Empresas & Negócios

Matéria de capa

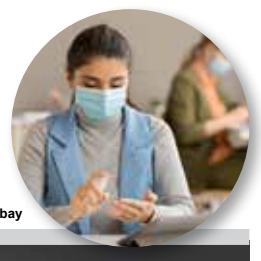

Imagem de StartupStockPhotos por Pixabay

ROTINA

RETORNO AO ESCRITÓRIO: COMO SE PROTEGER DE AMEAÇAS ADORMECIDAS DA PANDEMIA

Enquanto as organizações estão perto de implementar seus planos de retorno ao trabalho, a maioria dos colaboradores está animada sobre ter de volta suas rotinas no escritório. Eles perderam seus colegas, seus locais favoritos de almoço, e a cultura corporativa interna, que não puderam ser totalmente replicados através das plataformas de videoconferência. Os gestores de TI têm uma visão diferente.

Rick Vanover (*) e Dave Russell (**)

Eles sentem falta de todos os benefícios do escritório também, mas, para eles, a perspectiva de ter todos os colaboradores de volta à rede depois de um ano de trabalho remoto é assustador. Os profissionais de Segurança temem que os dispositivos deles estejam comprometidos após um longo período fora do escritório, o que pode expor a companhia a novas ameaças.

Eles podem ter razão. Os computadores tiveram vários papéis durante a pandemia hospedando de tudo: de reuniões sociais à ginástica, sessões de aprendizado online, compras em casa e Netflix. Membros da família pegaram emprestado o dispositivo da mãe para jogar jogos online, e senhas foram repassadas. A diligência cibernética teve uma prioridade menor do que deveria ter.

Os cibercriminosos estão bem conscientes do quão inseguros os ambientes de colaboradores têm sido. Eles tiveram contatos com uma série de ataques de phishing durante o período de lockdown. Agora, os gestores estão preocupados que os atacantes possam implantar vulnerabilidades em laptops inseguros e liberá-las quando os funcionários se reconectarem com uma gama mais ampla de recursos dentro das redes corporativas.

Algumas companhias fizeram um bom trabalho ao se anteciparem quanto às ameaças de segurança. Quando o trabalho remoto virou prática padrão, alguns foram capazes de emitir os dispositivos padrão da empresa com segurança de antivírus recomendada regularmente. Mas a maioria da luta que eles encontraram para habilitar rápida e adequadamente as configurações do trabalho remoto, não requeriam atualizações, patches e checagem de segurança.

Uma pesquisa de segurança conduzida em fevereiro reflete o quanto as empresas estão despreparadas para retornar ao ambiente de trabalho com segurança. Dos entrevistados, 61% usaram seus dispositivos pessoais – não computadores da empresa – em casa. Somente 9% usaram uma solução de antivírus fornecida pela empresa, e somente 51% receberam serviços de suporte de TI enquanto transitavam para as estações de trabalho remotas. Os gestores estão esperando eventuais problemas de segurança.

Além de receber inúmeros dispositivos potencialmente contaminados voltando ao ambiente de trabalho, eles precisam se preparar para o novo normal baseado no modelo híbrido casa/escritório, o que impõem riscos. De acordo com o Relatório de Proteção de Dados da Veeam, 89% das organizações aumentaram significativamente o uso dos serviços em nuvem como um resultado do trabalho remoto, e a tendência é que continue, demandando mais endpoints para proteger.

Foto de Alena Darmel no Pexels

Então, como as organizações podem se preparar para essa transição? Aqui estão alguns passos que podem ser adotados

Submeta-se a uma rigorosa preparação de retorno ao escritório – Este é essencialmente o passo onde gestores de TI vasculham, fisicamente, todos os recursos que possam ter sido afetados para garantir que eles estão prontos para entrar novamente no jogo. Comece por executar as avaliações dos riscos para cada colaborador e cada dispositivo.

Quais dispositivos têm sido corrigidos e mantidos regularmente? Computadores usados para o trabalho remoto têm probabilidade de ter dados confidenciais da companhia, onde os dados da empresa têm sido salvos? Em que conta? Essas checagens precisam ser feitas para minimizar riscos e garantir que os padrões de conformidade como a Lei Geral de Proteção de Dados sejam mantidos.

Além disso, veja se os funcionários distribuíram senhas para os membros da família usando os computadores do trabalho. Os funcionários mudaram suas senhas? Eles usaram os mesmos passwords nas contas de trabalho e nas contas pessoais? Eles instalaram ou removeram algum novo software durante o período de trabalho remoto? Os gestores precisam saber disso antes de deixarem os funcionários voltarem para suas redes.

Em seguida, certifique-se de escanear todos os dispositivos relevantes por apps e softwares não autorizados. Os funcionários precisaram ser criativos com as soluções de trabalho, então eles podem ter usado os recursos que os ajudaram nas tarefas diárias, mas que não estão à altura dos padrões de segurança da sua empresa.

Execute escaneamento de detecção de endpoints em todos os dispositivos que voltarem para a organização para descobrir quaisquer vulnerabilidades escondidas. Os cibercriminosos costumam mirar nos endpoints, então os times de TI precisam vasculhar todos os equipamentos pessoais e corporativos do colaborador que voltarão para a rede.

Melhore a higiene digital dos funcionários – À medida que os colaboradores voltam ao ambiente corporativo, é preciso que eles façam uma higiene digital mais adequada. Faça-os a usar senhas separadas para os dispositivos de casa e do trabalho. E tenha certeza que eles estejam usando combinações complexas e difíceis de decifrar.

Traga de volta os treinamentos para garantir que eles sejam capazes de identificar emails de phishing e outras ameaças. Configure as diretrizes para o uso do wi-fi público e o download de materiais. À medida que funcionários voltam ao escritório, cabe aos administradores refinar as práticas de TI, uma a uma, para se proteger contra as principais ameaças corporativas.

Monitore todas as atividades – A melhor maneira de perceber um problema é configurar um sistema para mostrá-los conforme eles acontecem. Essa prática pode ser aplicada às ferramentas e comportamentos dos funcionários à medida que eles se reintegram com todos os aplicativos da empresa. Aproveite as ferramentas de monitoramento que rastreiam as mudanças no uso e nos aplicativos. Se um colaborador fizer uma mudança num aplicativo, você precisa saber.

Pode ser um bug, que altera uma parte do código, ou uma mudança que você fez proposital ou inadvertidamente que você vai precisar redefinir. Tenha como hábito verificar as suas ferramentas de monitoramento pelo menos algumas vezes por dia. Leva um minuto, mas lhe permite avaliar constantemente a sua estratégia de cibersegurança.

Foto de Jopwell no Pexels

Garanta que o gerenciamento de dados em nuvem em backup seja sólido

Esse é o momento para os gestores de TI garantirem que todos os serviços de backup e gerenciamento de dados estejam em ordem. Se um dispositivo malicioso colocar qualquer dado em risco você vai querer que os backups estejam prontos e programados, com práticas que vão garantir que os dados em questão sejam protegidos e totalmente disponíveis.

Tenha em mente a regra chamada 3, 2, 1 – Certifique-se de manter pelo menos três cópias dos dados corporativos, armazene dados críticos em pelo menos dois tipos diferentes de armazenamento e mantenha uma cópia dos backups em um lugar fora da empresa. Para isso, na era do ransomware nos expandiríamos 3-2-1 para 3-2-1-1-0: adicionando um outro 1 à regra, em que a mídia está offline e garantindo que todas as soluções de recuperação tenham zero erros.

Conclusão – Enquanto gestores de TI estão ansiosos por retomar a conversa nos corredores dos escritórios e a colaboração presencial tanto quanto qualquer um, eles estão preocupados com as implicações de cibersegurança para um retorno mais seguro ao trabalho. Pode ser um desafio, mas com planejamento e acompanhamento adequados, as empresas podem gerenciar os riscos e consolidar suas estratégias de proteção para seguir em frente.

(*) - É VP of Enterprise Strategy at Veeam;
(**) - Rick Vanover é Senior Director Product Strategy at Veeam.