2016, o ano do software

Otto Berkes (*)

A tecnologia da informação no formato em que conhecemos hoje está morta. O que antes era apenas uma missão para "manter as luzes acesas" evoluiu para a necessidade de engajar e fidelizar clientes. E, cada vez mais, para que uma empresa se beneficie da nova tecnologia da informação, precisa investir em software.

Com o software agora posicionado no centro do negócio, organizações estão se transformando digitalmente no sentido de adotar práticas ágeis e novas tecnologias que entreguem inovações ao mercado de maneira rápida e segura. Desta forma, conseguem fazer com que seus clientes estejam sempre por perto, desejando novos produtos e soluções.

Mas quais são os principais desafios para que estas organizações comecem esse processo de transformação digital em 2016?

1. Para desenvolvimento flexível e em escala, invista em containers

O ano de 2016 verá pelo menos um sonho de décadas tornar-se realidade – a criação de um fluxo de desenvolvimento baseado em componentes, ligado a práticas ágeis e contínuas de desenvolvimento, permitindo que organizações se transformem num ritmo mais acelerado do que nunca.

O foco será nos serviços menores, que poderão ser implantados independentemente, entregando novos recursos de maneira contínua. Os dias de espera para a revisão de aplicativos inteiros estão acabados.

Microsserviços e containers (tecnologia que permite executar processos e testes de maneira isolada, com segurança e estabilidade) proporcionarão maior poder de flexibilidade e escala no processo de desenvolvimento. As duas tecnologias transformarão a maneira com que desenvolvedores constroem, implantam e atualizam aplicativos e acelerarão a necessidade de que práticas ágeis fiquem à frente das mudanças no mercado e das exigências dos clientes.

2. "Segurança ágil" entra em campo

Segurança não pode mais ser uma reflexão tardia. Tem que ser preparada sob todos os aspectos do design de aplicativos, desenvolvimento e implantação.

A aceleração dos ciclos de desenvolvimento de softwares faz com que a segurança tenha que estar na base de qualquer projeto ou processo de desenvolvimento.

Para 2016, todos os caminhos levam à ideia emergente de "segurança ágil". Trazer segurança mais cedo ao processo, junto à metodologia DevOps e a práticas ágeis, adiciona o imprescindível terceiro pilar ao desenvolvimento de software em escala e alta velocidade.

3. Analytics por todas as partes ditarão o valor do cliente

Com o passar dos anos, os analytics evoluíram de inteligência de negócios para transacional e big data. A partir de agora, análises em tempo real que elevam a experiência do cliente na medida em que ligam previsões a ações prescritivas se tornarão praxe.

Em 2016 nós entraremos em uma era na qual o fator demográfico permitirá às organizações personalizar serviços, definir preços, vendas e produtos em tempo real para o indivíduo. Com os analytics, levaremos melhores experiências ao cliente, na medida em que colocamos a segurança que protege os consumidores como pano de fundo. Novas técnicas de análises usarão padrões de comportamento e o aprendizado das máquinas para separar clientes reais de fraudadores e proporcionarão transações e experiências com menos costuras.

4. Internet das coisas: do reino das possibilidades interessantes ao mundo da aplicação real

Ainda que a internet das coisas, um elemento da transformação digital, seja uma tecnologia de alto potencial, podemos dizer que ela ainda engatinha. Analytics e segurança seguram a chave para abrir a porta que agregará mais valor aos consumidores.

As particularidades inerentes ao mundo da internet das coisas criam mais vulnerabilidades e pontos de ataque do que nunca e aumentam as chances de conflito. Conceitualmente, a internet das coisas é aquela elegante nova onda que todos querem surfar, mas abaixo da superfície há um terreno cheio de complexidades que precisam ser acessadas e entendidas.

Na medida em que a internet das coisas chega ao mainstream, a "identidade das coisas" passará a ser fundamental. Da mesma maneira que a identidade de uma pessoa precisa ser autenticada, a "identidade" de um dispositivo e qualquer fluxo de dados que chegue a ele também precisam ser confirmados e definidos como confiáveis.

Ferramentas como identidade e gerenciamento de acesso (IAM) para internet das coisas e tabelas de interação são necessárias para assegurar que estamos engajados com as "coisas certas" e elas não estão conflitando, anulando ou duplicando a si mesmas no ambiente.

Enquanto sensores de internet das coisas e dispositivos inteligentes proliferam e interagem conosco em áreas críticas, como Saúde e indústrias automotivas, eles ajudarão a simplificar – e talvez salvar – nossas vidas e melhorar as experiências dos clientes.

5. Blockchain encontra o seu fundamento

A surpresa de 2016 será o ressurgimento da tecnologia blockchain e o seu refinamento ao ponto de que realmente encontrará seu lugar fora do livro de contabilidade do Bitcoin.

Blockchain era uma palavra-chave para muitas startups há dois anos e está pronta para renovação, quando olhamos para o crescimento da internet das coisas e necessidade de envolvimento seguro entre dispositivos.

Uma tecnologia como a blockchain, que depende de uma rede de computadores e tem a privacidade como elemento central, será um importante facilitador da internet das coisas e da transformação digital de qualquer organização, uma vez que simplifica ainda mais as operações para se ter mais agilidade e receptividade do cliente.

A tecnologia blockchain terá que superar sua "culpa por associação" aos problemas relacionados ao Bitcoin, mas há claramente a capacidade para se tornar a "bola da vez" para sensores e internet das coisas em geral.

(*) É Chief Technology Officer da CA Technologies

Os cinco estágios do luto (do monitoramento)

Se você já trabalhou com TI por mais de dez minutos, sabe que as coisas saem errado. Na verdade, deveria ser óbvio que temos empregos em TI justamente porque as coisas saem errado

Leon Adato (*)

É disso que o monitoramento e a automação de TI tratam: criar sistemas que se cuidem automaticamente, avisem quando as coisas começam a dar errado e forneçam as informações necessárias sobre o que aconteceu e quando, de modo que você possa evitar o mesmo problema no futuro.

Após mais de uma década implementando sistemas de monitoramento em empresas de grande e pequeno portes, me familiarizei com o que se poderia chamar de "luto do monitoramento", algo que ocorre com frequência quando você é incumbido de monitorar alguma coisa para outra pessoa – o que é quase inevitável – e essa pessoa lhe pede para fazer coisas que você sabe que causarão problemas. Ele envolve uma série de comportamentos que agrupei em cinco estágios. São como os cinco estágios do luto, só que no monitoramento.

Embora as empresas passem com frequência por esses estágios ao implantarem o monitoramento pela primeira vez, eles também podem ocorrer quando um grupo ou departamento começa a implementar seriamente uma solução existente, quando novos recursos são adicionados a um conjunto de monitoramento atual ou simplesmente em um dia qualquer.

E aqui vou entregar o final da história: se você está familiarizado com o modelo Kubler-Ross padrão, sabe que a aceitação não consta nesta lista.

Primeiro estágio: monitorar tudo

Trata-se da falta de decisão inicial quanto ao monitoramento, uma resposta à pergunta simples e inocente: "O que preciso monitorar?". A opção favorita de gerentes e equipes que não irão de fato lidar com o tíquete é simplesmente ligar a mangueira de incêndio com força máxima e pedir que você monitore "tudo". Essa escolha também é feita com frequência por administradores que estão bem no meio de uma catástrofe. Essa decisão parte do pressuposto de que toda a informação é útil e pode ser "ajeitada" posteriormente.

Segundo estágio: momento Prozac

Ainda nos moldes do primeiro estágio, o destinatário de 734 e-mails de alerta de monitoramento recebidos em um intervalo de cinco minutos vem até você e diz: "Tudo isso não pode estar dando errado ao mesmo tempo!" Embora pareça correta a princípio, essa afirmação ignora o fato de que um computador define "dar errado" com o mesmo grau de especificidade dos humanos que solicitaram os monitores. Dessa forma, você reduz as coisas a proporções razoáveis, mas, ainda assim "coisas demais" estão indicadas em vermelho e a reação continua a mesma.

O pior é que, como o "monitoramento era ruim" antes – o que, logicamente, foi decorrência de uma solicitação estúpida – ele deve estar errado novamente. Só que desta vez não está. Ele está captando alterações em todos os níveis há semanas, meses ou anos, e ninguém reparou. Ou as falhas se corrigiram sozinhas muito rapidamente, ou os usuários nunca reclamaram, ou alguém em algum lugar se antecipou e consertou tudo.

Essa é a hora em que você gostaria de poder dar um Prozac para o responsável pelo sistema para ele relaxar e se dar conta de que saber sobre as interrupções é a primeira etapa para evitá-las no futuro.

Terceiro estágio: pintando as rosas de verde

O próximo estágio ocorre quando uma enorme quantidade de coisas permanecem "inativas" e, não importa o quanto você tente, nada as faz mudar para "ativas" porque, afinal de contas, elas estão mesmo inativas.

Em um impulso de orgulho e teimosia, o responsável pelo sistema com frequência ainda admite algo do tipo: "Eles não estão totalmente inativos, estão só 'meio inativos'." E mandam você fazer o que for preciso para que os sistemas se mostrem ativos/bons/verdes.

E com isso quero dizer qualquer coisa mesmo, inclusive alterar os limites dos alertas para níveis impossíveis ("Alertar somente quando estiver inativo por 30 horas. Não, coloque uma semana."), desativar alertas por completo – em uma ocasião, sob ameaça de perder o emprego – criar uma página completamente falsa com GIF's vermelhos pintados de verde para mostrar para a gerência sênior.

O que torna este estágio ainda mais constrangedor para todos os envolvidos é que o trabalho decorrente costuma ser maior do que a tarefa derealmente corrigir o problema.

Quarto estágio: uma verdade inconveniente

E por aí segue a rede de intrigas, que pode durar semanas ou meses, até o ponto em que ocorre um erro crítico que não pode ser disfarçado (nem no Photoshop). A essa altura, você e o responsável pelo sistema estão no telefone com a equipe de restauração do serviço, mais uma dúzia de engenheiros e alguns altos executivos de TI, a fim de analisar, verificar e reiniciar tudo em tempo real.

Nesse momento, alguém pede para ver os dados de desempenho do sistema – aquele que está inativo há um mês e meio, mas que apareceu como "ativo" nos relatórios. Para um responsável por sistema que desenvolveu o hábito de comprar tinta verde por atacado, não dá mais para fugir ou se esconder.

Quinto estágio: burlando as regras

Supondo que o responsável pelo sistema permanceceu com seu cargo intacto até o quarto estágio, o quinto envolverá manter você à distância. As pessoas menos sofisticadas encontrarão maneiras de fazer o monitoramento sem de fato ter a inconveniência de realmente ter que monitorar, enquanto as pessoas que já estão na empresa há algum tempo solicitarão informações detalhadas sobre exatamente quais permissões você precisa para monitorar. Essas informações são encaminhadas para uma equipe de auditoria de segurança inevitavelmente nova que nega a solicitação categoricamente porque as permissões envolvem risco demais para serem concedidas.

A esta altura, você tem uma escolha: apresentar toda a documentação e insistir que recebeu as permissões que já tinham sido combinadas ou sair em busca de outro grupo que de fato queira o monitoramento.

E quanto ao responsável pelo sistema que começou dizendo "monitore tudo"? Não se preocupe. Ele estará de volta depois da próxima interrupção do sistema.

Com mais motivos para luto.

(*) É gerente técnico da SolarWinds.

Brinquedos, sites de relacionamento e dados médicos foram alvos de ataques cibernéticos em 2015

2015 foi um ano de novos aprendizados e aumento da consciência dos consumidores sobre a segurança cibernética. Houve casos graves de violações e contas comprometidas, mas também vemos que a segurança está mais presente em todos os setores, e estamos mais preparados para o que o ano novo nos reserva. Relembre alguns dos destaques do ano sobre segurança cibernética.

Brinquedos e serviços infantis são alvos de cibercriminosos:

A VTech, fornecedora de brinquedos infantis educativos conectados à Internet não teve um bom ano. Cerca de cinco milhões de pais e seis milhões de crianças tiveram suas credenciais de conta - com informações de identificação pessoal, fotos e registros de bate-papo - comprometidas. Simplificando: esta foi uma das maiores violações de segurança do ano.

Empresa japonesa Sanrio, dona da marca Hello Kitty, sofreu um vazamento do banco de dados do seu site de fãs no final de dezembro, de acordo com a WIRED. Os arquivos continham nomes completos, datas de nascimento, endereços de e-mail e muito mais. Alguns dados, como senhas e respostas a perguntas de segurança, foram criptografados. Dados localizados em outro lugar no sistema da Sanrio não contavam com controles de segurança rigorosos, fazendo muitas dessas credenciais potencialmente decifráveis. O número de vítimas soma 3,3 milhões de pessoas, muitas menores de 18 anos.

Consumidores chantageados:

Clientes da Ashley Madison - um serviço online que reúne adultos com intenção de casos extraconjugais - tiveram seus e-mails, dados de cartão de crédito e outras informações roubadas do site da empresa no final de junho. O vazamento afetou 37 milhões de pessoas, e também apresentou uma tendência crescente no cibercrime: hackers chantageando os consumidores ou empresas com fins lucrativos.

No caso da Ashley Madison foi uma das primeiras vezes que vimos os cibercriminosos chantageando tanto a empresa como seus clientes diretamente. O incidente foi um bom lembrete de que o que se passa na Internet permanece on-line, e exemplificou como ataques como este podem ter consequências de longo alcance.

Registros médicos comprometidos:

Em 2015 também vimos muitos casos de registros médicos pessoais vazarem na internet, como o caso do the Premera Blue Cross, em março. O motivo não é nenhum mistério: registros médicos são exclusivos do paciente, e não podem ser alterados, falsificados, ou facilmente protegidos. Isso geralmente dá aos dados médicos uma longa vida no mercado negro. Afinal de contas, este tipo de informação geralmente inclui nomes completos, datas de nascimento, prescrições, condições, operações e outros dados que são muito difíceis de mudar e também de proteger.

(Fonte: Gary Davis é Chefe de Segurança do Consumidor na Intel Security).

News @TI

Vídeocurrículo agiliza processo seletivo de empresas

@Um processo seletivo mais ágil, barato e assertivo. É esse o objetivo ao utilizar-se o vídeocurrículo, que agora integra a gama de serviços oferecidos pela Talentix (www.talentix.com.br), recrutadora focada no mercado de TI com mais de 800 profissionais em sua base. As empresas com vagas abertas podem postá-las na plataforma, solicitar gravações de entrevistas – com perguntas customizadas – dos candidatos que mais se encaixam em suas demandas ou assistir a vídeos já publicados por R$ 70 cada.

Solução propõe trazer nova experiência de compra para o consumidor

@A Telit, líder global na área de Internet das Coisas (IoT), anuncia que seus módulos celulares vão integrar o FastSensor, produto que será comercializado para o rastreamento e sensoriamento passivo de pessoas em PDVs a fim de identificar padrões de consumo off-line e reverter em Experiência Diferente de Consumo (do inglês Real Time Experience Tracking - RET). O produto, voltado para todo o setor varejista, pretende inovar na forma que as empresas investem em marketing e mídia para atrair e fidelizar clientes (www.telit.com).