



Política de acesso adequada, controle rigoroso e atualização constante do perfil do usuário, entre outras medidas, podem impedir vazamentos de dados dos hospitais

SIGILO MÉDICO NA WEB

ANALICE BONNATTO – editorialsau@itmidia.com.br

O controle de segurança para web e e-mails tem se tornado cada vez mais frequente nos hospitais brasileiros, mas ainda não conta com regras específicas. "Nos Estados Unidos, por exemplo, há lei sobre isso. Aqui, infelizmente, não há algo tão explícito, mas as empresas brasileiras começam a se preocupar com as informações sobre os diversos tipos de usuários", avalia o consultor Edison Fontes, que possui as certificações CISM, CISA, é professor de segurança da informação dos cursos de pós-graduação da FIAP e blogueiro do site ITWeb.

Dos usuários externos - o paciente que acessa a internet de casa para obter o resultado de um exame -, aos usuários internos de uma instituição hospitalar - áreas administrativa e médica, que podem colocar em risco dados corporativos, muitas vezes de forma acidental -, a maior preocupação é que o controle garanta a confidencialidade dos pacientes.

Fontes lembra também que as empresas às vezes se esquecem do essencial: as pessoas e os processos. "Esse processo tem de ser estudado e estruturado e aí entra a figura do gestor de segurança da informação, que fará com que as pessoas recebam essa mudança cultural de forma profissional. Ninguém gosta de ser controlado, mas será, porque trabalha com informações preciosas", diz Fontes.

Hoje, cada vez mais, a vida do hospital passa a depender dessas informações. "Antes era só controle administrativo, mas, hoje, há outras questões críticas, como o prontuário eletrônico, as escalas de operação, medicação, etc. Assim, os hospitais devem ter também um plano de contingência", diz Fontes.

PRODUTIVIDADE E REDUÇÃO DA BANDA CORPORATIVA

No Hospital Vera Cruz, em Campinas, no interior de São Paulo, mais de 17 mil pessoas acessam mensalmente o site da instituição para conhecer sua estrutura ou buscar serviços, como impressão de exames laboratoriais. Para garantir a segurança dos usuários, o hospital adotou, desde 2006, as soluções Websense, implementadas pela revenda Workhelp. A solução também foi adotada para as 300 pessoas que trabalham lá.

Para William Cândido de Oliveira, analista de segurança da equipe de TI do hospital, a rede ficou mais segura e houve uma economia de 30% em banda larga. "Nossa banda larga estava no gargalo e alguns usuários burlavam os acessos. Além disso, os softwares utilizados anteriormente não eram tão maleáveis na configuração de regras", diz.

Dessa forma, o hospital pôde criar perfis de acordo com cada departamento. O bloqueio é realizado por uma solução da Websense, que também impede o acesso a sites não-relacionados ao trabalho ou à produtividade

pessoal. Hoje, com exceção de médicos, coordenadores e gerentes, por exemplo, as pessoas só acessam e-mail particular das 11h às 13h. Sites pessoais são bloqueados e o uso do MSN é liberado mediante a solicitação de um coordenador.

Segundo Oliveira, o sistema é bem flexível. "Eu libero regras e permissões. Na pediatria, temos duas máquinas para crianças acessarem a internet, mas foram criadas listas de sites próprios para elas", diz o analista.

Ainda sobre redução de custos, segundo o gerente de desenvolvimento de canais da Websense para a América Latina, Marcos Prado, a área de e-mails é crítica para qualquer empresa, mas é possível fazer a segurança sem se preocupar com a infraestrutura, utilizando o sistema software as a service (SaaS - software como serviço). "Hoje, em média, 40% do link de internet de uma empresa é voltado ao uso de e-mail. Se 40% é e-mail, e o spam (mensagem eletrônica indesejada), segundo estatísticas, representa de 90% a 95% do tráfego de e-mails, então a empresa tem um custo de internet, mas, dos 40% do link só 4% são úteis para ela. Assim, ela está usando espaço em disco e servidores para armazenar esse tipo de informação indesejada", avalia Prado.

DISPOSITIVOS PESSOAIS

Cada vez mais comuns nos ambientes de trabalho, os dispositivos pessoais, como laptop, smartphone, CD-ROM e pen drive muitas vezes são usados para gravar um trabalho que será terminado em casa. "Mesmo bem intencionado, será que o usuário está seguindo o que a empresa preza em relação à segurança?", questiona Prado. Segundo o executivo, uma pesquisa realizada há quatro anos pela Websense aponta para o fato de que muitas pessoas levam trabalho para casa por e-mail pessoal, pen drive e site de armazenamento remoto.

"Isso é assustador. A pessoa tem boas intenções, pois quer terminar um trabalho no prazo, mas expõe as informações a um meio totalmente inseguro. Será que o computador que ela usa em casa tem todos os dispositivos de segurança? E nós falamos dos processos frágeis também. Se a empresa tem consciência de que aquela informação é de extrema confidencialidade, como permitiu que saísse de lá?", questiona.

O controle de segurança é importante para todas as empresas, mas é um assunto crítico na área hospitalar, por conta da exigência de sigilo sobre os dados médicos dos pacientes. "No exterior há regulamentações de mercado e o Brasil ainda está caminhando para isso. Muitas empresas estão preocupadas, mas talvez não enxerguem os problemas. Perder uma informação é uma coisa, mas expor o nome da empresa é um risco muito maior", conclui.



Marcos Prado, da Websense: 40% do link de internet é voltado ao uso de e-mails e o spam representa de 90% a 95% das mensagens



Hospital Vera Cruz: economia de banda de 30% e mais segurança para os 17 mil usuários mensais do site da instituição



Edison Fontes, especialista em segurança da informação: questões críticas dos hospitais exigem plano de contingência