Os sistemas operacionais e aplicativos sempre podem ser reinstalados, mas seus dados são únicos, tornando -os a coisa mais importante no seu computador ou rede.

“As organizações agora devem manter medidas robustas de privacidade, incluindo políticas de privacidade claras, processos de opção e conformidade com as leis de proteção do consumidor, para mitigar riscos financeiros e reputação”, disse Kayne McGladrey, membro sênior da IEEE, em um email para a TechRepublic.

Aqui estão 10 maneiras pelas quais você pode proteger esses dados contra perda e acesso não autorizado.

O que você vai ler:

1. Proteja tudo com senhas

A proteção de senha é a primeira linha de defesa contra acesso não autorizado aos seus dados; Também ajuda a aumentar a segurança multicamada para seus sistemas, permitindo que você combine proteção de senha com outras medidas de segurança. Algumas empresas devem usar a proteção de senha como parte dos regulamentos de conformidade, como o regulamento geral de proteção de dados.

Para proteger a senha dos dados da sua empresa, implemente uma política rigorosa de senha para garantir que os funcionários criem senhas complexas. Além disso, você deve atualizar suas senhas regularmente.

2. Backup regularmente

O backup de seus dados antecipadamente e regularmente é um componente importante de uma estratégia de prevenção de perda de dados. A perda de dados pode acontecer devido a ataques cibernéticos, desastres naturais, erro humano e outros eventos. Se você fazer backup de seus dados, poderá restaurá -los após perder dados.

Embora o backup manual funcione, você também deve considerar as soluções de backup de dados que backup automaticamente de backup de dados com base em um cronograma que você pode configurar. Soluções de backup mais sofisticadas permitem que você escolha os dados para fazer backup.

3. Mantenha o software de negócios atualizado

Mantenha seu software de negócios atualizado para garantir que ele tenha os patches de segurança mais recentes, correções de bugs e outras atualizações para proteger contra ameaças novas e existentes em segurança cibernética. A maioria dos ataques cibernéticos explora as vulnerabilidades de segurança recém -encontradas; portanto, esteja vigilante para manter o software de negócios atualizado para a versão mais recente.

Veja: Ameaça os atores do jailbreak IA generativa para usá -lo para criar e -mails de phishing, ignorando salvaguardas.

4. Use uma VPN

As redes privadas virtuais são ótimas para manter seus dados comerciais em segurança. Uma VPN cria um túnel criptografado para seus dados, escondendo -os de hackers e outros atores maliciosos; Também ajuda a minimizar sua pegada on -line.

Uma VPN é obrigatória para os funcionários que se conectam a redes de negócios ou acessando arquivos confidenciais de suas casas ou durante a viagem. Embora você possa usar um serviço VPN gratuito, idealmente, você deve investir investir em uma assinatura VPN paga de um provedor respeitável. As versões VPN pagas oferecem conexões mais confiáveis, servidores dedicados e outros recursos premium.

Cobertura de segurança de leitura obrigatória

5. Instale o software antivírus

O software antivírus moderno ajuda a proteger dados de ransomware, spyware, cavalos de Trojan, seqüestradores de navegador e outras ameaças cibernéticas. Embora uma licença de

software antivírus para uma empresa tenha um custo, é um preço relativamente pequeno a pagar para manter seus dados seguros.

Se você estiver usando o Windows 10 ou superior, você já possui software antivírus instalado. Os computadores Mac possuem um ecossistema relativamente fechado e proteção de malware embutida, mas você também pode comprar defesas antivírus extras separadamente.

Na era da IA generativa, a proteção antivírus é ainda mais crítica. Os atores de ameaças podem usar modelos de IA em ataques ou dados comprometidos podem envenenar o modelo se for usado para treinamento.

“Uma vez que é um conteúdo malicioso, o agente da IA que você está tentando treinar também aprenderá usando conteúdo malicioso”, disse Ravi Srinivasan, diretor executivo da empresa de proteção de dados Votiro, em um email para a TechRepublic.

6. Use autenticação multifator

Uma maneira confiável de proteger seus dados é usar a autenticação de vários fatores em dispositivos conectados à rede de negócios. Com o MFA, os usuários inserem uma senha e uma senha única enviada a outro dispositivo para obter acesso. Dessa forma, o usuário precisa de pelo menos dois dispositivos, ou “fatores”, para fazer login no sistema.

O MFA atua como uma camada adicional de segurança para seus dados e está se tornando uma parte vital dos protocolos de segurança cibernética para as empresas. Sem usar o MFA, seus dados permanecem vulneráveis ao acesso não autorizado devido a dispositivos perdidos ou credenciais roubadas.

“Mesmo que uma organização fique sem senha”, disse Srinivasan, “você ainda terá usuários externos, contratados externos de terceiros e provedores de serviços que ainda podem estar acessando seus serviços usando senhas como padrão”.

Portanto, ele disse, os líderes de tecnologia devem pensar no MFA como parte da solução para um problema de acesso. Qualquer que seja a maneira como sua organização usa para proteger suas contas, é essencial ter acesso e controle de identidade de algum tipo.

Veja: Aqui está tudo o que os líderes de TI precisam saber sobre a autenticação multifator.

7. Faça uso de uma infraestrutura de chave pública

Uma infraestrutura de chave pública é um sistema para gerenciar pares de chave pública/privada e certificados digitais. Como as chaves e os certificados são emitidos por um terceiros confiáveis (ou seja, uma autoridade de certificação, interna instalada em um

servidor de certificados em sua rede ou público), a segurança baseada em certificado é mais forte.

Você pode proteger os dados que deseja compartilhar com outra pessoa, criptografando -os com a chave pública de seu destinatário pretendido, que está disponível para qualquer pessoa. A única pessoa que pode descriptografar é o titular da chave privada que corresponde a essa chave pública.

8. ocultar dados com Steganografia

Você pode usar um programa de steganografia para ocultar dados dentro de outros dados. Por exemplo, você pode ocultar uma mensagem de texto dentro de um arquivo gráfico .jpg ou um arquivo de música .mp3, ou mesmo dentro de outro arquivo de texto; No entanto, o último é difícil porque os arquivos de texto não contêm dados redundantes que podem ser substituídos pela mensagem oculta.

A Steganografia não criptografa a mensagem, por isso é frequentemente usada com o software de criptografia. Os dados são criptografados primeiro e depois escondidos dentro de outro arquivo com o software Steganografia.

Algumas técnicas Steganographic exigem a troca de uma chave secreta. Outros usam criptografia pública e privada. Um exemplo popular de software de steganografia é Stegomagic, um download de freeware que criptografará as mensagens e os esconderá em arquivos .txt, .wav ou .bmp.

O esconderijo de dados pode ser particularmente importante se “os dados reais da organização (s) (de clientes, pacientes, funcionários e qualquer outra pessoa) para testar e/ou treinar ferramentas de IA”, disse Rebecca Herold, membro do IEEE.

9. Eduque a si mesmo e a seus funcionários sobre a segurança cibernética

Uma das etapas mais cruciais para proteger seus dados é educar a si e a seus funcionários sobre segurança cibernética. Você precisa promover uma mentalidade cética ao interagir com qualquer site, email ou mensagem desconhecido; Isso inclui aprender a importância de seguir as melhores práticas para proteção de dados, como não abrir e -mails de remetentes não reconhecidos e não clicar em anexos suspeitos.

Veja: Aproveite este pacote de treinamento em segurança cibernética da TechRepublic Academy.

10. Procure orientação profissional

Você pode escolher empresas de consultoria de segurança para avaliar as vulnerabilidades de segurança em seu sistema e como corrigi -las.

Se você precisar de uma proteção mais abrangente para seus dados, considere contratar um provedor de serviços de segurança gerenciado; Eles oferecem uma variedade de serviços de segurança, incluindo monitoramento de segurança 24/7 e gerenciamento de incidentes. Além disso, se você deseja garantir seus ativos digitais, considere comprar uma apólice de seguro de segurança cibernética.

A IA generativa traz novas considerações de privacidade de dados

Embora as mesmas regras se apliquem à IA generativa, a nova tecnologia da moda também apresenta novas preocupações de privacidade de dados.

“Todas as empresas integrando a IA enfrentam um desafio de privacidade sem precedentes: eles estão essencialmente criando uma ponte entre os dados confidenciais de sua empresa e os modelos públicos de IA”, disse Oliver Friedrichs, diretor executivo e co-fundador da empresa de segurança cibernética Pangea, em um email para o TechRepublic .

Quando se trata de IA, a autorização adequada é fundamental.

“Em 2025, estamos vendo uma tendência preocupante em que a exposição sensível de dados através da IA não vem principalmente de ataques sofisticados – isso está acontecendo através de supervisões básicas de autorização e controle de acesso”, disse Rob Truesdell, diretor de produtos da Pangea, em em Pangea, em em Pangea, em em Pangea, em em Pangea, em em Pangea, em em Pangea, em em Pangea, em em Pangea, em em Pangea, em em Pangea, em um email. “As organizações estão descobrindo que seus sistemas de IA estão compartilhando inadvertidamente informações confidenciais simplesmente porque não definiram quem deve ter acesso ao quê”.

Srinivasan disse que a mudança para a IA exige considerações de privacidade de dados além do que as organizações consideraram antes de 2022; Em particular, as organizações podem usar dados de negócios para treinar modelos internos. As organizações precisam estar cientes do mascaramento de dados ou do anonimato para impedir que dados privados borbulhem na saída do modelo.

“A próxima geração de tecnologias de compartilhamento de dados que preserva a privacidade, como desidentificação e anonimização, está sendo desenvolvida para abordar o desafio de privacidade de dados representado por IA generativa”, disse o companheiro de IEEE Houbing Herbert Song.

As organizações devem perguntar: “Como você preserva a privacidade antes de treiná -la?” Srinivasan disse.

“As empresas devem realizar avaliações completas de risco para identificar e mitigar possíveis danos associados aos produtos de IA, compreendendo suas limitações e potencial uso indevido”, disse McGladrey. “Manter a documentação clara das métricas e metodologias do sistema de IA, além de divulgar riscos ou limitações conhecidos aos clientes, é essencial para a transparência”.

A transparência sobre o que a IA generativa pode e não pode fazer é a chave, disse McGladrey, assim como os mandatos de privacidade estaduais e federais.

(Tagstotranslate) Controle de acesso