As quatro maiores tendências e riscos de segurança cibernética para pequenas empresas em 2024

Nos últimos anos, vimos a tecnologia avançar rapidamente em diversas áreas. Os desenvolvimentos em automação e inteligência artificial estão sendo extremamente benéficos para as empresas, ajudando a poupar tempo e agilizar processos, como os de marketing.

Com os avanços tecnológicos, surgem ameaças cibernéticas novas e mais complexas. Embora um sistema robusto de segurança cibernética possa ajudar a proteger sua empresa contra riscos comuns, como vírus e malwares, as ameaças cibernéticas estão cada vez mais complexas e os empresários ainda podem ser pegos de surpresa.

Confira um resumo das maiores tendências e riscos de segurança cibernética que você deve conhecer em 2024.

Inteligência artificial generativa

A inteligência artificial (IA) generativa é um tipo de tecnologia que pode ser usada para criar novos resultados, como conteúdo, áudio, código, imagens e vídeos. O ChatGPT é um tipo de IA generativa. GPT significa "transformador pré-treinado generativo".

É muito popular entre empresários pela capacidade de poupar tempo e recursos. Pequenos empresários estão usando essa ferramenta para escrever material de marketing, organizar dados e criar código de sites, mas as funcionalidades dela estão avançando rapidamente.

A versão mais recente do ChatGPT pode gerar vozes humanas sintéticas e realistas usando apenas alguns segundos de amostra de fala. O Spotify já está usando a tecnologia para experimentar o recurso de tradução por voz, que traduzirá podcasts para diferentes idiomas, tudo na voz do apresentador do podcast.

A OpenAI, criadora do ChatGPT, admite que "essas funcionalidades também apresentam novos riscos, como a possibilidade de usuários mal-intencionados se passarem por figuras públicas ou cometerem fraude".

É uma área importante a ser acompanhada por pequenos empresários em 2024. A tecnologia ainda está em uma fase inicial, mas poderá abrir caminho para tentativas de phishing mais inteligentes e personalizadas no futuro. E-mails, mensagens de texto e ligações podem, por fim, imitar a voz de outra pessoa. Portanto, você e sua equipe precisam se atentar a qualquer coisa suspeita.

Resiliência cibernética

O pequeno empresário com quem conversamos recentemente falou sobre como é exaustivo acompanhar os riscos de segurança cibernética em rápida evolução. Isso gerou a maior tendência seguinte: resiliência cibernética.

A segurança e a resiliência cibernética são frequentemente usadas de modo intercambiável, mas são conceitos um pouco diferentes. A segurança cibernética ajuda a proteger sua empresa contra ataques, mas a resiliência cibernética permite que esta continue funcionando mesmo que seja atacada.

A maioria das empresas reconhece que mesmo a melhor segurança cibernética não garante uma proteção infalível. Estabelecer uma estratégia de resiliência cibernética ajudará sua empresa a reagir rapidamente caso sofra um ataque cibernético ou uma violação de dados.

Como parte do seu plano de resiliência cibernética, estas são nossas recomendações:

- Identificar processos, sistemas e tecnologias essenciais e fazer upgrade na segurança
- Implementar a tecnologia em nuvem para fazer backup das partes mais importantes da sua empresa
- Criar um plano de resposta a incidentes cibernéticos que estabeleça claramente como sua empresa reagirá e se recuperará caso sofra um ataque

Zero Trust

O Zero Trust faz parte do movimento em direção à resiliência cibernética e se baseia na ideia de que nenhum sistema é 100% seguro.

Uma estratégia de segurança com o Zero Trust consiste em dar aos usuários apenas a quantidade necessária de acesso para realizar o trabalho e nada mais. Os usuários precisarão ser autenticados e ter o acesso reautorizado constantemente.

Isso envolve as seguintes questões:

- Quem pode acessar o quê e quando
- A autenticação necessária para acessar essas ferramentas ou ativos
- Quais informações podem entrar ou sair da sua rede

Se você estiver usando uma plataforma de armazenamento em nuvem e compartilhamento de arquivos como o Google Drive, a maneira mais fácil de começar com uma estratégia do Zero Trust é verificar as permissões disponíveis e garantir que o acesso seja restrito quando necessário. Essas permissões devem ser revisadas com frequência e o acesso imediatamente negado se alguém (por exemplo, um freelancer) parar de trabalhar para sua empresa.

Normalização das práticas recomendadas

Um dos maiores desafios da segurança cibernética sempre foi o fato de ela ser tão forte quanto seu elo mais fraco: a equipe. Notoriamente, o ataque cibernético WannaCry (em inglês) ao NHS em 2017 foi tão destrutivo porque os hospitais públicos locais simplesmente não atualizaram os sistemas informáticos antigos.

Nos últimos seis anos, a segurança cibernética se tornou um assunto mais conhecido. A maioria das pessoas que trabalham com sistemas digitais reconhece a importância dela, e ferramentas de segurança cibernética, como autenticação baseada em vários fatores e gerenciadores de senhas, são mais comuns e acessíveis do que nunca.

Por isso, as práticas de segurança cibernética estão se normalizando nas empresas e esperamos que essa tendência continue até 2024. Em vez de ser responsabilidade exclusiva de uma pessoa, manter uma organização segura é algo que deveria ser prioridade de todos.

Leia mais sobre maneiras econômicas de aprimorar as habilidades de sua equipe em segurança cibernética.