GUÍA DE TRABAJO REMOTO PARA LAS PYME

Lista de verificação de segurança de acesso remoto para administradores de TI

Quando ocorre uma perturbação social, a opção de poder trabalhar de casa é essencial para a continuidade dos negócios. Porém, na tentativa de manter os funcionários produtivos e os negócios em andamento e de repente passar para um modelo de trabalho remoto pode deixar a sua empresa vulnerável em termos de segurança. Se há algo que podemos afirmar acerca cibercriminosos, é que não hesitam em agarrar toda e qualquer oportunidade. Utilize esse passo a passo da lista de verificação para ajudar na proteção da força de trabalho em qualquer localização.

☐ Ajuste suas políticas de senha

Se você não era atento a isso, agora é a hora de fortalecer suas políticas. Exija senhas longas (ou ainda melhor, frases de segurança) e mudanças regulares de senhas, e bloqueie contas após um certo número de tentativas de login. Explique aos funcionários que não podem reutilizar suas senhas de trabalho em nenhum de seus logins pessoais.

☐ Demande a autenticação multifatorial (MFA)

Também conhecida como autenticação de dois fatores (A2F), que é, sem dúvidas, sua melhor defesa contra cibercriminosos que se valem de técnicas coercitivas, pulverização de senhas ou credenciais roubadas e compradas na dark web para se disfarçarem de funcionários e se infiltrarem na sua rede. Se você utiliza e-mail em nuvem, suítes de produtividade ou outros aplicativos, acione a AMF se estiver disponível. Se os usuários precisarem acessar sua rede interna, instale uma solução de AMF.

☐ Demande uma VPN para acessar sua rede interna

Uma VPN criptografa seu tráfego corporativo ao atravessar a internet pública, de forma que não possa ser lido por invasores. Além disso, uma conexão VPN permite que a sua equipe de TI amplie ainda mais as medidas de segurança da sua rede interna para dispositivos remotos. Se você já usa uma VPN com alguns funcionários, certifique-se de que há licenças e capacidade suficientes para cobrir todos os funcionários novos. Se os funcionários forem acessar recursos na sua rede interna, a combinação de uma VPN e AMF é indispensável.

☐ Se possível, use uma solução de interface de área de trabalho virtual

Com esse tipo de solução, os funcionários acessam uma máquina virtual, que está na nuvem ou no seu centro de dados, controlada remotamente. Pode ser configurada para ser exatamente igual a um sistema de escritório. A vantagem é que dados ou arquivos sensíveis existem apenas na máquina virtual, e nunca ficam armazenados no sistema de casa do funcionário.

☐ Lembre seus funcionários de estarem atentos à rede e terem cuidado com seu Wi-Fi

A rede doméstica de seus funcionários e outros dispositivos à ela conectados é algo que está completamente fora de seu controle. Peça que desliguem qualquer compartilhamento de arquivos no sistema que estiverem usando para trabalhar e que verifiquem o roteador de casa ou ponto de acesso Wi-Fi para ter certeza de que a segurança WPA2 está ativada. Lembre-os de que nunca devem se conectar a pontos de acesso de Wi-Fi público ou inseguro que não peça uma chave de segurança.

Invista na segurança de endpoint com recursos completos para seus funcionários

Não se pode confiar em um antivírus que já veio com um sistema doméstico ou em um dispositivo pessoal para protegê-los. Uma solução completa é capaz de proteger contra todos os tipos de ameaças com múltiplas camadas de defesa, incluindo um firewall pessoal, proteção contra sites maliciosos e malware em discos USB portáteis. A melhor opção é um suíte de segurança de endpoint corporativo que seu departamento de TI consiga administrar remotamente.

Exija criptografia caso os funcionários forem trabalhar em arquivos sensíveis

Se os funcionários forem baixar arquivos corporativos em seus dispositivos pessoais, forneça uma solução de criptografia para eles. Ressalte que devem manter seus arquivos pessoais separados de documentos corporativos, e que devem salvar os documentos corporativos em uma pasta criptografada. Além disso, implemente uma política para que salvem documentos revisados no armazenamento de dados corporativos para que você não se preocupe quanto ao backup remoto.

Instaure o hábito de fazer log out

Sempre que os funcionários forem almoçar, terminarem seu dia de trabalho ou precisarem se afastar de seu dispositivo por mais de um ou dois minutos, devem fazer log out da rede corporativa. É um bom hábito a ser mantido. E essencial se o computador for compartilhado ou outras pessoas em casa tiverem acesso a ele.

Estimule a realização de ajustes e atualizações

Informe seus funcionários remotos para ativarem atualizações automáticas em todos seus sistemas, a fim de garantir que estejam em dia com todas as medidas de segurança. Verifique se o seu ambiente interno também está atualizado, especialmente itens e sistemas de segurança fundamental que podem ficar sem ajustes por funcionarem 24/7. Tenha muito cuidado com máquinas conectadas no ambiente doméstico que operam com Windows 7, que já não é mais atualizado. Talvez seja necessário bloquear o acesso até que seja atualizado para uma versão suportada.

Forneça treinamento em segurança cibernética para os funcionários

Ainda que você utilize muita tecnologia para trabalhar, outro fator de proteção importante reside no ouvido de seus funcionários. Notícias falsas de trabalho para confirmar credenciais de login, acessar sites relacionados à empresa, lidar com solicitações do chefe para facilitar um pagamento ou transferir fundos, e outros golpes aparecerão com frequência , conforme cibercriminosos tentam se aproveitar de funcionários trabalhando de casa. Os funcionários bem informados e atentos são menos propensos a caírem nessas armadilhas. Ainda mais quando estiverem trabalhando de forma remota, um programa de treinamento regular irá mantê-los protegidos.

Agora, a notícia boa

Suítes de produtividade na nuvem, colaboração on-line por meio de chats e conferências e outras tecnologias de acesso remoto e conexão na internet são capazes de manter os funcionários tão produtivos quanto são no escritório – muitas vezes, até mais. Assim que levarem seu trabalho para casa com eles, lembre-se .

Para mais informações sobre as soluções de segurança da ESET, acesse: www.eset.com/br