

As tendências para melhorar a saúde através de informação e tecnologia

Luciana Cartocci (*)

Fazer um overview do que pude ver na HIMSS 2018, em Las Vegas, é praticamente impossível pela quantidade de novidades

Um verdadeiro showrooom de tecnologia e soluções para a saúde contemporânea, mais de 300 sessões de educação, 1300 expositores, centenas de programas especiais, atraindo mais de 45 mil profissionais da área da saúde. Tudo em busca de um ambiente de saúde mais prático, mais eficiente e de certa forma mais gentil para os pacientes.

O que envolve tudo isso é uma verdadeira imersão de soluções tecnológicas que se tornam um verdadeiro desafio para nós profissionais da tecnologia na área de saúde. Existe uma grande preocupação para que possamos estar sempre atualizados com essas tendências e principalmente sabermos avaliar a usabilidade no nosso país.

A realidade dos Estados Unidos e Europa ainda caminha em passos divergentes dos nossos. Muito do que vi são temas que já estão em evidência por aqui, porém ainda demandam de regulamentações e investimentos significativos.

Privacidade, segurança cibernética, integração de dados, interoperabilidade e troca de informações de saúde foram temas de várias palestras e que têm um alto grau de importância no contexto tecnológico atual.

Análise de dados e Business Intelligence, estão remodelando os conceitos tradicionais de gestão hospitalar, trazendo benefícios enormes com os indicadores gerados.

Saúde conectada e telemedicina, soluções já bem amadurecidas e recursos avançados para o tratamento de baixa complexidade. Dessa forma o hospital torna-se o local para o tratamento de doenças de maior complexidade. Inteligência Artificial, machine learnings, soluções precisas e sem intervenção humana. Utilizando essas soluções podemos através de informações já conhecidas como genética, hábitos e outras informações, trabalharmos com o preventivo descobrindo a probabilidade de desenvolvermos uma doença e até em que momento.

Mobilidade - A solução do Meridien da Aruba para atender hospitais e centros de saúde, oferece tags de

tamanho reduzido que fazem o rastreamento de posições e deslocamento de equipamentos importantes, profissionais e até pacientes dentro da instituição. Orientação interna e notificações automáticas com localização diretamente nos smartphones.

Imagem como fonte de informação - A Axis empresa sediada na Suécia, fabricante de câmeras, as quais até pouco tempo atrás serviam apenas como videomonitoramento, estão se tornando dispositivos de captura de dados e comunicação na rede, o que reforça a tão mencionada satisfação do paciente. Em um futuro bem próximo, os hospitais terão câmeras de videomonitoramento que captarão dados de forma contínua para aferir riscos, gerar alertas automáticos, agilizar processos sem intervenção humana, analisar grandes volumes de dados e cruzar informações, com inteligência. O responsável por todas essa inteligência nos sistemas de segurança são os vídeos analíticos.

Na HIMSS, a Axis apresentou um terminal móvel com uma câmera que pode se movimentar para qualquer lugar do hospital, resolvendo problemas comuns dos hospitais, pacientes em estado crítico ou que precisam de uma observação em tempo integral, fazendo registros sobre o estado de saúde do paciente, ou mesmo acompanhar algum procedimento de forma remota. É possível ter vários terminais desses no hospital ou em outras unidades e uma única central de observação.

Hoje, no Brasil, vários hospitais já aderiram à certificação da HIMSS e muitos outros estão em processo de certificação, isso mostra um setor já bem mais maduro nas boas práticas de TI e experiência do paciente, com foco na segurança.

Para nós, que trabalhamos como provedores de infraestrutura de TI, é importantíssimo conhecer todas essas tecnologias a fundo para que possamos ajudar os hospitais e instituições de saúde a definir os requisitos mínimos para a adoção das tecnologias de base, para que os projetos, principalmente os mais inovadores, sejam bem-sucedidos e possam estar preparados para as tecnologias que já estão aí, assim como as promissoras como IOMT e Blockchain.

(*) É diretora executiva da **TeleInfo Soluções**.

Como o nome da loja na fatura do cartão pode evitar prejuízos ao e-commerce?

Há uma tendência no mercado de e-commerce em acreditar que todo chargeback (quando o comerciante é obrigado a estornar o valor de uma venda ao consumidor) seja ocasionado por uma fraude de clonagem de cartão de crédito

Tom Canabarro (*)

Esta crença tem fundamento, mas é um pouco distorcida: há outras razões para que um consumidor conteste uma transação e solicite o dinheiro de volta, e uma delas pode ser o simples fato de como o nome de uma loja é lançado na fatura de cobrança. A boa notícia é que este problema é muito fácil de ser contornado.

É importante lembrar que, por contrato, todo portador de cartão tem o direito de solicitar junto ao banco emissor ou à operadora o cancelamento de alguma transação não-reconhecida e que foi aprovada sem a validação por senha (também chamada de transação de cartão não presente). Isso abre uma brecha muito grande para fraudadores, que obtêm dados de cartão de terceiros (número, data de validade e código CVV) e os utilizam para compras on-line. Quando o dono legítimo do plástico se dá conta do golpe e solicita o reembolso da compra, a loja virtual provavelmente já despachou o produto e arcará com aquele prejuízo do chargeback.

Segundo estudo recente da Konduto, tentativas deste tipo de golpe ocorrem a cada 5 segundos na internet brasileira e correspondem a 3% de todos os pedidos feitos no e-commerce nacional – cabe às ferramentas antifraude identificar as transações fraudulentas e barrar estes pedidos. Entretanto, alguns chargebacks podem ocorrer não necessariamente por má fé, mas por conta de uma simples falha de comunicação.

São poucos os clientes que conferem diariamente o extrato do cartão de crédito. A maioria deles se limita a conferir a lista uma vez por mês, correndo grosseiramente os olhos sobre os vários lançamentos dos últimos 30 dias. Provavelmente o consumidor não se lembrará de todas aquelas transações, mas boa parte delas não lhe levantará suspeita. Afinal, ele pode haver se "esquecido" de que gastou R\$ 50 no supermercado certa vez ou que pagou R\$ 8 em um café logo depois do almoço em um dia de trabalho. Só que e quanto a um lançamento de R\$ 200 em um estabelecimento chamado ABC Comm Mod Masc Lj Web, sobre o qual ele nunca ouviu falar?

Provavelmente este cliente não se lembrará do presente que ele mesmo comprou para um amigo em um e-commerce cujo nome



fantasia é Camisas ABC. Mas, receoso de ter sofrido um golpe, ele não hesitará em contestar aquele pedido junto ao banco.

Isso acontece por conta da forma como o nome da loja virtual foi lançado na fatura: aparece ali a razão social, que, além de estar abreviada, é menos conhecida e ligeiramente diferente do nome fantasia do empreendimento. Há outros casos ainda mais conflitantes para o cliente, quando o estabelecimento utiliza um intermediário de pagamento – e é o nome desta empresa que aparece na fatura, e não do e-commerce em si.

Neste caso, o portador do cartão entra em contato com o banco, solicita o estorno e o lojista sofre o chargeback. Não foi uma fraude "clássica", mas uma "fraude amiga", impossível de ser detectada por sistemas antifraudes porque não houve má fé do cliente, apenas um desacordo.

No entanto, há uma maneira relativamente simples de contornar esta situação. Adquirentes e subadquirentes oferecem um serviço chamado soft descriptor, que permite alterar e personalizar a maneira como o nome da loja virtual é lançada em um extrato de cartão de crédito. Esta atividade, inclusive, já é muito mais desenvolvida em outros mercados fora do Brasil: há empresas que colocam telefone do SAC ou até oferecem descontos em uma próxima compra.

Caso não seja possível a utilização de um soft descriptor, ainda há uma alternativa para tentar evitar uma "fraude amiga". Basta avisar o cliente como aquela compra será lançada na fatura. No caso das Camisas ABC, que usamos como exemplo anteriormente, poderia ser um aviso como: "Você verá no seu extrato uma cobrança em nome de ABC Comm Mod Masc Lj Web".

É crucial trabalhar para evitar contestações e prejuízos desnecessários, como por exemplo como o nome da sua loja é lançado em uma fatura de cartão. Afinal, seja uma fraude clássica ou uma fraude amiga, lidar com chargebacks é uma tarefa nada amigável.

(*) É co-fundador da Konduto, sistema antifraude inovador e inteligente para barrar fraudes na internet sem prejudicar a performance das lojas virtuais.

Quais são os limites para o compartilhamento de dados nas redes sociais

Há poucos dias o mundo soube por meio da imprensa sobre uma operação da Cambridge Analytica que, depois de realizar um teste de personalidade via Facebook, reuniu informações de mais de 270 mil usuários e seus contatos para criar uma base com detalhes sobre aproximadamente 50 milhões de pessoas e usa-la para campanhas eleitorais. Isso causou ao Facebook uma desvalorização de US\$49,6 bilhões na bolsa de valores em apenas dois dias.

Muitas pessoas se assustaram ao descobrir que reunir tais dados é algo comum às redes sociais e feito de acordo com o regulamento de uso. Ou seja, os usuários aceitaram que isso acontecesse quando - com ou sem conhecimento - concordaram com os termos e condições e, assim, forneceram acesso às suas informações. Além disso, muitas pessoas alegavam não ter conhecimento que esses dados poderiam ser transferidos para outras empresas para fins diversos.

Independentemente do destino dado pela empresa de pesquisa, o dado inicial, disponível nas contas do Facebook, é passível de utilização por terceiros, de acordo com cláusula de propriedade intelectual. Em relação ao conteúdo com direitos de propriedade intelectual, como fotos e vídeos, a rede social solicita em seus termos de adesão que o usuário conceda licença não exclusiva e transferível, com a possibilidade de ser inclusive outorgada a terceiros, isenta de direitos autorais e aplicável globalmente para usar qualquer conteúdo de propriedade intelectual que forem postados no Facebook ou em conexão com Facebook. A licença termina ao excluir o conteúdo ou a conta, a menos que o conteúdo tenha sido compartilhado com terceiros e eles não tenham sido removidos por estas pessoas.

No que diz respeito a manutenção de informações por parte



dos aplicativos, a rede social explica em seus termos que um aplicativo terceiro "pode pedir permissão para acessar seu conteúdo e informações, bem como o conteúdo e as informações que outras pessoas compartilharam com você". O que significa que, ao assinar o serviço do Facebook, o usuário concede a permissão para a utilização de seu nome, imagem de perfil, conteúdo e outras informações.

Tudo isso parece bastante assustador para um usuário comum e desavisado. No entanto, é importante saber que redes sociais como o Facebook e outras sempre deixam claro em seus termos que, quando o usuário seleciona um público específico para seu conteúdo ou informação, essa escolha será respeitada. Portanto, ao entrar nas configurações do aplicativo e adequar suas preferências de privacidade, isso protegerá a maior parte de suas informações pessoais.

Para evitar situações desconfortáveis, é fundamental e imprescindível primeiramente a informação. Os usuários precisam ter conhecimento dos termos e condições que estão aceitando ao usar qualquer aplicativo ou enviar informações pessoais em uma rede social. A ideia não é se tornar paranoico, mas simplesmente estar ciente do que acontece com a informação e agir em conformidade. Os usuários devem saber onde eles compartilham dados e quais permitem que sejam expostos.

A questão é ser inteligente na utilização das mídias sociais, optando por configurações de privacidade que protejam suas informações de terceiros e também estar sempre ciente de termos e condições de cada uma das contas que possui, para assim evitar surpresas desagradáveis.

(Fonte: Camilo Gutierrez, Chefe do Laboratório da ESET América Latina).

Aplicativo permite conversação em tempo real em diferentes idiomas

A falta de fluência ou conhecimento em um idioma muitas vezes pode atrapalhar uma nova parceria de trabalho ou adiar uma amizade com um estrangeiro. A solução para que isso não se torne um problema está no aplicativo Greengow, que traduz ligações e mensagens em tempo real. Com essa ferramenta, empresas e pessoas comuns podem ter contato no mundo inteiro sem perder grandes chances por não falar a língua local.

A plataforma permite, por exemplo, que uma pessoa na Irlanda se comunique com uma brasileira e outra francesa ao mesmo tempo.

Um diferencial do aplicativo Greengow é manter a entonação pelo áudio, considerando a emoção da conversa.

As empresas que abrem uma conta no aplicativo adquirem um número Greengow que pode ser repassado aos clientes de qualquer parte do mundo. Assim, um estrangeiro pode entrar em contato falando a língua local dele e a empresa receber a tradução em seu idioma. "Esta opção permite que estabelecimentos aumentem suas vendas e negociações sem nenhuma barreira com o idioma ou custos de ligações."

"A ideia é usar a tecnologia para eliminar barreiras de distância e idioma. Assim, você pode conhecer ou trabalhar com pessoas do mundo inteiro sem precisar viajar ou saber falar uma outra língua, facilitando a comunicação e aumentando parcerias ou vendas através do Greengow", conta Carlos Tanaka, diretor da Greengow.

O aplicativo que permite conversas em até 10 idiomas diferentes, é gratuito e está disponível para download no sistema Android através do Google Play ou IOS pelo sistema Apple Store.

News @TI

Inscrições abertas para o Simpósio Brasileiro de Redes de Computadores

Estão abertas as inscrições para participar do Simpósio Brasileiro de Redes de Computadores e Sistemas Distribuídos (SBRC) 2018. Coordenado pelo Instituto de Ciências Matemáticas e de Computação (ICMC) da USP, em São Carlos, e pelo departamento de computação da Universidade Federal de São Carlos (UFSCar), o 36º SBRC será realizado de 6 a 10 de maio em Campos do Jordão, no interior de São Paulo. Reconhecido como o mais importante evento científico nacional em redes de computadores e sistemas distribuídos, o SBRC é promovido anualmente pela Sociedade Brasileira de Computação (SBC) e pelo Laboratório Nacional de Redes de Computadores (LARC). Esta é a primeira vez que a iniciativa será realizada em Campos do Jordão e também marca a volta do evento ao estado de São Paulo após 21 anos. As inscrições devem ser feitas por meio do link icmc.usp.br/e/dcee4 até 2 de maio.

Redes obsoletas tornam concessionárias elétricas mais vulneráveis a ameaças

A maior parte das empresas elétricas mundiais está com suas estruturas pouco eficientes e vulneráveis a ataques do cibercrime e do ciberterrorismo, mesmo em países avançados, como é o caso dos EUA. A afirmação é do especialista israelense em segurança cibernética de infraestruturas críticas, Amir Barnea, um dos convidados a palestrar no Congresso Internacional do Utilities Telecom Council (UTCAL 2018), que acontece entre 03 e 06 de abril no Rio de Janeiro. Ele diz que o próximo passo para a modernização das concessionárias é realizar a conversão de suas estruturas inteligentes, hoje alicerçadas no paradigma IT (de Tecnologia da Informação), para o paradigma OT (de tecnologia de operação, que integra a monitoração de eventos, processos e dispositivos num console único de observação e intervenção). Segundo Barnea, que é líder em tecnologias de infraestrutura crítica da fabricante de redes seguras RAD, nada menos que dois terços (67%) das concessionárias elétricas norte-americanas identificam o combate às vulnerabilidades como o principal vetor de seus investimentos em tecnologia. "Para sair dessa situação, as operadoras necessitam acelerar a migração de suas estruturas analógicas (padrão TDM) para tecnologias digitais (Carrier Ethernet e MPLS), que são uma precondição para que elas adotem estratégias eficientes de segurança cibernética", afirma ele (<http://www.utcalamericalatina.org/summit2018/>).