Como vencer ataques digitais baseados em Internet das Coisas (IoT)

Rita D'Andrea (*)

Antes apenas um conceito, a Internet das Coisas tornou-se, agora, tangível. Isso acontece porque, no final de outubro, milhares de dispositivos IoT foram usados de forma massiva durante ataques DDoS (de negação de serviço) que praticamente derrubaram a Internet nos EUA

A empresa mais atingida pelo uso de sensores IoT "zumbis" por hackers foi a Dyn. Como a Dyn é o provedor de DNS para muitos grandes portais, o ataque DDoS baseado em IoT acabou derrubando gigantes como Twitter, Netflix, Spotify, Airbnb, Reddit, Etsy, SoundCloud e até mesmo o The New York Times.

A Botnet de onde surgiram os ataques automatizados a esses portais usou como base pequenos roteadores domésticos, decodificadores de TVs a cabo e câmeras de vídeo. São dispositivos IoT com alta capacidade de CPU – capazes, portanto, de abrigar malware sofisticado – e uplinks de alta largura de banda, o que permitiu que esses dispositivos fossem usados para lançar ataques de até 100 Mb/s cada.

Os hackers responsáveis pelos mega ataques de outubro usaram o software Mirai, que usa malware de e-mails de phishing para infectar inicialmente um único computador ou uma única rede doméstica. A partir daí, o malware é distribuído automaticamente para todo tipo de dispositivo IoT, que se transforma em submisso elemento de uma Botnet.

Vale destacar que, ao final do dia, o poder de fogo coletivo de milhares de dispositivos IoT inseridos numa Botnet é até dez vezes maior do que o das Botnets baseadas em computadores tradicionais. A força destruidora pode ficar acima de terabits por segundo.

O que aconteceu em outubro mudou o modo como se pensa a segurança de TIC, obrigando o mercado a analisar as estratégias para, simultaneamente, tornar o dispositivo IoT e a rede corporativa mais seguras.

Como tornar o dispositivo IoT mais seguro

As sugestões aqui listadas são para pessoas e empresas que compram ou simplesmente utilizam dispositivos IoT em seus ambientes, seja um carro, o quarto de um bebê ou o chão de fábrica de uma indústria.

- Assegurar-se de que todas as senhas padrão sejam trocadas por senhas fortes. Isso é importante porque nomes de usuário e senhas para a maioria dos dispositivos IoT podem ser facilmente encontrados na Internet. Isso torna os dispositivos com senhas padrão extremamente vulneráveis.
- Atualizar dispositivos IoT com patches de segurança logo que estes se tornam disponíveis. Um IoT com configuração desatualizada é um alvo fácil para hackers.
- Desabilitar o Universal Plug and Play (UPnP) em roteadores.
- Adquirir dispositivos IoT de empresas que tenham reputação de fornecer tecnologia segura. Como preço é um fator-chave em tudo o que diz respeito aos sensores IoT, essa orientação pode encontrar resistência em alguns consumidores/usuários.

Como tornar a rede corporativa mais segura

Devido à complexidade dos ambientes corporativos, são muitas as frentes de batalha contra os ataques DDoS baseados em Botnets de dispositivos IoT "zumbis".

Contrate "limpadores de nuvem" – Ataques semelhantes ao realizado em outubro só podem ser mitigados por cloud scrubbers (limpadores de nuvem) especializados em defesa em escala. É a nuvem protegendo a nuvem. Os serviços de segurança cloud scrubbers interceptam o tráfego de ataque, limpam esse fluxo de dados e devolvem para a corporação usuária deste serviço de segurança somente o tráfego "bom".

As organizações devem certificar-se de que têm contratos com um ou mais cloud scrubbers antes de ser atacadas. Configurar os túneis pré-estabelecidos não é algo que possa ser feito facilmente em meio a um ataque volumétrico.

Construa um plano resiliente de DNS - O ataque sofrido pela Dyn tornou urgente renovar a forma de se trabalhar com DNS, enfatizando a importância das empresas usuárias manterem um "plano B". O objetivo é saber o que fazer se o seu provedor de DNS ficar offline em decorrência de um desses novos tipos de ataques. Para evitar essa situação, é essencial que as empresas construam um plano resiliente, que inclua múltiplos provedores de DNS para servir endereços para as aplicações críticas de cada corporação usuária de TIC.

Uma alternativa interessante é alocar o DNS em uma nuvem segura. Neste caso, transfere-se o DNS para um serviço de scrubbing center ou "limpador de nuvem". Grandes provedores de serviços no Brasil já estão tomando esta precaução, uma atitude que pode evitar situações como as vivenciadas pelos clientes da Dyn.

Aposte no firewall da rede – A camada de defesa da rede é construída em torno do firewall da rede. Ela é projetada para mitigar alguns dos mais terríveis ataques computacionais. Mas atenção: muitos firewalls só resistirão a ataques DDoS se forem adequadamente configurados. Verifique as configurações com o seu fornecedor de firewall de rede. Alguns clientes instalam dispositivos anti-DDoS antes do firewall para repelir ataques.

Defenda suas aplicações – Vimos que a Botnet Mirai tem capacidade para gerar impressionantes inundações de solicitações de acesso. Devido a essas solicitações parecerem aos dispositivos de defesa da rede um tráfego normal, essas ameaças acabam sendo enfrentadas na camada de aplicação (4 a 7). Diante disso, alguns especialistas recomendam o que se chama "login-wall". Um login wall exige que uma conexão seja autenticada antes de começar a acessar a aplicação. Essa checagem é feita antes do sistema, para atender a essa solicitação, passar a consumir recursos computacionais da corporação.

Hacker vivem em bando, experts em segurança farão o mesmo

Ficou claro, portanto, que estamos em uma nova fase de ataques DDoS – a era da Internet das Coisas usada em Botnets. Nesta nova era, os criminosos trocam informações entre si o tempo todo. Nos ataques de outubro, por exemplo, hackers de todo o mundo compartilharam entre si o Mirai. A comunidade de Segurança da Informação precisa copiar essa estratégia e aprender a trabalhar unida para resolver as ameaças que surgem com a disseminação do IoT.

Nos próximos anos, os ataques DDoS crescerão em tamanho, os serviços de limpeza da nuvem ampliarão a largura de banda para acomodar esses grandes ataques, e os fabricantes de dispositivos IoT descobrirão como lidar com as inseguranças dos seus dispositivos.

Essa evolução é certa.

Ainda assim, governos, empresas e pessoas terão de constantemente reaprender como lidar com a ameaça crescente das Botnets baseadas em dispositivos IoT. A batalha pela segurança é uma história sem fim, e o uso da Internet das Coisas pelos hackers está apenas começando.

(*) É country manager da F5 Networks Brasil

Tecnologia pode gerar economia de R$ 10,00 por fatura em uma operadora de telecom

Você sabia que um "tradutor" de notas fiscais eletrônicas pode representar uma economia de R$ 10,00 por fatura em uma operadora de telecomunicações?

Marcelo Brancato (*)

Se há uma área onde o mercado brasileiro pode evoluir é a do envio das faturas eletrônicas no segmento B2B (business to business), principalmente nas telecomunicações. Os custos inerentes à situação atual (envio da fatura impressa) são altos e trazem diversas desvantagens. Além do custo associado à impressão e postagem, há ainda que contar com o tempo e garantia de entrega da mesma, com um problema adicional: hoje em dia há uma grande porcentagem de faturas não entregues e, consequentemente, não pagas. O que causa um grande prejuízo para a operadora de telecomunicações.

A solução passa pela adoção de uma espécie de intermediário entre a operadora e os clientes B2B. A operadora emite (eletronicamente) a fatura que é integrada no portal e disponibilizada para os clientes. Desta forma não há custo de impressão e postagem e a operadora tem a certeza de que a fatura foi entregue, pois tudo fica registrado eletronicamente. O cliente recebendo a fatura mais cedo consegue planejar e efetuar o pagamento a tempo, trazendo a receita no prazo previsto.

Feitas as contas, há todo um conjunto de vantagens na adoção desse tipo de solução. Só na impressão, os valores custam cerca de R$ 0,05 por cada folha. A esse valor há ainda que acrescentar a postagem, o não recebimento, o reenvio, o que faz com que, facilmente, o custo de uma fatura atinja valores entre R$ 7,00 e R$ 10,00. Multiplique isso por todos os clientes de uma operadora de telecomunicações e facilmente se percebe o nível de economia a cada ciclo de faturamento.

Ainda mais porque a solução (a do portal que serve de intermediário entre as duas empresas – operadora e cliente) não exige qualquer tipo de investimento em desenvolvimento de software. O portal trabalha com o arquivo gerado pelo sistema de faturamento da operadora. O único custo associado é o de licenciamento. Do lado dos destinatários das faturas o portal pode igualmente integrar automaticamente com os seus sistemas de gestão, facilitando o processo operacional e administrativo da organização, independentemente do formato selecionado (o portal já conta com alguns formatos padrões, como por exemplo CNAB, XLS entre outros). Caso o destinatário não queira efetuar a integração automática, ele pode consultar todas as informações diretamente no portal, com o mesmo layout da fatura em papel.

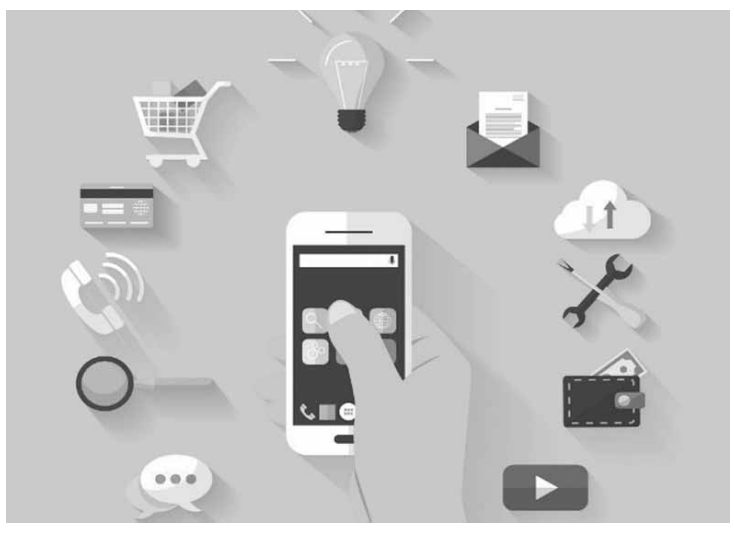
Em uma fase seguinte, e pensando de forma mais abrangente, a operadora de telecomunicações pode integrar esta ferramenta com outros sistemas e definir qual o melhor portfólio de clientes, aumentando o valor por cliente e minimizando a inadimplência.

E convém não esquecer a imagem junto do público. Hoje cada vez mais as pessoas estão atentas e dão preferência às organizações que adotam uma estratégia amiga do ambiente, as "empresas verdes", com responsabilidade socioambiental.

(*) É Country Manager da Saphety Brasil.

Em busca do app de ouro para os clientes "on the move"

Segundo dados da Aspect, 90% dos consumidores afirmam que estar disponível e atender às expectativas faz com que os aplicativos móveis sejam a primeira opção enquanto canal de atendimento. A quantidade de aplicativos para atendimento ao cliente é imensa. De acordo com a Gartner, em 2017, 35% de todas as interações de atendimento ao cliente será realizada por meio de dispositivos móveis.



Para ser perfeito, o aplicativo móvel deve permitir ao consumidor escolher e colaborar. Optar por usar o autoatendimento ou entrar em contato com um agente, a qualquer momento e, ao mesmo tempo, colaborando com ferramentas multimídias: chat em tempo real com o agente; envio de vídeos, links, SMS; e chamadas de voz. Tudo isso por meio do app.

Entretanto, muitas empresas têm ficado presas a uma experiência móvel fragmentada, pois a maioria dos aplicativos móveis não está integrada à infraestrutura de suporte ao cliente, as informações sobre o usuário são perdidas ao passar de um canal para outro e a experiência se torna um fracasso. Um em cada 3 clientes são perdidos devido a uma experiência ruim.

Escolher uma solução móvel de atendimento ao cliente é um pilar fundamental para as empresas. Há no mercado muitas opções disponíveis, mas como saber qual é a mais adequada? Confira quais devem ser as 9 principais funcionalidades:

- **Multicanal:** é a chave para a continuidade entre o autoatendimento e o serviço prestado pelos agentes aplicado a todos os canais disponíveis: aplicativos, SMS, chat e redes sociais.
- **Contexto e continuidade** deve garantir que o usuário possa mudar de um canal para outro, sem obstáculos e sem que as informações do atendimento sejam perdidas.
- **Integração:** todos os canais móveis devem estar integrados à infraestrutura de atendimento existente
- **Arquitetura em nuvem:** avaliar as opções oferecidas de software baseado em nuvem
- **Adaptabilidade das aplicações:** a plataforma deve construir, implementar e gerenciar aplicativos por meio de voz, texto, web móvel e redes sociais que se adaptem às mudanças nas exigências do negócio e experiência do cliente.
- **Funcionalidades de negócio:** é importe que o app permita, por exemplo, renovações ou envio de notificações de pagamentos para que o cliente aja instantaneamente; avaliação de soluções que permitam o envio de e-mail ou SMS com opções de resposta instantânea e acesso aos dados de forma segura.
- **Aplicações com IVR:** permite passar a chamada telefônica podendo escolher diretamente a opção de telefone que resolva as dúvidas.
- **Equilíbrio entre autoatendimento e contact center:** dá a liberdade de escolha, sem perder a prioridade na fila de chamadas. Se você optar por resolver os problemas por meio do app, por exemplo, a chamada é cancelada, mas se você não encontrar a solução, pode ligar para um agente de atendimento.
- **Nível de interação entre usuário e operador:** a solução deve permitir uma experiência de 360 graus. O cliente deve ser capaz de comunicar-se com um operador sem sair do aplicativo e também usado simultaneamente bate-papo, áudio, vídeo ou navegação colaborativa.

Encontrar o app de ouro para os consumidores exige uma solução de mobilidade cuja chave é saber fazer as perguntas certas para inovar, sem esquecer que o objetivo é entregar o que é realmente relevante para os consumidores.

(Fonte: Asier Bollar é Director de Marketing da Aspect para América Latina).

News @

2º melhor fornecedor de Sistema de Gestão Tributária pelo Prêmio CONFEB 2016

@Com o objetivo de valorizar e dar visibilidade aos profissionais e fornecedores das áreas tributária e fiscal, o CONFEB – Conselho Fiscal Empresarial Brasileiro, criou o Prêmio CONFEB, que realizou sua primeira edição em 2016. Inédita, a premiação teve como foco eleger os principais profissionais, fornecedores e projetos por meio de votações e avaliações de especialistas do setor tributário. Na categoria "Fornecedores do Ano" a TaxWeb, empresa de compliance fiscal, ficou em segundo lugar entre os melhores Sistemas de Gestão Tributária, com 13% dos votos, ficando atrás da Thomson Reuters. Nessa categoria, foram consultados cerca de 600 executivos entre Diretores, Heads e VPs da área tributária e fiscal de 200 grandes empresas do mercados brasileiro (www.taxweb.com.br).