Como proteger sua pequena empresa com orçamento limitado

Por Yusuph Kileo (Especialista em segurança cibernética e forense digital, BC-Rep (subcomitê financeiro) @ICANN Membro do Conselho, , @AfICTA Grupo de Trabalho de Abuso de DNS do BC. #KileoOnCybersecurity)

A noção de que você não é um alvo para invasores cibernéticos: que você, seus sistemas ou contas não têm nenhum valor é falsa. Se você usa a tecnologia de alguma forma, você tem valor para os cibercriminosos.

As ameaças cibernéticas vêm de várias formas, desde e-mails de phishing até ataques de ransomware. As pequenas empresas podem ser particularmente vulneráveis a ataques que exploram vulnerabilidades comuns, como software desatualizado ou senhas fracas.

De acordo com o estudo Cost of Cybercrime da Accenture, 43% dos ataques cibernéticos são direcionados a pequenas empresas, mas apenas 14% estão preparados para se defender. Quando as pequenas empresas se tornarem alvos de um ataque cibernético, eles podem acabar enfrentando consequências financeiras e operacionais, das quais alguns podem nunca se recuperar.

Infelizmente, a segurança cibernética pode não estar no topo da lista de prioridades da maioria das pequenas empresas. Mas deveria ser. A boa notícia é que existem etapas acessíveis você pode tomar para proteger sua empresa contra ataques cibernéticos.

IMPORTÂNCIA DA CIBERSEGURANÇA PARA PEQUENAS EMPRESAS

As pequenas empresas são frequentemente visadas porque podem ter medidas de segurança mais fracas devido à falta de recursos em comparação com as grandes empresas. Uma violação de dados pode resultar em perda de receita, danos à sua reputação e possíveis consequências legais. Em alguns casos, um ataque cibernético pode até forçar o fechamento de uma pequena empresa.

Avaliando seu risco

Identifique dados e ativos confidenciais: o primeiro passo para proteger sua empresa é identificar os ativos mais importantes para sua empresa.
Isso inclui dados financeiros, informações de clientes ou propriedade intelectual.
Seus ativos também incluem o hardware sobre o qual sua empresa funciona. Se o hardware for tornado inoperável de um ataque cibernético, a incapacidade de realizar negócios pode ser igualmente devastadora.

Compreender o impacto potencial de uma violação de dados: Depois de identificar seus dados e ativos mais confidenciais, é importante entender o impacto potencial de uma violação de dados.

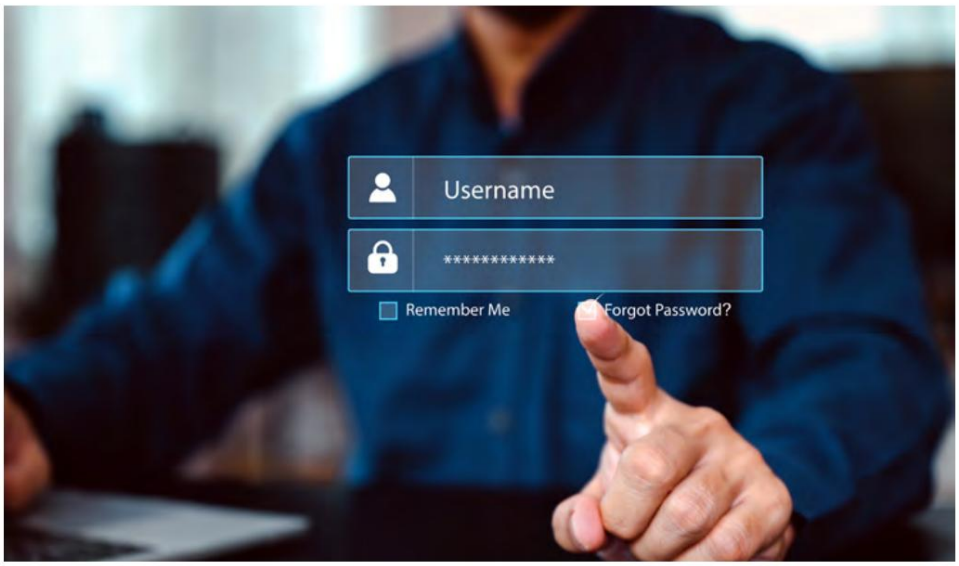
Considere como uma violação pode afetar seus clientes, suas operações comerciais e sua reputação.

Avaliando as medidas de segurança existentes: Avalie as medidas de segurança que você possui atualmente. Isso pode incluir tecnologia antimalware, firewalls ou programas de treinamento de funcionários. Procure lacunas em sua segurança e identifique áreas onde você pode melhorar.

Uma matriz de avaliação de risco pode ser usada para delinear a probabilidade e o impacto de um possível ataque cibernético. Isso permite que você priorize suas áreas mais vulneráveis.

Melhorando sua segurança cibernética

Implementação de protocolos básicos de segurança:



Uma das etapas mais importantes para proteger sua pequena empresa é implementar protocolos básicos de segurança. Esses protocolos são projetados para proteger contra os tipos mais comuns de ataques cibernéticos e podem reduzir significativamente o risco de violação.

Gerenciamento de senhas: senhas fortes e exclusivas são uma parte crítica da boa higiene da segurança cibernética. Você deve incentivar seus funcionários a usar senhas complexas e difíceis de adivinhar. As ferramentas de gerenciamento de senhas são a melhor maneira de ajudar a controlar várias senhas exclusivas.

Monitoramento de rede: embora ferramentas como firewalls, sistemas de detecção de intrusão e software antimalware possam proteger sua rede contra ameaças cibernéticas, monitorar regularmente sua rede pode ajudar a identificar possíveis ameaças à segurança.
Um sistema de gerenciamento de log barato pode ajudar a identificar comportamentos suspeitos, como bloqueios de várias contas, bem como tentativas de login com falha e acesso não autorizado a arquivos.

Atualizações regulares de software: manter seu software atualizado é essencial para garantir que as vulnerabilidades sejam corrigidas e que seus sistemas estejam protegidos contra as ameaças de segurança mais recentes. Você deve atualizar regularmente seus sistemas operacionais, navegadores da Web e outros softwares para as versões mais recentes
versões.

EDUCAR OS FUNCIONÁRIOS SOBRE O MELHOR PRÁTICAS DE CIBERSEGURANÇA

Seus funcionários podem ser seu maior trunfo quando se trata de segurança cibernética, mas também podem ser uma responsabilidade se não forem treinados adequadamente. Educar seus funcionários sobre as melhores práticas de segurança cibernética é, portanto, crucial para proteger sua pequena empresa. Certo práticas das quais seus funcionários devem estar cientes incluem:

Evitando e-mails suspeitos: e-mails de phishing são uma tática comum usada
por cibercriminosos para obter acesso a dados confidenciais. Instrua seus funcionários sobre como identificar e evitar e-mails suspeitos e considere implementar um software de filtragem de e-mail para reduzir o risco de ataques de phishing.

Não compartilhar senhas: Incentive seus funcionários a manter suas senhas privadas e nunca compartilhá-las com ninguém. Implemente a autenticação de dois fatores para adicionar um extra
camada de segurança para o seu processo de login.

Protegendo dispositivos móveis: dispositivos móveis, como smartphones e tablets, podem ser um elo fraco em sua estratégia de segurança cibernética. Incentive seus funcionários a usar senhas fortes, habilitar atualizações automáticas e evitar o download de aplicativos suspeitos ou clicar em links em mensagens de texto.

Políticas e procedimentos de segurança cibernética: Estabeleça políticas e procedimentos claros que enfatizem a importância da segurança. Isso pode ajudar a garantir que todos estejam trabalhando em direção a um objetivo comum. Essas políticas podem abranger áreas como gerenciamento de senhas, trabalho remoto e uso de dispositivos pessoais no local de trabalho. Tudo isso pode servir para construir uma cultura de segurança na organização.

RESPONDENDO A UM INCIDENTE DE CIBERSEGURANÇA

Apesar de seus melhores esforços, sempre há uma chance de que sua pequena empresa sofra um incidente de segurança cibernética. Nesse cenário, é importante responder de forma rápida e eficaz para minimizar os danos.

Na maioria dos casos, as técnicas forenses para descobrir o que causou o problema estão fora do alcance de muitas pequenas empresas.
A coisa mais importante para um pequeno empresário é voltar a funcionar o mais rápido possível.
É aqui que os backups de dados se tornam uma das ferramentas mais valiosas em um ambiente.

Outra maneira de se preparar e se recuperar de qualquer evento de segurança é contratar um provedor de serviços gerenciados confiável que possa aconselhá-lo e orientá-lo sobre a melhor segurança dentro do seu orçamento.

A segurança cibernética é um aspecto essencial da administração de uma pequena empresa no mundo digital de hoje. A prevalência de ameaças cibernéticas está aumentando, e o impacto de um ataque cibernético em uma pequena empresa pode ser devastador. Ao avaliar seu risco, implementar práticas recomendadas, criar uma cultura de segurança e fazer parceria com um consultor confiável, você pode proteger sua empresa dos perigos do crime cibernético.