RECOMENDAÇÕES SOBRE CIBERSEGURANÇA EM TEMPOS DE TRABALHO REMOTO

Publicações recentes têm destacado que cibercriminosos e agentes *nation-state* estão usando o momento atual de pânico e desinformação para colocar em prática métodos tradicionalmente adotados por *hackers* para roubar dados – desde o uso de mapas interativos com estatísticas de infecção pelo coronavírus para plantar *malware* em dispositivos a golpes de *phishing* nos quais os *hackers* se apresentam como funcionários do CDC. Embora a resposta ao COVID-19 tenha sido focada, corretamente, no número de pessoas afetadas, e enquanto as organizações tomam medidas para enfrentar a ameaça representada pelo COVID-19, elas também devem se preparar para o aumento dos riscos de segurança cibernética que estamos vendo. Seguem, abaixo, algumas dicas práticas que podem ser implementadas rapidamente, sem a necessidade de reconstruir a sua infraestrutura de TI ou reformular políticas (o que provavelmente não será viável no curto prazo).

- **Lembre seus empregados sobre riscos e o perigo do *phishing***. O *phishing* é uma tática muito conhecida que os *hackers* usam há anos, mas é uma ferramenta ainda mais poderosa durante uma pandemia global, quando as pessoas têm mais perguntas do que respostas. Os cibercriminosos já usaram golpes de *phishing* para explorar sentimentos de insegurança e pânico, e os indivíduos correm um risco maior de tornarem-se vítimas de tais esquemas em meio ao caos e à irregularidade de seus novos arranjos de trabalho. Você deve considerer o envio de um lembrete aos seus empregados para que fiquem sempre alerta para tentativas de *phishing* e para lembrá-los de ter muito cuidado com emails externos e solicitações incomuns de informação.

- **Instrua seus empregados sobre as práticas recomendadas para trabalho remoto**. Muitos de seus funcionários podem não ter um escritório em casa, uma boa conexão à Internet em banda larga ou acesso a uma impressora. Esse cenário apresenta riscos para a sua segurança que você precisa solucionar. Listamos abaixo algumas áreas que exigem um cuidado especial.

    - *Redes públicas de WiFi*: Ao contrário do ambiente do escritório, você não poderá controlar como os seus funcionários acessam a Internet em casa ou em outros locais. Funcionários podem confiar em redes sem fio que não são seguras para trabalhar. Para reduzir o risco de acesso não autorizado às informações da sua organização, você pode fornecer aos funcionários instruções para proteger sua

rede sem fio pessoal, por exemplo, protegendo-a com uma senha, restringindo o acesso a dispositivos específicos e atualizando o roteador *firmware* regularmente. Se possível, os funcionários devem se conectar ao ambiente corporativo usando uma rede virtual privada (VPN), e configurar uma para sua organização levará menos tempo do que você imagina.

- *Informações comerciais confidenciais*: Lembre seus funcionários da necessidade do manuseio adequado de informações comerciais confidenciais durante a transição para o trabalho remoto. Se sua empresa tiver dados confidenciais, você provavelmente preferirá evitar que seus funcionários encaminhem e-mails de trabalho para suas contas pessoais ou que enviem informações confidenciais a uma gráfica local para impressão. Se um funcionário já tiver informações sigilosas em cópia impressa, considere recomendar que as cópias sejam mantidas até que possam ser descartadas adequadamente quando for possível retornar ao escritório ou usando uma trituradora doméstica, se uma estiver disponível.

- *Instalação de software*: À medida que mais empresas passam a autorizar trabalho remoto, funcionários e empresas descobrem diversas novas ferramentas de software (para chamadas em conferência e videoconferências, por exemplo) desenvolvidas para facilitar o teletrabalho. Tenha cuidado com isso. Você deve instruirseus empregados sobre quais ferramentas seriam as suas ferramentas preferidas e aprovadas, para ter algum controle sobre como suas informações estão sendo manipuladas e compartilhadas.

- **Considere sua abordagem em relação aos dispositivos BYOD**. Permitir que seus funcionários trabalhem remotamente pressupõe que eles tenham os dispositivos adequados para fazê-lo. Nem todas as organizações fornecem laptops para os funcionários, e trabalho remoto pode exigir que as empresas permitam que seus funcionários usem seus dispositivos pessoais para fins relacionados ao trabalho. Sua organização precisará estar atenta aos riscos dessa abordagem de BYOD. Ao decidir se deve permitir esse acesso, considere o risco que sua organização enfrenta, tendo em vista, entre outras coisas, a necessidade dos funcionários de acessar sua rede remotamente, as proteções de segurança existentes para permitir tal acesso e o risco potencial de danos caso seus dados sejam comprometidos.

- Depois de estabilizar suas operações, você poderá considerar outras etapas para habilitar o acesso seguro de dispositivos pessoais, como ambientes de área de trabalho virtual e sistemas de gerenciamento de dispositivo móvel (MDM).

- **Garanta que sua equipe de TI pode responder a eventuais incidentes remotamente**. Sua equipe de TI pode ser limitada na forma em que presta suporte para seus empregados. Sua equipe local de TI pode precisar trabalhar remotamente e, mesmo que não precise fazer isso, com mais funcionários que não são de TI trabalhando remotamente, a equipe de TI pode não ser capaz de prestar o mesmo nível de suporte que faria aos funcionários se estivesse presente no escritório. Prepare-se para essas limitações agora. Você deve garantir que seus protocolos de resposta a incidentes sejam claros, que os incidentes continuem sendo adequadamente sinalizados e escalados conforme apropriado e que a equipe de resposta a incidentes possa se comunicar usando comunicações fora da banda, se necessário. Para conseguir isso, você precisa de canais de comunicação claros e confiáveis, tanto para partes internas quanto externas.

- **Revise e atualize sua política de teletrabalho**. Embora a atualização de políticas possa não ser sua primeira prioridade entre as várias medidas que você precisará adotar para preparar seus empregados para o trabalho remoto, considere se as medidas de emergência que você está executando são consistentes com sua política de teletrabalho e deixe claro que exceções serão autorizadas em caso de circunstâncias incomuns. Quando o tempo permitir, e com o benefício das lições que você aprendeu com resposta inicial de sua organização ao COVID-19, convém reler sua política de teletrabalho e garantir que tal política reflete com precisão suas práticas e melhores práticas de cibersegurança.