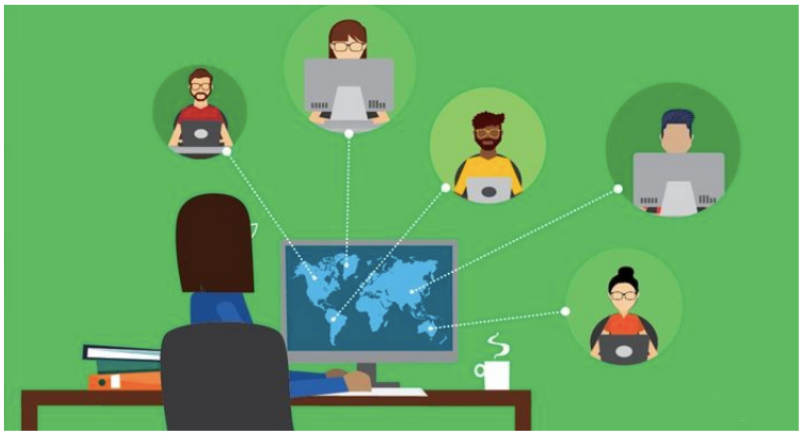
Artigo: As melhores práticas para garantir a segurança de dados durante o trabalho remoto

de João Monteiro — 18 de maio de 2020 no Artigos 0



Compartilhar no Facebook Compartilhar no Twitter

**Por Snehaa Elango*

A covid-19 interrompeu rotina de muitos ao redor do mundo em um período surpreendentemente curto. Com grande parte da população global sob quarentena, muitas organizações adotaram medidas temporárias de home office para se manterem funcionais. Os administradores de sistema estão sob pressão para garantir a continuidade dos negócios durante a pandemia. Além de permitir que os funcionários acessem os recursos organizacionais remotamente, os profissionais com esse cargo devem, também, garantir que a segurança não seja comprometida no processo.

67% de profissionais brasileiros não receberam orientações de cibersegurança para o trabalho remoto

De acordo com a Axur, empresa brasileira de monitoramento e reações a riscos digitais, que divulgou o Relatório de Atividades Criminosas Online no Brasil referente ao primeiro trimestre de 2020 e alguns números chamam muito atenção: 10.910 ataques de phishing foram detectados no Brasil durante os primeiros três meses do ano, número recorde. Pela primeira vez no Brasil, 35,9% desses ataques afetaram bancos e instituições financeiras. O relatório aponta, também, que os ataques aumentaram ainda mais por conta da pandemia do COVID-19, colocando em risco as organizações.

Não são apenas as organizações privadas que estão em risco, os departamentos governamentais são

Não são apenas as organizações privadas que estão em risco, os departamentos governamentais são igualmente vulneráveis. Recentemente, foi relatado que o site do Departamento de Relações Públicas de Kerala foi invadido por criminosos, que coletaram dados pessoais pertencentes a milhares de usuários registrados.

À luz da incerteza econômica devido à pandemia, as organizações não podem permitir que ocorram grandes violações de segurança. Quando os dispositivos corporativos são usados para necessidades pessoais, basta um aplicativo errado para colocar os dados empresariais em risco por uma violação de segurança. Quando esses dispositivos deixam a segurança de sua rede, bloquear ou manter uma vigilância cuidadosa sobre eles é, geralmente, a aposta mais segura.

As práticas recomendadas abaixo podem ajudar os administradores de TI em suas tarefas, tanto durante esse período de crise quanto depois.

1. **Impedir ataques drive-by**

Os ataques drive-by são um dos métodos de entrega de malware mais usados.
Os cibercriminosos identificam sites não seguros e injetam códigos maliciosos. Quando usuários inocentes chegam a essas páginas, o malware é baixado no sistema. Esses downloads geralmente acontecem sem nenhuma interação do usuário.

Para impedir o acesso a sites perigosos, ative a navegação segura para Chrome e Firefox e o filtro SmartScreen para Microsoft Edge e Internet Explorer. Esses recursos garantem que os usuários não acessem sites infectados.

Administradores de sistema também devem usar um filtro da web para restringir downloads somente para sites confiáveis. Dessa forma, se os usuários acessarem sites maliciosos, apesar do modo de navegação segura e do filtro SmartScreen, os downloads maliciosos ainda serão bloqueados.

2. **Detecte e remova extensões prejudiciais**

As extensões do navegador aprimoram sua experiência de navegação, mas exigem permissões do usuário para acessar vários aspectos do sistema. Com as políticas de home office embaçando as linhas entre a navegação comercial e a pessoal, as extensões adicionadas às necessidades pessoais também poderiam estar minerando dados corporativos. Por isso, os administradores de sistema precisam acompanhar as extensões instaladas nos dispositivos corporativos e remover as que não são necessárias para fins comerciais.

Uma vez concedida a permissão, muitas extensões leem o conteúdo presente em qualquer página da web que o usuário visite, rastreiam o histórico de navegação, fazem alterações no conteúdo da web e executam outras ações potencialmente comprometedoras. Todas as informações presentes em um navegador deixam de ser seguras depois que um usuário instala uma extensão de fonte questionável ou usa uma extensão que não possui um banco de dados na nuvem adequadamente protegido.

3. **Bloqueie aplicativos não autorizados e implemente a segurança doendpoint**

Um bom número de aplicativos gratuitos está prontamente disponível dentro e fora da nuvem, e os funcionários costumam usar essas ferramentas para realizar seu trabalho com mais eficiência. Quando eles desfrutam desses aplicativos gratuitos sem a aprovação da equipe de TI, colocam os dados corporativos em risco e deixam os administradores tentando, em vão, garantir a segurança dos dados.

Os administradores de sistemas precisam acompanhar o uso para identificar e bloquear o acesso a aplicativos não autorizados. Quando acompanhar os dispositivos corporativos é uma necessidade, uma ferramenta de gerenciamento unificado de endpoints pode ajudar muito esses profissionais. O gerenciamento e a segurança de endpoints são essenciais para as organizações, independentemente de onde seus usuários estão trabalhando. As equipes de TI podem bloquear pontos de extremidade para restringir o acesso apenas a sites e aplicativos autorizados.

Hoje, com os usuários trabalhando remotamente, essas medidas de segurança são necessárias para garantir que os dados corporativos estejam seguros e que os funcionários permaneçam produtivos.

**Snehaa Elango é consultora de Produtos da ManageEngine.*

Tags: aplicativo | Axur | drive-by | endpoint | ManageEngine | prática | Segurança | trabalho remoto

Postagem Anterior

Covid-19: Vivo doa link de internet ultra rápida para hospital de campanha no RJ

Próxima Postagem

Covid-19: laboratório do BID cria rede para compartilhamento espontâneo de dados pessoais

Linx vai distribuir solução para acelerar migração de farmácias para o e-commerce

19 DE MAIO DE 2020

CenturyLink Brasil doa links de acesso à internet para hospitais públicos em SP

19 DE MAIO DE 2020

Crise da Covid-19 terá impacto leve sobre os negócios nas áreas de cloud e cibersegurança

19 DE MAIO DE 2020

Pesquisa aponta que 76% executivos temem que sua empresa tenha alguma brecha de segurança

19 DE MAIO DE 2020

João Monteiro

Discussão sobre isso post

0 comentários Classificar por Mais antigos

Adicione um comentário...

Plugin de comentários do Facebook