Por que dispositivos "inteligentes" podem ser um perigo?

Vladimir Prestes (*)

Uma vez que o mundo foi convencido sobre as possibilidades da Internet das Coisas (IoT), tudo começou a "ficar inteligente"

Ao mesmo tempo, surgiu um problema: o controle dos objetos e dispositivos inteligentes, com os quais eles estão conectados, pode cair em mãos de pessoas mal-intencionadas, e quanto mais essas coisas penetram em nossa vida cotidiana e sabem demasiado sobre nós, mais séria a ameaça se torna. Geralmente, os fabricantes de dispositivos inteligentes lançam seus produtos, e só depois resolvem os problemas relacionados à segurança. Isto por que:

1. O fabricante implementa um sistema de proteção simplificado

A grande quantidade de dispositivos genéricos de origem desconhecida que suportam conexão com a rede tem um procedimento de autorização, mas logins e senhas já vêm pré-definidos de fábrica e, muitas vezes, os usuários não alteram as configurações após a compra do equipamento. Isso faz com que os dispositivos fiquem vulneráveis e é dessa fragilidade que os fraudadores se aproveitam.

2. O fabricante "esqueceu" de remover vulnerabilidades do dispositivo

Temos como exemplo casos quando a versão de lançamento de um produto deixou disponível uma das contas utilizadas no processo de desenvolvimento do programa. Isso aconteceu com o roteador D-Link DWR-932 B LTE, que entrou no mercado com duas contas administrativas disponíveis e algumas dezenas de vulnerabilidades de gravidade variável. E, mesmo assim, a D-Link não demonstrou intenção de repará-las.

3. O fabricante não reconhece as falhas como um problema

"Isso não é uma falha. É uma função adicional!" – assim respondem muitos dos fabricantes de coisas inteligentes às reclamações sobre as vulnerabilidades. E, aqui, podemos nos lembrar do caso com a empresa Xiaomi, em que o desenvolvedor pode instalar remotamente qualquer aplicativo em seus smartphones. Foi o que descobriu um estudante, que notou um estranho aplicativo - AnalyticsCore.apk - pré-instalado no smartphone Xiaomi MI4 e que funciona em modo 24/7. O interessante é que não há como se livrar do aplicativo, já que mesmo depois de totalmente desinstalado, o AnalyticsCore.apk aparece novamente no aparelho depois de um tempo.

4. Os dispositivos possuem funcionalidades das quais não se pode escapar

Alguns "dispositivos inteligentes" são equipados com funções que possuem componentes "spyware". A saída mais simples pode ser desligar a função, caso isso funcione. Foi assim com as TVs LG que enviavam o tráfego de informações independentemente de o usuário permitir sua coleta ou não. Ao ser questionado por um usuário sobre isso a LG simplesmente o aconselhou a conformar-se com a situação.

Em que patamar está atualmente a segurança da IoT?

Cada fabricante tenta fechar seu ecossistema, criando protocolos exclusivos e, portanto, incompatíveis com outros dispositivos. Gradualmente, a maioria deles deixará o mercado, enquanto outros surgirão buscando estabelecer-se como padrão universal – como aconteceram com os cassetes de áudio e vídeo, discos de vinil e sistemas operacionais móveis. Ainda há muitos protocolos (ZigBee, Insteon, Z-Wave, etc.), mas em breve o mercado determinará de dois a três modelos que acabarão sendo usados pelo mundo inteiro.

Hoje, existem muitos dispositivos e não são necessários conhecimentos específicos para que estes sejam hackeados. A partir disso, surgem ataques de softwares maliciosos e uma série de outras ameaças. No entanto, a ameaça não se limita aos botnets. Assim, a partir de pulseiras inteligentes, são "vazados" diferentes dados sobre a vida do usuário ou informações enviadas para redes sociais acabam sendo interceptadas. O caso recente das pulseiras inteligentes da empresa Strava é uma ameaça direta à paz e segurança internacionais - o serviço carregava as rotas do usuário em um mapa interativo e "revelou" a disposição de instalações secretas em todo o mundo.

E quanto aos smartphones? Desde que o serviço de internet banking se tornou popular, notícias sobre roubos de saldos de contas através do sistema Android em smartphones deixaram de nos surpreender.

Para o que devemos estar preparados?

Embora o problema seja evidente, apenas recentemente foram tomadas medidas concretas para a solução. Os documentos, sob os títulos "Princípios estratégicos para garantir a segurança da Internet das coisas", de novembro de 2016, e "Incentivo ao avanço da Internet das Coisas", de janeiro de 2017, com informações básicas e recomendações para o uso da IoT, foram divulgados pelos Ministérios da Segurança Nacional (Department of Homeland Security, DHS) e do Comércio (Department of Commerce) dos EUA, respectivamente. A aliança para a "segurança em nuvem" (Cloud Security Alliance, CSA) também contribuiu para o desenvolvimento do manual de segurança da IoT.

Contudo, apenas documentos não são o suficiente nestas situações. Paradoxalmente, a maior dificuldade em garantir a segurança da Internet das coisas é ocasionada pelos próprios usuários. Por exemplo, temos dois dispositivos inteligentes com funções semelhantes: o primeiro oferece alto nível de proteção, mas seu preço é muito mais elevado se comparado ao outro dispositivo desprotegido. Na maioria dos casos, o usuário não pode avaliar objetivamente a ameaça, por isso escolhe a opção mais barata. Outro aspecto deste problema é que os consumidores não são especialistas em proteção de dados e, por isso, não estão preparados para compreender os manuais com dezenas ou centenas de páginas. O usuário quer que tudo seja simples e rápido e o fabricante vai de encontro a esta expectativa lhe propondo executar tudo rapidamente.

Podemos avaliar esta questão a partir de diferentes pontos de vista. Por um lado, falando da vida privada, em que cada usuário adquire um dispositivo e é responsável pelo seu uso. Por outro, falando da vida em sociedade, onde o usuário pode levar seu dispositivo inteligente para o trabalho. Para evitar diferentes tipos de problemas com a IoT no local de serviço, é necessário treinar os funcionários implementando políticas e tecnologias de segurança e desenvolvendo habilidades para operar junto com a IoT.

Uma ligação óbvia entre o vazamento de dados e a IoT foi demonstrada por especialistas do centro de segurança da Universidade de Tecnologia e Design de Cingapura: eles conseguiram acessar dados pessoais usando um drone e um smartphone. O smartphone acoplado ao drone voou em torno de um prédio de escritórios, procurando por impressoras com a função Wi-Fi Direct e conectou-se à rede com o nome de uma das impressoras. Como resultado, todos os documentos enviados para impressão foram carregados para o smartphone. Apesar do método de invasão, os cientistas demonstraram que proteger uma impressora sem fio é um problema sério, uma vez que muitas informações confidenciais passam por ela. Para controlar as informações enviadas às impressoras, é melhor usar um sistema DLP, mas proteger o dispositivo contra invasões é tarefa dos fabricantes.

De acordo com a Gartner, o número de objetos conectados à Internet crescerá para 20,4 bilhões até 2020. Essa rede armazenará uma série de dados críticos, cujo vazamento poderá causar danos não apenas indivíduos ou organizações, mas também a economia do país como um todo. E, está claro que a velocidade do desenvolvimento das soluções para proteção de dados da IoT, ainda é significativamente inferior à velocidade da entrada de dispositivos inteligentes em nossas vidas.

(*) É Diretor Geral da SearchInform no Brasil, líder russa em sistemas de segurança da informação há mais de 20 anos. Com mais de dois mil clientes e cerca de 1.200.000 computadores protegidos, possui escritórios em 16 países.

Mudanças nas ferramentas de anúncios do Google

Atrair tráfego de qualidade, aumentar a taxa de conversão de campanhas digitais, reduzindo o custo por conversão, são alguns dos principais objetivos de quem trabalha com publicidade na internet

Denis Casita (*)

Mas, para fazer isso acontecer, é essencial conhecer as ferramentas voltadas para a divulgação de marcas, tirando, assim, um melhor proveito delas.

Neste momento, o segmento passa por mudanças, tanto para quem quer comprar, quanto para quem quer vender mídia. Isso porque, com o objetivo de otimizar as ferramentas para os anunciantes, o Google, recentemente, divulgou uma série de alterações nas suas plataformas.

Os produtos da corporação voltados para campanhas online, responsáveis por nada menos do que 86% de sua receita, sofreram uma reformulação, ganhando novos nomes e alguns recursos.

Para começar, o Google Adwords, plataforma básica do Google que possibilita a criação de anúncios para buscas pré-definidas, passa a se chamar Google ADS, ganhando uma interface mais descomplicada. Esse processo marca os 18 anos do lançamento do Adwords, que, até hoje, diga-se de passagem, tem sido a "galinha dos ovos de ouro" da gigante de tecnologia.

Já o DoubleClick e o Google Analytics 360 Suite, outras ferramentas de entrada para anunciantes, formam agora uma única marca, o Google Marketing Platform. Em um só lugar, o cliente poderá planejar, comprar, avaliar e otimizar mídias digitais.

As atualizações não param por aí: para aumentar o grau de eficiência das campanhas, fazendo com que elas apareçam para as pessoas certas, o Google vai utilizar, cada vez mais, o machine learning, que são regras criadas com base no reconhecimento de padrões sistematicamente analisados.

Uma das faces da nova experiência que o Google ADS passa a oferecer é a criação de campanhas smart, destinadas às pequenas empresas. Com ela, empreendedores de menor porte terão acesso a um recurso de machine learning, que possibilitará a eles um melhor resultado de seus investimentos.

Além disso, após adaptações no algoritmo do Google, o sistema seleciona combinações mais assertivas de palavras-chave, títulos e descrições, criando os chamados anúncios responsivos. Agora, em vez de criar várias versões do mesmo anúncio para testar o melhor, o cliente insere várias opções de título e descrições em um único anúncio e é como se o Google "batesse tudo no liquidificador", realizando essa otimização por ele mesmo. Ou seja, são geradas múltiplas combinações, sempre direcionadas ao perfil de quem fez a pesquisa.

Ainda seguindo a lógica do machine learning, a corporação anunciou também o Maxime Lift, ferramenta que atrai pessoas que, após assistirem aos vídeos de publicidade de determinadas marcas, ficaram propensas a considerá-las; a Local Campaigns, tipo de campanha desenvolvida para aumentar as visitas ao varejo físico - nesse tópico, a ideia é que o cliente forneça dados básicos da sua empresa para que a plataforma faça a otimização dos anúncios e indique, entre os produtos do Google, qual o melhor; e a Smart Shopping Campaigns, que otimiza o desempenho das campanhas com base nos objetivos de negócios dos clientes.

Nas Smart Shopping Campaigns, grande parte do processo é automatizado. Para isso, o Google ADS analisa itens como segmentação, público-alvo, localização geográfica, comportamento e tipo de dispositivo que a pessoa está utilizando. Assim, consegue determinar para quem e quando o anúncio será exibido.

O objetivo é ajudar as marcas a atraírem fluxo para seus sites e, consequentemente, para as lojas físicas. Essa funcionalidade contempla, inclusive, empresas que não possuem sites, criando páginas de destino para esses anunciantes, fazendo a otimização com base no texto do anúncio.

Para quem vê de fora, pode parecer que esse movimento é irrisório, mas ele vai além: reflete o processo de simplificação, praticidade, dinamismo e inteligência que a empresa quer transparecer aos seus clientes e ao mercado de forma geral.

As mudanças, apesar de não serem drásticas e, a princípio, não alterarem os valores praticados pela corporação, trazem uma grande vantagem competitiva para os profissionais de marketing e para os anunciantes, que mais do que nunca poderão se conectar com o seu público-alvo com mais facilidade e precisão e, melhor, entregando uma performance de qualidade. Em suma: é um panorama com um impacto ainda intangível para o mercado, mas, acima de tudo, muito promissor.

(*) É especialista em Marketing Digital e CEO da Performa Web. Graduado em Administração para Internet pela FIAP, possui especializações na área de Marketing Online, Análise e Planejamento Financeiro, Técnicas de Feedback e Liderança pela FIA, além de ser Especialista em Search Marketing.

Transporte urbano na era digital: novos serviços a usuários que demandam modernidade

O cidadão digital exige, cada vez mais, que as empresas aprimorem seus serviços, o que inclui o transporte urbano. Neste quesito, o conceito de mobilidade urbana deve ser adaptado à economia digital, trazendo às cidades modernas uma infraestrutura alinhada às demandas e necessidades de seus habitantes.

Para tornar realidade essa mudança, é preciso reduzir os tempos de viagem, minimizar os custos e integrar diferentes meios de transporte e de pagamento. Isso somente é possível com a adoção de sistemas integrados de pagamento, assim como soluções eficientes de gerenciamento de frota e plataformas de informações ao usuário de última geração.

E quando falamos em sistema integrado de pagamento, a proposta é utilizar uma cobertura ampla de rede comercial de carga ou seja, pontos de vendas e máquinas de autoatendimento.

Além disso, é fundamental expandir o sistema para que ele possa ser pago com cartões nas modalidades crédito ou débito e também com novas tecnologias utilizando dispositivos inteligentes (smartphones, wearables) e aplicativos de pagamentos, que não exigem uma rede de recarga física e específica, o que facilita a vida do usuário, oferecendo conveniência e maior cobertura à rede de transporte.

Para suportar estes meios de pagamento, são necessários um sistema de processamento robusto e uma plataforma tecnológica e de segurança da informação sólida, que transmitam ao sistema central todas as informações sobre a viagem e a tarifa paga, de acordo com o registro das transações realizadas.

Além disso, o provedor de tecnologia deve ser capaz de realizar a compensação de transações, que consiste nas validações de todas as passagens pagantes e as que possuem benefícios parciais ou totais, assim como a distribuição da cobrança para os múltiplos operadores, de acordo com os contratos estabelecidos.

Todos esses sistemas, por sua vez, precisam de uma plataforma tecnológica sólida, que demande uma série de elementos que incluam infraestrutura ad-hoc e software especializado: validadores, zonas pagas, totens e terminais de recarga e autosserviço, cartões, ferramentas de software, servidores, bases de dados, data warehouses, antenas, sensores, equipamentos de inspeção, entre outros. Tudo isso, por sua vez, precisa contar com serviços de suporte e manutenção especializados.

Em paralelo, deve haver progressos na concepção e implementação de soluções inovadoras para controlar a evasão, tais como o mapeamento de "zonas de pagamento" eficiente e autossustentável.

Os provedores de tecnologia que têm trabalhado intensamente nesta evolução estão constantemente testando soluções que estão alinhadas com os novos requisitos dos usuários e às novas ferramentas digitais que estão surgindo. O foco é aplicar diferentes elementos que traduzem em um melhor serviço para o usuário, que deve ser o centro de qualquer sistema de transporte moderno.

(Fonte: Anderson Benino é business development manager de Transportes da SONDA, maior companhia latino-americana de soluções e serviços de Tecnologia, que mantém um centro de competência no Chile para a aplicação de projetos digitais de mobilidade urbana).

News @TI

Núcleo de inovação com foco em IoT

@Assim como no consagrado Vale do Silício, nos Estados Unidos, cada vez mais as empresas brasileiras se aproximam de startups para o desenvolvimento de soluções inovadoras. Com estas parcerias, companhias já consolidadas têm sua capacidade de inovação ampliada a um custo menor e com maior agilidade. Já as startups, ganham em acesso ao mercado e na validação dos seus produtos e serviços. A Alert System, empresa especializada em sistemas inteligentes e soluções de segurança, anunciou a abertura do seu primeiro núcleo de inovação em Belo Horizonte, com o objetivo de se unir às startups locais, principalmente, aquelas que atuam com Big Data e Internet das Coisas (IoT).

e-commerce de dados históricos

@A B3 lança hoje sua loja online para comercialização de séries históricas de dados do mercado de capitais. O UP2DATA ON DEMAND oferece dados retroativos de preço de fechamento, referência, ajuste, cadastro de instrumentos, índices, dados intraday e de posições em aberto dos ativos da B3, entre eles commodities, juros, moedas e renda variável. Os dados serão utilizados principalmente por acadêmicos, investidores e instituições financeiras, para compor estudos e análises que embasarão importantes tomadas de decisão.

Managed Service Provider pela AWS

@A Claranet Brasil, multinacional de serviços gerenciados em cloud service, passa pelo processo de auditoria da AWS e renova, pelo terceiro ano consecutivo, sua qualificação de Managed Service Provider. O título é concedido aos parceiros que cumprem com as exigências e estão habilitados a gerenciar ambientes na nuvem, de acordo com as melhores práticas do cloud provider (http://br.claranet.com/).