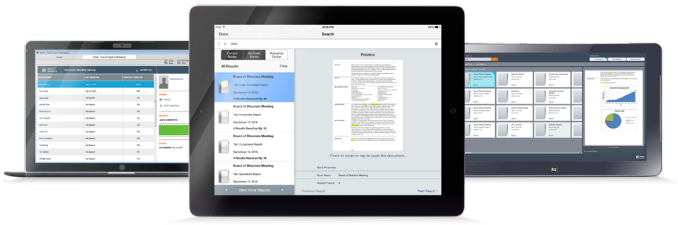
Diligent

Aproveitando todo o potencial da informação. De maneira segura.

A Diligent ajuda as organizações mais importantes do mundo a aproveitar todo o potencial da informação e da colaboração de maneira segura, capacitando conselhos e equipes de gestão a tomar as melhores decisões. Mais de 4.000 clientes, em mais de 70 países, contam com a Diligent para ter acesso imediato às suas informações mais urgentes e confidenciais, apoiados por ferramentas de análise, discussão e colaboração com os principais tomadores de decisão. O Diligent Boards agiliza e simplifica como o material do conselho é produzido e distribuído através de navegadores e dispositivos para iPad e Windows. Ele também oferece vantagens práticas, como redução nos custos de produção, apoio às metas de sustentabilidade e economia de tempo administrativo e de TI.

Junte-se aos líderes. Seja Diligent.



Para obter mais informações ou solicitar uma demonstração, entre em contato hoje mesmo:

Tel.: 0800-591-9013
E-mail: info@diligent.com
Site: www.diligent.com

AICPA SOC | ISO 27001 CERTIFIED BY BRIGHTLINE | Baixar na App Store | Obter para Microsoft

Diligent é uma marca comercial da Diligent Corporation, registrada nos Estados Unidos. As marcas comerciais de terceiros pertencem aos respectivos proprietários. ©2016 Diligent Corporation. Todos os direitos reservados.

Ameaça cibernética e a segurança do conselho: **três equívocos que prejudicam a segurança da sala de reuniões**

Ben Bourne
Diretor de Sucesso do Cliente, Região EMEA

Magdalena Borcal
Diretora de Sucesso do Cliente, Região EMEA

Nathan Birtle
VP de Vendas e Desenvolvimento Comercial, Região EMEA

O número de ataques cibernéticos tem aumentado no mundo inteiro. Os criminosos estão cada vez mais hábeis em contornar os sistemas de segurança, e falhas graves são veiculadas regularmente na mídia internacional. Apesar disso, muitos conselhos ainda ignoram a ameaça imposta pelo crime cibernético e, entre os que já tomaram precauções, muitos não conseguem blindar-se adequadamente. Em resposta, publicamos este artigo com o intuito de ajudar diretores e gerentes a compreender melhor a questão do crime cibernético e mostrar a eles como reduzir o risco de segurança para os conselhos.

Há muitos fatores que sustentam o crescimento do crime cibernético. A probabilidade de ser pego é baixa em comparação com outros tipos de crime; os dados podem ser encaminhados através de milhares de computadores para que os ataques sejam anônimos e indetectáveis. Os criminosos cibernéticos podem esperar um retorno financeiro na ordem de milhões. A maioria dos crimes é cometida pelo crime organizado, e os analistas estimam que o crime cibernético custe à economia global USD 455 bilhões por ano.[1]

Um ataque bem-sucedido pode causar danos gigantescos a uma organização. Além das perdas financeiras, o roubo de dados e de propriedade intelectual pode prejudicar o comércio, a competitividade, a inovação e a reputação. Repensando a forma como trabalham com os dados e protegem as informações, as organizações podem resguardar-se para limitar sua exposição a ataques.

1 "Net Losses: Estimating the Global Cost of Cybercrime,
" McAfee, 2014. http://www.mcafee.com/uk/resources/reports/ rp-economic-impact-cybercrime2-summary.pdf

Diligent

AVALIANDO SEU CONSELHO

Como tomadores de decisão na organização, os conselhos precisam compreender as ameaças existentes, mas isso às vezes é difícil. Muitos diretores podem não perceber o quanto os processos de negócios estão cada vez mais digitais e não reconhecer como a convergência entre TI, Tecnologia Corporativa e Tecnologia Operacional tem moldado as atividades operacionais e aberto fendas profundas para os criminosos cibernéticos.

As estruturas hierárquicas dentro da organização também devem ser levadas em conta. O fato de o conselho estar posicionado "acima" da organização significa que a equipe responsável pela segurança organizacional pode não se sentir à vontade o suficiente para relatar quaisquer dúvidas sobre o esquema de segurança da empresa. Uma pesquisa realizada pela Deloitte em parceria com a Systemec sugere que, em algumas regiões, até 70% dos responsáveis por tomadas de decisão não confiam nas políticas de segurança de suas empresas e conclui que mais de dois terços das organizações não têm capacidade para se proteger contra ataques.[2] Da mesma forma, a equipe de segurança pode não estar ciente de que a segurança do conselho faz parte de suas atribuições, presumindo, em vez disso, que esta seja de competência da secretaria corporativa, e não do esquema de segurança da própria organização.

"Os conselhos precisam compreender as ameaças existentes às suas organizações, mas isso pode ser difícil, pois muitos diretores podem não perceber o quanto os processos de negócios estão cada vez mais digitais."

Outro fator são as ações dos próprios diretores que contribuem para aumentar o risco de segurança potencial do conselho. Ao optar por acessar, armazenar e distribuir documentos de maneira insegura, mas prática, os diretores expõem potencialmente esses dados a terceiros e perdem o controle que têm sobre eles. E-mail, PDF e sistemas de armazenamento em nuvem, por exemplo, tendem a ser muito menos seguros do que os métodos empregados pela organização.

Os diretores e toda a equipe precisam ser diligentes em relação à tecnologia da comunicação. No entanto, as práticas de trabalho mais seguras ainda assim podem ser prejudicadas pelos equívocos associados à tecnologia e aos fluxos de trabalho em uso.

OS TRÊS EQUÍVOCOS DE SEGURANÇA

Para evitar que os diretores trabalhem de maneira a prejudicar a segurança de seu conselho, é necessário considerar os equívocos a seguir:

1. O e-mail é seguro

Embora o uso de e-mail seja prático, rápido e fácil como um meio de comunicação de informações confidenciais, ele simplesmente não se adapta a essa finalidade, pois não é possível restringir o encaminhamento do conteúdo. Além disso, cancelar uma mensagem enviada é difícil. Portanto, assim que o e-mail é enviado, o remetente perde o controle da informação.

2. Proteção de senha significa segurança

Embora seja razoável supor que adicionar uma senha a um PDF o torna inacessível a usuários não autorizados, uma pesquisa rudimentar em qualquer mecanismo de pesquisa popular produz milhões de resultados mostrando a qualquer um como contornar a segurança de um PDF. Faça essa pesquisa no Google, e você encontrará mais de 2.300.000 resultados documentando como é simples violar esse meio aparentemente seguro. A verdade é que a tecnologia de PDF não é segura e você não deve confiar nela.

3. O armazenamento de dados local é mais seguro

Talvez o equívoco mais importante esteja relacionado ao armazenamento de dados, especificamente ao fato de que armazenar dados localmente é mais seguro do que armazená-los em instalações de terceiros. Na verdade, frequentemente ocorre o contrário. Por exemplo, as soluções locais dependem dos próprios administradores da organização para acessar e gerenciar os dados, mas 55% dos ataques cibernéticos podem ser realizados por pessoal interno, cujo acesso pode mostrar-se catastrófico.[3] Da mesma forma, em termos técnicos e operacionais, o programa e a infraestrutura de segurança da própria organização podem não ser suficientes para proteger os dados contra as ameaças de hoje. Por outro lado, um fornecedor de SaaS como a Diligent restringe o acesso a dados apenas a usuários que sejam clientes finais autorizados. Nossa equipe não tem acesso aos dados do cliente. Além do mais, auditamos completamente as políticas de segurança, fornecendo backup de dados e funções de recuperação de desastres, bem como monitoramento de segurança acima e além das capacidades da maioria das outras organizações. Além disso, realizamos uma auditoria completa das políticas de segurança, fornecendo recursos de backup de dados e recuperação de desastres, bem como monitoramento de segurança muito superior à capacidade da maioria das outras organizações.

2 Global Risk Insights, Setembro de 2015. "globalriskinsights. com/2015/09/how-strong-are-the-middle-easts-cybersecurity-net-works/
3 "IBM 2015 Cyber Security Index" e "IBM X-Force Threat Intelligence Quarterly Q2 – 2015" https://securityintelligence.com/ the-threat-is-coming-from-inside-the-network/

AVALIANDO A SEGURANÇA DO CONSELHO

Os líderes que desejam avaliar suas práticas de segurança cibernética relacionadas ao conselho podem fazer isso por meio de três perguntas simples:

Como são armazenados os dados do conselho?

Qualquer avaliação de segurança deve começar examinando-se quem controla os dados. Não saber onde a informação está e não poder controlar para onde ela vai significa que a solução é altamente insegura.

Esta é a razão pela qual enviar documentos do conselho como arquivos PDF não representa uma solução segura. Os arquivos podem ser acidentalmente encaminhados por diretores para outras pessoas de fora do conselho ou alojados em contas de e-mail pessoais, com segurança de nível de consumidor mínimo, em sistemas que os próprios fornecedores admitem não ser seguros.

O mesmo vale para soluções baseadas em "nuvem", que podem armazenar seus arquivos em qualquer servidor da rede de compartilhamento de arquivos e você não tem como saber exatamente onde eles estão. O sucesso das soluções em nuvem baseia-se na suposição de que elas são seguras, quando, na realidade, casos de hacking de grande repercussão, como revelação de senhas e fotos de celebridades a partir de provedores de serviço de nuvem[4], demonstram como são falhas essas suposições de segurança.

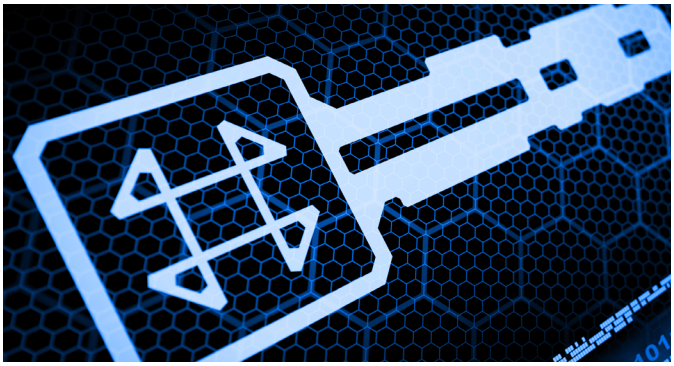
Embora os portais para a hospedagem de conselhos pareçam iguais a uma nuvem e sejam com frequência incorretamente referidos como "armazenamento em nuvem", há diferenças importantes: os portais para conselhos controlam cuidadosamente onde seus dados são armazenados e mantêm segregadas as informações de cada organização hospedada. Saber onde os dados estão localizados e como são protegidos proporciona maior controle e garantia sobre quem tem acesso às informações.

Qual é o nível de proteção dos bloqueios?

Embora seja fundamental saber onde os dados estão localizados, também é crucial garantir que apenas usuários autorizados possam acessá-los. Isso pode ser realizado por meio da criptografia de dados, ou seja, convertendo os dados em uma cadeia de 0s e 1s sem sentido, de maneira que somente aqueles que possuam a chave digital correta possam decifrá-la.

Pacotes do conselho em papel não possuem nenhuma chave digital. Portanto, qualquer pessoa que tenha uma cópia pode ler as informações. Embora possa ser verdade que os PDFs enviados por e-mail ou armazenados em sistemas de compartilhamento de arquivos possam ser criptografados e ter suas senhas protegidas, isso coloca o ônus de gerenciar os protocolos de senha sobre quem está distribuindo e recebendo o material. Mesmo nesse caso, os documentos PDF permanecem vulneráveis a ataques de "força bruta", que usam prontamente o software disponível.

Portais para a hospedagem de conselhos de alta qualidade normalmente usam criptografia de 256 bits e, como há mais combinações possíveis do que estrelas no universo, é seguro dizer que, para quebrar o código, demoraria uma eternidade, até mesmo para os hackers mais determinados usando a tecnologia mais avançada.



Quem controla as chaves?

Não importa o quanto o sistema de criptografia é forte: alguém com a chave certa ainda assim poderia acessar as informações. A pessoa que tenha em mãos a senha de um PDF protegido por senha praticamente possui o documento. Senhas roubadas significa documentos roubados.

Porém, um portal forte nunca perde o controle sobre os documentos. A pessoa que faz logon só visualizará aquilo para a qual tem permissão. Além disso, se uma senha é roubada, o administrador pode simplesmente negar o acesso a essa senha.

No caso de usuários autorizados, os administradores podem limitar o acesso a documentos específicos, bem como atribuir acesso e visibilidade de documentos a determinado grupo de usuários; por exemplo, um comitê de compensação pode preferir negar o compartilhamento de suas informações com o conselho como um todo.

O administrador de um portal para conselhos pode controlar também o acesso ao dispositivo, restringindo o acesso do diretor a dispositivos pessoais menos seguros e obrigando o acesso por meio de sistemas de propriedade da organização. Igualmente, quando documentos confidenciais não são mais necessários, o administrador pode realizar uma "limpeza virtual", fechando os documentos para todos os usuários que tentem acessar os arquivos. De forma semelhante, o acesso pode ser restrito de acordo com o usuário ou dispositivo, o que é útil se um diretor deixa o conselho e há material a ser recuperado, ou se uma senha foi roubada.

UM EXEMPLO SEGURO

A segurança cibernética, particularmente a segurança das informações e dos dados do próprio conselho, devem se de consideração primordial. Ter um portal para conselhos para a gestão segura e intuitiva de todas as suas informações, incluindo os processos de comunicação e colaboração, aumenta a segurança do conselho e melhora as práticas de trabalho.

Quando um conselho não consegue aplicar padrões de segurança de alto nível, o esquema de segurança da organização como um todo pode ser prejudicado. No entanto, quando um conselho lidera pelo exemplo, a segurança da organização torna-se cada vez mais eficiente e robusta face às crescentes ameaças.

4 BBC News, http://www.bbc.co.uk/news/technology-29011850