para gerenciar o acesso a esses documentos. Essa confiança ultrapassa as especificações técnicas. Por isso, é essencial que conselhos, secretários do conselho, assessores jurídicos e CIOs estejam confortáveis com a segurança de seu provedor de portal para conselhos e confiem nessa segurança.

Veja 10 perguntas que as organizações devem fazer a potenciais provedores de portais para conselhos:

1 O provedor faz investimentos consideráveis em pesquisa e desenvolvimento de tecnologias de segurança cibernética

As ameaças à segurança cibernética evoluem continuamente, não apenas em razão dos avanços tecnológicos, mas também das mudanças no submundo cibernético. Hackers solitários deram lugar a sofisticadas organizações que podem causar perturbações em escala global. Um provedor de portal para conselhos deve ser capaz de demonstrar capacidades de pesquisa e desenvolvimento que permitam a ele estar à frente das ameaças emergentes.

2 O provedor é transparente em relação aos seus processos de segurança?

O provedor deve ser capaz de explicar claramente suas medidas de segurança física (proteção de servidores, roteadores e outros equipamentos), o processo de seleção de novos funcionários contratados, os controles internos, o monitoramento do sistema (se houvesse uma invasão de hackers, como seria possível detectá-la?) e qualquer histórico de violações da segurança e sua resolução.

3 O provedor satisfaz aos mais elevados padrões do setor?

Como portadores de informações confidenciais de terceiros, os portais para conselhos devem atender a padrões de segurança comparáveis àqueles dos departamentos de TI mais exigentes de diversos setores. As principais certificações incluem um histórico limpo de auditorias anuais SOC/SSAE 16 (abordando como os provedores relatam seus controles internos) e a certificação de segurança ISO 27001 (conformidade dos sistemas reais de gerenciamento de segurança da informação do provedor de software com os padrões internacionais, em oposição à conformidade meramente dos data centers que hospedam seus dados).

4 O provedor permite a realização de testes externos de penetração?

A maior parte dos provedores de portais para conselhos realiza testes de penetração como parte de seu controle de qualidade. Portais com elevados padrões de segurança conduzirão testes praticamente de forma contínua, não apenas anualmente, a fim de acompanhar a evolução das ameaças. Eles também devem permitir que clientes e clientes potenciais realizem seus próprios testes independentes de segurança e penetração (ou envolvam terceiros escolhidos por eles). Essa é uma poderosa demonstração de confiança, bem como uma confirmação de que a segurança é, em última análise, um esforço em equipe.

5 O provedor depende de plataformas ou software de terceiros?

Muitos portais para conselhos são criados a partir de plataformas disponíveis comercialmente ou utilizam componentes de plug-in prontos para alguns elementos de seu software. Entretanto, esses elementos de terceiros apresentam suas próprias vulnerabilidades de segurança, que são atraentes para hackers justamente por que essas plataformas são bastante conhecidas e não foram criadas para as exigências de um portal para conselhos. Em vez disso, os portais para conselhos devem ser criados do zero, com recursos de segurança projetados para o aplicativo, sob todos os aspectos.

6 Qual é o nível de segurança física empregado pelo provedor?

Embora as informações digitais geralmente sejam vistas como algo intangível, na verdade, elas são armazenadas em servidores reais. Essas instalações para hospedagem de dados devem ser protegidas com seguranças no local, circuito fechado de monitoramento e várias camadas de segurança de perímetro. Os próprios servidores devem ser alojados em compartimentos protegidos por grades, com segregação física dos dados hospedados de cada organização. Além disso, suas chaves de criptografia devem ser protegidas por robustos dispositivos antiviolação.

AICPA SOC | ISO 27001 CERTIFIED BY BRIGHTLINE | Baixar na App Store | Baixe na Windows Store

7 Qual é o grau de redundância de dados fornecido?

É realizado backup dos dados e ocorre failover dos data centers primários para os data centers de recuperação de desastres? Provedores de portais para conselhos devem oferecer locais remotos, geograficamente dispersos, para garantir que qualquer evento que afete um local não afetará o local secundário. Além disso, a redundância dos dados deve receber suporte de informações sobre o desempenho dos dados em tempo real, 24/7.

8 O acesso do usuário ao portal pode ser restrito a um dispositivo específico?

Com os membros do conselho espalhados ao redor do mundo e viajando com frequência, a necessidade de proteger seus dispositivos móveis é algo extremamente importante. O acesso do usuário ao portal pode ser restrito a um dispositivo específico, registrado junto ao portal do conselho? Há também uma opção para desabilitar o acesso pelo navegador? Soluções de autorização de dispositivos permitem que as organizações impeçam o acesso por meio de dispositivos desconhecidos e não confiáveis. O resultado é maior controle sobre os direitos e os locais de acesso.

9 O provedor permite que você dimensione o nível de segurança do portal?

Cada solução de segurança envolve um equilíbrio entre conveniência e segurança. Como resultado, essas dimensões definitivamente não são adequadas a todas as organizações. Em vez disso, um portal para conselhos deveria ser capaz de personalizar funções para satisfazer às necessidades de segurança específicas de uma organização, permitindo, por exemplo, diferentes níveis de força de senha, políticas de bloqueio e opções de exportação e impressão dos documentos do conselho no portal.

10 Os recursos de segurança do portal estão incluídos no suporte ao cliente?

Não importa o nível de segurança de um portal: o monitoramento humano é necessário para garantir que todas as questões sejam resolvidas prontamente. Por exemplo, um diretor que digita a senha de forma incorreta repetidamente e é bloqueado no sistema deve receber uma chamada telefônica de suporte ao cliente imediatamente, tanto para prestar assistência quanto para verificar a causa das tentativas malsucedidas.

Para obter mais informações ou solicitar uma demonstração, entre em contato hoje mesmo:

E-mail: info@diligent.com

Tel.: + 55 11 9 9707 0212

Site: www.diligent.com

C0083_PORT