Notificação de Incidente

Riscos decorrentes do uso dos *stories* no LinkedIn

cipher 20 ANOS
a PROSEGUR company

ACESSO AO DOCUMENTO:

SUMÁRIO EXECUTIVO

No dia **24 de setembro de 2020**, o LinkedIn apresentou uma nova funcionalidade para o mundo: **histórias** (mais conhecida como **stories**). Mas esse formato de postagem nas redes sociais não é novo. Em 2011, o **Snapchat** foi o primeiro a lançar esse tipo de publicação, neste caso voltado para o público adolescente, que não queria que seu conteúdo postado permanecesse para sempre na internet. Naquela época, o mais preocupante era que esses jovens compartilhavam imagens ou vídeos íntimos entre si nessa modalidade.
Porém, quando esse formato atingiu outras redes sociais ou serviços de mensagens como o Facebook, WhatsApp ou Instagram, ficou claro que **as publicações feitas por meio de stories, mesmo que excluídas da rede social após 24 horas**, podem ficar registradas durante esse período para serem retransmitidas em outros canais. Existem métodos para registrar as publicações no modo story, alguns deles tão simples como fazer uma captura de tela ou vídeo no próprio dispositivo móvel. Por último, embora a ferramenta agora lançada pelo LinkedIn siga um modo de operação bem semelhante ao que tornou o Snapchat famoso, o público-alvo não é o mesmo e os riscos, embora semelhantes, também são outros.

REVISÕES

Data	Descrição da Revisão	Revisor(es)
Out/2020	Riscos decorrentes do uso dos stories no LinkedIn	Equipe de Serviços de Inteligência Cibermética

Stories do LinkedIn

O que é?

Os ***stories*** são uma funcionalidade nova que permite a você publicar fotos e vídeos curtos que ficarão disponíveis por 24 horas a partir da publicação no seu perfil do LinkedIn. Totalmente diferenciados do restante do conteúdo, eles aparecem em fila na parte superior da tela principal do aplicativo. Esta função é **exclusiva dos aplicativos móveis do LinkedIn**, o que significa que no momento eles não podem ser visualizados nem produzidos na versão web.

Para que servem?

De acordo com um post de Pete Davies, diretor de Produtos de Consumo em um blog na rede social, a empresa estava procurando uma forma rápida para os **membros interagirem em um contexto profissional**. Em outras palavras, a rede social incentiva o compartilhamento de vídeos e imagens da **rotina de trabalho**, o que pode ser um risco em termos de privacidade para qualquer empresa.

Quem pode ver os stories?

Seus **contatos de primeiro grau e seguidores** poderão ver os stories por um período de **24 horas** assim que forem publicados. Eles também podem **compartilhar esses stories com qualquer outra pessoa** dessa rede social por meio de mensagens privadas. Não existe nenhuma restrição de privacidade que limite essa ação. Por isso, tome cuidado especial com todas as informações que você decidir compartilhar por meio dessa ferramenta e, ainda mais, com os membros com os quais se conecta.

Tipologia de riscos e recomendações

O **LinkedIn incentiva os usuários a se conectarem** com outros membros dessa rede social com os quais você tenha algum tipo de vínculo educacional (mesma universidade) ou profissional (mesma

empresa ou setor)**, ainda que não seja necessariamente alguém que você conheça**, com o objetivo de expandir sua rede de contatos profissionais.
Por isso é importante que os usuários **revisem sua lista de amigos e mantenham só as pessoas que realmente conhecem** e em quem eles confiam. Caso contrário, a pessoa e/ou a empresa onde eles trabalham podem se expor a uma série de riscos de vários tipos: **físicos,** à reputação ou **tecnológicos**. Um criminoso cibernético pode se esconder atrás de qualquer tipo de identidade na Internet.

Riscos físicos

Os **maiores riscos para as empresas e sua segurança** não vêm dos criminosos cibernéticos nem de graves vulnerabilidades do sistema, mas dos próprios funcionários da empresa. Eles têm acesso fácil **aos computadores, arquivos e a todos os tipos de informações confidenciais**. O uso indevido dos *stories* poderia
resultar na divulgação. Portanto, não só da privacidade de uma pessoa, mas também de dados sigilosos da própria empresa, sem contar que pode **facilitar a localização das pessoas.**
As imagens ou vídeos veiculados neste meio, podem revelar informações sobre a localização de quem está publicando o conteúdo. Últimamente, tem havido casos de pessoas que postaram fotos, por exemplo, de **passagens aéreas** de viagens de negócios.
Além da localização e destino, o rastreamento desses documentos permite obter **dados pessoais** do usuário, o que pode levar a um outro tipo de risco e facilitar um ataque de engenharia social.
De uns anos para cá estamos vendo também a presença cada vez **maior de executivos de grandes empresas nas redes sociais**. Geralmente isso faz parte de ações de comunicação específicas dessas empresas que buscam maior proximidade com clientes em potencial. Porém, qualquer post que esses perfis façam em eventos ou congressos ou no seu dia-a-dia, facilita a localização deles. Isso ganha importância quando é uma ferramenta como o *Stories* que incentiva a publicação de conteúdo gerado em um momento específico.

Alguns usuários já estão postando informações confidenciais usando esta ferramenta.

Riscos à reputação

Quando usar uma conta corporativa ou de um **executivo com exposição significativa na mídia**, é aconselhável estabelecer algumas diretrizes ou designar um responsável que defina a imagem que se deseja passar e que conteúdo será publicado.
O uso dessa nova função pode levar a **publicar conteúdo de forma mais espontânea e com menos limitações do que o habitual**. A publicação de juízos de valor nesses tipos de perfis ou a troca de comentários com mais veemência podem prejudicar não só a reputação pessoal do executivo, mas também da própria empresa que, inevitavelmente, esta rede social representa.
Por isso, apenas alguns **funcionários autorizados cientes da estratégia da empresa,** devem ter acesso para publicação de conteúdo. Isso não se limita só aos *stories*, mas a todas as contas de mídia social da empresa ou dos seus executivos.
Da mesma forma, até mesmo o uso do LinkedIn por funcionários em seus perfis pessoais pode causar **danos à imagem da empresa**. Isso porque a forma como eles se apresentam nas redes sociais, continua vinculada aos seus empregadores atuais e anteriores, mesmo que implicitamente.

Riscos tecnológicos

Finalmente, há uma série de riscos tecnológicos, principalmente derivados do uso incorreto **dessa nova função do LinkedIn**, que podem comprometer ou expor dados pessoais ou informações dos usuários:

- **Risco de usar aplicativos de terceiros**. Outro perigo é usar **aplicativos de terceiros** (ou seja, aplicativos que não são criados pelo LinkedIn), pois é possível que alguns deles sejam na verdade spywares dedicados à coleta de fotos e vídeos privados (ou outros tipos de dados). Por exemplo, poderia ser criado um aplicativo que permita aos usuários aplicar filtros virtuais para melhorar a estética dos seus posts. Quando os usuários instalam esses aplicativos, geralmente concordam com os termos de uso e as políticas de privacidade sem ler o texto com cuidado, que pode incluir concessão de permissões ao aplicativo.

- **Riscos do uso de extensões não oficiais do navegador**. Por ser uma função disponível apenas na versão móvel, os usuários podem recorrer ao download de **extensões não oficiais do navegador** (ou seja, não criadas pelo LinkedIn) para que possam usar os *stories* também na versão para web. Ao instalar esse tipo de extensões, é necessário verificar sua titularidade ou autoria, uma vez que, como no caso anterior, extensões não oficiais podem ser programas maliciosos dedicados ao roubo de informação.

- **Riscos de exposição de informações pessoais**: Se um usuário está compartilhando suas atividades diárias por meio dessa função, é importante que ele se certifique com quem essas informações estão sendo compartilhadas. Isso porque os criminosos cibernéticos aproveitam os dados que coletam nas redes sociais para, posteriormente, fraudar e enganar suas vítimas. Um exemplo claro desse caso é o ***phishing***. Além das informações publicadas no LinkedIn sobre o cargo ou empresa em que a pessoa trabalha, os *stories* permitem que o criminoso cibernético saiba mais detalhes pessoais do usuário: seus colegas de trabalho próximos, cargo ou ainda, características da sua personalidade. Isso facilita o uso de técnicas de engenharia social para gerar confiança na vítima e induzi-la a ações indevidas, por exemplo, fazendo-se passar por uma pessoa da empresa em uma aparente comunicação eletrônica oficial.

- **Risco de vazamento de dados**: Quando os usuários postam fotos e vídeos, os arquivos ficam armazenados nos servidores do LinkedIn. Portanto, os criminosos cibernéticos que conseguem violar as barreiras de segurança dessa empresa podem descobrir o código do arquivo, encontrar sua URL e baixá-lo.

Conclusões

A forma de usar uma rede profissional como o LinkedIn é diferente da forma de usar outras redes como o Facebook ou o Instagram. O objetivo do LinkedIn é **conectar pessoas** com outros profissionais para criar uma rede que agregue valor à carreira profissional de cada pessoa. Não precisam ser necessariamente pessoas com as quais temos um **relacionamento pessoal**.

Assim, a idéia de que uma publicação no LinkedIn *Stories* desaparecerá depois de 24 horas dá uma **falsa sensação de privacidade** e as informações publicadas atingem um círculo bem maior do que gostaríamos. Além disso, se você incluir qualquer tipo de **informação pessoal**, ela poderá ser exposta e caracterizar um vazamento de **informações** dos seus dados ou da empresa onde você trabalha.

O LinkedIn permite que seus contatos compartilhem os seus *stories* com qualquer pessoa nessa rede social por meio de mensagens privadas e não há nada que você possa fazer para evitar isso. O segredo é ter muito cuidado com as informações que você decidir compartilhar usando essa ferramenta.

Quem deve redobrar a atenção são os **executivos**, que não estão habituados a redes sociais e que lidam com muitas informações confidenciais.

Recomendações

Abaixo estão sugestões que deveriam ser seguidas para mitigar os riscos que o uso desse tipo de ferramenta pode acarretar:

- As empresas devem **treinar** os funcionários sobre como usar bem as redes sociais, especialmente no ambiente de trabalho. As redes conseguem determinar quem dentro de uma empresa pode ser mais suscetível a postar informações confidenciais usando essas ferramentas, às vezes até por negligência ou sem intenção.

- Devem ser definidas algumas **diretrizes** sobre o uso do perfil tanto corporativo como dos executivos com exposição significativa na mídia. Pode-se avaliar a indicação de um gerente de conteúdos de redes sociais que conheça a estratégia da empresa e os riscos aos quais a empresa e os seus funcionários estão expostos.

- Muitos **aplicativos de terceiros** solicitam permissão para acessar dados do usuário e fazer login em nome dele. Verifique com quem essas informações são compartilhadas e tente limitar o uso desse tipo de aplicativos ao estritamente necessário.