Expondo as Lacunas da Cibersegurança: Brasil

Parte 2: Obstáculos, Renovação e Aumento da Educação em Segurança

Patrocinada por Websense, Inc.

Realizada de forma independente pelo Instituto Ponemon LLC

Data da Publicação: 17 de Julho de 2014

Expondo as Lacunas da Cibersegurança: Brasil
Parte 2: Obstáculos, Renovação e Aumento da Educação em Segurança

17 de julho de 2014

O Instituto Ponemon tem o prazer de apresentar o segundo relatório de seu estudo em duas partes, Expondo as Lacunas da Cibersegurança: Brasil, patrocinado pela Websense, Inc. Esta é a segunda e última parte de uma série sobre os desafios que profissionais de segurança de TI enfrentam ao lidar com riscos digitais. Neste relatório, é revelado como a melhoria nas comunicações e informações sobre segurança digital, o investimento certo em pessoal qualificado e tecnologias de base, e a adoção de medidas de segurança minimizarão o risco atual e emergente de ameaças virtuais.

Foram entrevistados 392 profissionais de TI e segurança de TI no Brasil, com uma média de oito anos de experiência em campo. Além do Brasil, esta pesquisa também foi realizada em 14 outros países – EUA, Canadá, Austrália, China, Hong Kong, Cingapura, Índia, Reino Unido, Alemanha, França, Holanda, Suécia, Itália e México. Este relatório abrange as conclusões do Brasil.[1]

Estas são as conclusões mais destacadas desta pesquisa:

Obstáculos na comunicação são fatores que interferem para a redução do risco de um ataque digital. De acordo com os resultados, 36% das equipes de segurança digital nunca conversam com sua equipe executiva sobre segurança digital. Entre os que conversam, 22% só conversaram com uma frequência anual e 18% conversaram semestralmente. Apenas 1% conversaram semanalmente.

As organizações querem uma atualização de segurança. Os ataques persistentes de ameaças avançadas e roubo de dados estão entre os principais receios dos profissionais de segurança. Esses receios provavelmente decorrem das preocupações de que a tecnologia não os protegerá. Muitos gostariam de ver uma atualização completa de suas soluções de segurança, porque com frequência ficam desapontados com o nível de proteção por elas fornecido. Na verdade, 61% dizem que suas organizações ficaram muito frequentemente ou frequentemente desapontados com seus investimentos em segurança.

Se tivessem os recursos e a oportunidade, 31% dos entrevistados fariam uma renovação completa do sistema de segurança corporativo atual. 55% dizem que se suas organizações tivessem uma violação de dados, considerariam mudar de fornecedores de segurança. Mais da metade (61% dos entrevistados) dizem que planejam fazer investimentos e ajustes significativos em suas defesas de segurança digital nos próximos 12 meses.

Os profissionais de segurança sentem que os três principais eventos que motivariam os executivos a alocar mais dinheiro às iniciativas de segurança digital são: roubo de propriedade intelectual (75% dos entrevistados), perda de receitas devido a tempo de parada do sistema (57% dos entrevistados) e violação envolvendo dados de clientes (46% dos entrevistados).

Ameaças internas colocam a propriedade intelectual e os dados de clientes em risco. 78% dos entrevistados dizem que conhecem pessoalmente outro profissional de segurança cuja empresa teve dados sensíveis ou confidenciais furtados como resultado de uma ameaça interna.

---

[1] O relatório completo, *Expondo as Lacunas de Cibersegurança: Uma Perspectiva Global, Parte I: Deficiente, Desconectado e no Escuro* contém os resulatdos globais consolidados.

59% dizem que os dados furtados pelo funcionário eram informações de clientes e 55% responderam que propriedade intelectual foi roubada.

Para corrigir as falhas, promova a Educação Digital. Somente 42% dos entrevistados acreditam que sua empresa está investindo o suficiente em pessoal qualificado e tecnologias para a eficácia na execução de seus objetivos ou missão de segurança digital. Na verdade, 58% das empresas representadas nesta pesquisa não fornecem treinamento sobre segurança digital para os funcionários.

O conhecimento das ameaças digitais é considerado importante para administrar o risco digital. 23% dos entrevistados disseram que suas organizações passaram por um processo de treinamento em ameaças digitais em suas funções atuais. Daqueles que passaram, 92% consideraram importante para administrar o risco digital.

São muito poucas as empresas que adotam medidas internamente para lidar com ameaças novas e emergentes. Quando há conscientização sobre uma nova ameaça digital, a resposta primária é consultar os colegas do setor para descobrir o que pensam e contatar fornecedores de segurança para obter uma correção. Uma resposta pouco frequente é comunicar e informar o pessoal de TI (6%) ou ter “simulações de emergência” para determinar no nível de prontidão (4%).

O excesso de propaganda dos fornecedores de segurança leva a investimentos frustrantes em tecnologia? 66% dizem que os fornecedores de soluções de segurança exageram as ameaças e riscos que as empresas enfrentam. 61% dos entrevistados dizem que sua empresa comprou com muita frequência ou com frequência uma solução de segurança que desapontou.

O tempo de parada é o principal motivo para trocar de fornecedor de segurança. Os entrevistados revelam os motivos por que mudariam os fornecedores de segurança. Tempo de parada e implementação difícil ou interface de usuário complicada são os principais motivos para uma troca de fornecedores de segurança. 55% dizem que uma violação de dados resultaria em término do relacionamento com um fornecedor de segurança.

Os profissionais de segurança digital querem mais financiamento para combater ameaças. Para lidar com o cenário de ameaças desafiador e dinâmico, as organizações precisam ter a inteligência para antecipar, identificar e reduzir as ameaças.

Os profissionais de segurança não acreditam que estão obtendo o nível certo de investimento para poder concretizar seus objetivos e missão de segurança digital. Somente 42% dizem que suas empresas estão investindo o suficiente em pessoal qualificado e tecnologias para ser eficaz na execução de seus objetivos ou missão de segurança digital. 58% dos entrevistados dizem que não é suficiente ou não têm certeza sobre o nível de investimento.

Conclusão

Os resultados deste estudo expõem as lacunas em defesas de segurança digital que existem em muitas organizações. Como as empresas podem administrar melhor os ataques digitais direcionados para suas informações sensíveis e confidenciais? Estas são algumas recomendações:

- Eliminar a incerteza dos riscos digitais. Investir em tecnologias que forneçam visibilidade e detalhes sobre comportamento de alto risco, tentativas de ataques e as consequências de um ataque bem-sucedido em sua organização.
- Aprimorar o acesso a melhor inteligência de ameaças e defesas em tempo real.
- Implementar uma estratégia de defesa completa, que incorpore canais da web e e-mail, incluindo comunicações SSL/TLS. Evitar o foco em apenas um canal. Em vez disso, examinar todos os canais usados para interagir com informações.
- Avaliar recursos e implementações da solução de segurança quanto à abrangência da cadeia de ameaças para eliminar lacunas e minimizar sobreposição excessiva. Expandir além de defesas altamente dependentes da identificação de um ataque apenas no estágio de entrega de “malware”.
- Criar programas de formação e conscientização em segurança com foco na gravidade dos ataques de segurança e na importância de reduzir os comportamentos de alto risco.

Instituto Ponemon

Promovendo a Gestão Responsável das Informações

O Instituto Ponemon dedica-se a pesquisas independentes e educação para promover práticas responsáveis de gestão de informação e privacidade em empresas e no governo. Nossa missão é fazer estudos empíricos de alta qualidade sobre questões críticas que afetam a gestão e a segurança de informações sensíveis sobre pessoas e organizações.

Como membro do **Council of American Survey Research Organizations (CASRO)**, apoiamos normas rigorosas de confidencialidade de dados, privacidade e pesquisa ética. Não coletamos quaisquer informações com identificação pessoal de indivíduos (ou informações com identificação de organização em nossas pesquisas empresariais). Além disso, temos padrões de qualidade rigorosos para garantir que nossos entrevistados não ouçam perguntas não pertinentes, irrelevantes ou inadequadas.
entrevistados não ouçam perguntas não pertinentes, irrelevantes ou inadequadas.