Segurança confiável

'Por que a indústria não produz melhores softwares?'

Pedro Antonio Dourado de Resende*

Parte I

Uma nota de 13 de fevereiro no Jornal do Commercio informa que a Microsoft começará a enviar, por email, boletins mensais de segurança, dentro de sua nova política chamada "Segurança Confiável", lançada há um ano. O boletim seria mais uma tentativa de melhor conscientizar usuários -- supõe-se os usuários dos seus produtos -- sobre os riscos a que se expõem pela intermediação dos seus softwares, e das proteções que deveriam dela obter, através da instalação atualizada de correções, dos chamados patches.

Mais uma vez, tal vulnerabilidade se manifestava, no dia 25 de janeiro, com o verme Sapphire/SQL Slammer. Ele trouxe, como novidade, a epidemia mais rápida da históra da computação. Após ser lançado -- segundo análise da Silicon Defense - pouco antes de 05:30 UTC, o verme passou a dobrar seu volume de infecção a cada 8.5 segundos (+ 1 seg), tendo atingido o pico de varredura em três minutos (55 milhões de varreduras por segundo), mais de 90% dos servidores vulneráveis em menos de 10 minutos, e todo o planeta em menos de meia hora.

Nada destruiu, por ser um verme e não um vírus. Mas seu tráfego obstruiu várias artérias da teia, perpetrando um ataque global de negação de serviço cuja severidade variou, conforme as características da rede local e das medidas emergenciais de defesa tomadas localmente. Medidas equivocadas terminaram por agravar o bloqueio. Também pelo mesmo motivo, o verme pôde se valer de um dos protocolos "menos inteligentes" da Internet (o UDP), que é por isso menos utilizado e menos vigiado pelos firewalls que controlam o tráfego entre as redes que a compõem, para propagar-se com menos carga (apenas 414 bytes), menos obstáculos e maior rapidez do que os vírus das grandes epidemias passadas, como o CodeRed, o Nimda e o ILoveYou.

Devido a estas caracterísitcas, o SQL Slammer consegue obstruir os canais de entrada e saída de qualquer rede local, com conexão à internet dimensionada em padrões usuais, com apenas uma ou duas máquinas infectadas saturando o tráfego. Seu único mecanismo de propagação é uma vulnerabilidade do tipo buffer overflow, presente originalmente nos servidores SQL Server 2000 e MSDE, da Microsoft.

O MSDE ("Microsoft Database Embedded"), uma versão leve do SQL, está presente em boa parte dos desktops (computadores pessoais), embutido em produtos tais como o Visio (Office), em servidores de aplicação como os gerenciadores de vírus (McAffee), e em sistemas para infraestrutura de redes (Cisco). Ou seja, diferentemente do MSSQL, o MSDE está meio que oculto em computadores de usuários comuns e em produtos de empresas

"parceiras", em posições estratégicas para a propagação de epidemias na internet.

Entretanto, conforme relato da empresa de segurança computacional Counterpane, durante os dias em que durou o ataque a Microsoft tentou rebater a culpa para seus clientes, afirmando que havia divulgado, há seis meses, um service pack contendo um patch que corrige tal vulnerabilidade do MSSQL.

Administradores é que seriam culpados pelos ataques sofridos, por não terem atualizado seus servidores SQL conforme recomendado. Voltaram, inclusive, a vociferar contra a publicização de falhas dos seus produtos, pois o Sapphire/SQL Slammer continha código muito semelhante ao que um pesquisador da segurança computacional, David Litchfield, havia divulgado para comprovar tal falha, após a empresa ter se manifestado publicamente a respeito, ao divulgar seu service pack para corrigir tal falha.

Porém, trata-se de código tão simples que o autor do verme, tendo produzido mecanismo de infecção tão eficaz, poderia muito bem tê-lo feito ele mesmo. Ao passo que a divulgação de código demonstrativo é a única ferramenta conhecida capaz de induzir empresas monopolistas de software a reconhecer falhas em seus produtos, havendo um acordo de cavalheiros na comunidade quanto a prazos para publicização.

Acontece que, dias depois, vazaram notícias de que a própria Microsoft havia sido severamente atingida pela epidemia do Sapphire/SQL Slammer. Teria ela ignorado sua própria recomendação a respeito do SQL? E se o fez, por qual motivo? Vamos aqui examinar as possíveis razões para o fracasso nas tentativas de se atribuir, à conscientização dos riscos por parte do usuário, papel tão importante na estratégia da segurança na informática.

Parte II

Como vimos acima o SQL Slammer, o verme digital mais contagioso que já atacou na internet (ao final de janeiro), atingiu severamente também a empresa produtora dos programas cuja falha explora. A notícia vazou depois da empresa ter responsabilizado seus clientes pelos próprios prejuízos. As vítimas do verme não teriam atualizado, com o patch lançado pela empresa seis meses antes, suas cópias do MSSQL.

Porém, estudos do ataque apontam como agente epidêmico mais frequente, e portanto também lá mais provável, uma versão mais leve de banco de dados usado em outros produtos seus e licenciado em softwares de terceiros: o MSDE, portador da mesma falha.

A empresa que acusa seus clientes de se vitimarem por não seguirem sua receita, teria, assim, razões técnicas para ter-se vitimado que talvez não venhamos a conhecer. Teria ela desprezado o remédio que prescreve? O remédio era ineficaz? Errou a empresa ao apontar responsabilidades? Mas a lição aqui não está na especulação sobre essas possíveis razões. Isto desviaria nossa atenção do que está no âmago da questão.

A segurança na informática tem três facetas. Existe a segurança do usuário através do software, referente aos dados que devem ser protegidos. Existe a segurança do usuário contra o software, referente à exposição dos dados a falhas e engodos, intencionais ou não, conhecidas ou não. E existe a segurança do produtor do software, referente ao seu negócio. São as seguranças através, contra, e do próprio software.

No âmago da questão, demarcado por um sentimento difuso e generalizado de insegurança do usuário devido à erosão do seu controle sobre o que se passa com os bits, reside o fato de que essas três facetas têm dinâmicas independentes, muitas vezes conflitantes. Sofware não é uma mercadoria como outra qualquer. Funciona como intermediadora da inteligência do usuário no mundo dos bits, para onde migram os processos sociais. Sua função social é, portanto, tão ou mais importante que seu mercado, principalmente quando o usuário não é o dono dos dados que processa. Enquanto ignorarmos tais fatos, ou fingirmos sua irrelevância "no mundo de hoje", esses conflitos só irão se agravar.

Entre as provas nos autos do processo que condenou, em última instância em 2001, a Microsoft por prática monopolista predatória, encontra-se um memorando interno com uma advertência do presidente aos diretores: "we are not in the business of fixing bugs, we are in the business of selling functionality". Na ocasião, Gates estava priorizando, de forma absoluta frente às outras, a faceta da segurança do seu negócio.

Meses depois da condenação, reconhecidos os efeitos prejudiciais desta priorização para o próprio negócio, a empresa deu início, com sua nova política de "segurança confiável", a uma campanha de marketing para esclarecer que agora leva a sério as outras duas facetas, havendo até então se comportado em público como se as três fossem a mesma.

Comportamento que não deve ser considerado erro estratégico, pois é reflexo do dogma central do fundamentalismo de mercado. Pode-se argumentar que a mudança de comportamento ensejada com a nova política não caracteriza confissão de negligência, e sim uma reação ao crescente anarquismo no ciberespaço. Por outro lado, pode-se também argumentar que este anarquismo foi alimentado pelo arrogante simplismo com que o fundamentalismo neoliberal encara os desafios da tríade da segurança na informática.

O que significa segurança? O dicionário Aurélio dá à palavra12 acepções distintas e o Houaiss 15, das quais seis seriam aplicáveis à nova política. Em qualquer dessas seis, confiança é ingrediente direto ou indireto, de forma que "segurança confiável" soa como pleonasmo. Como um reconhecimento velado de que a segurança antes oferecida ao usuário não era nenhuma dele (contra ou através do software), e sim a do negócio do software, mas que agora - pode-se confiar - as dele serão relevadas.

Parte III

A súbita conversão da Microsoft à importância dos seus clientes confiarem na segurança oferecida por seus programas não implica em sucesso automático da sua nova política, nomeada aqui no título. Entre intenção e sucesso, faz-se necessária certa capacidade. E tal capacidade não se esgota, como poderia sugerir a campanha publicitária desta nova política, com a conscientização dos usuários para a importância de manterem atualizados as sucessivas correções nos softwares. Esta é uma das lições do incidente "SQL Slammer".

Assim como o Code Red, o SQL Slammer espalhou-se através duma falha num software da empresa para a qual já havia um patch disponível há meses. Entretanto, até redes nas quais todas as instalações do MSSQL estavam devidamente atualizadas se viram vítimas diretas, porque o patch não corrigia o MSDE embutido em outros softwares. Doutra feita, devido às características do verme, remendar 99% das instalações seria inútil.

Administradores de redes sabem que o custo extra para se garantir 100% de atualizações,

comparado a 99%, não compensa a risco direto de uma infecção como a do SQL Slammer. O custo extra para os últimos 1% é desproporcional, ferindo prioridades. E mais uma vez, bastou que administradores de umas poucas redes seguissem a lógica, poupando gastos injustificáveis de proteção contra um risco anunciado, para que mais uma epidemia se alastrasse. A própria empresa responsável pela vulnerabilidade pode ter seguido esta lógica.

O que mais isto nos ensina? Que o risco direto não é o único. Mesmo se a minha rede estiver "100% protegida", com os patches 100% aplicados e supondo que todas as vulnerabilidades conhecidas estão corrigidas por esses patches (o que não ocorreu com a falha explorada pelo SQL Slammer) , posso ainda ser vitimado por brechas nas redes vizinhas. Em ataques de negação de serviço como o do SQL Slammer, redes vizinhas infectadas podem saturar meus canais de tráfego. Portanto, que o risco indireto é global, transitivo e relacionado principalmente à qualidade dos softwares predominantes na internet.

Embora não se possa condenar a lógica econômica dos adminstradores de rede, pode-se condenar a hipocrisia doutrens que persistem em julgamentos simplistas sobre as responsabilidades. Mesmo que eu não use drogas e seja cauteloso, as chances de uma bala perdida me atingir são proporcionais à desenvoltura com que os traficantes atuam na minha vizinhança. A escolha de onde viver não pode me condenar por isso, caso os criminosos atuem com inaceitável desenvoltura por toda a cidade. E tal vem ocorrendo, quaisquer que sejam as opções para votar em governantes, apesar dos impostos que pago para obter segurança pública. Antes de ser culpado, sou refém.

Quando se trata de software proprietário monopolista, os patches só surgem de alguma ameaça de dano à imagem do fabricante. Na maioria dos casos levam meses para ficarem prontos, muitas vezes devido à dependência em relação a outras modificações no software, planejadas ou não. Frequentemente a primeira versão é inócua. E quando não o é, pode ocorrer de subverter alguma correção anterior doutra vulnerabilidade. Cada vez em maior número, fazem da atualização 100% um objetivo cada vez mais utópico, um objetivo que precisa ainda enfrentar, além do custo meteórico, a esquizofrenia dos principais fabricantes.

A indústria monopolista de software proprietário quer instituir a censura sobre vulnerabilidades nos seus produtos, como reza a missão da OIS, ao mesmo tempo em que quer também dos usuários uma melhor conscientização sobre as mesmas. Ora dizem que software proprietário é mais seguro porque seu código fonte é desconhecido, ora que vão abrir o código fonte para clientes que precisem de auditoria (os grandes, é claro), ora que não podem abrir o código porque isso revelaria mais vulnerabilidades.

Querem ser os únicos intermediadores do conhecimento sobre os riscos que corremos com seus produtos, sendo também os responsáveis por esses riscos. Sem, é claro, submeterem-se às regras gerais de comércio ou da epistemiologia, como querem suas licenças de uso e seus lobbies por novas leis. A adjetivação da segurança que nomeia esta nova política. pode, portanto, a eles parecer necessária, mas é apenas um pleonasmo a nos revelar o absolutismo com que almejam sacramentar o seu poder econômico. Por que é assim?

Parte IV

Dito de outra forma, por que a indústria simplesmente não produz melhores softwares? A resposta é simples, porém, ofuscada pelo discurso da ideologia dominante: Por limitações no modelo de negócio prevalente, monopolista. Nele, a evolução do software é guiada pelo

efeito rede e pelo fluxo de caixa do produtor, este guiado pelas expectativas de retorno do capital investido. Em decorrência, a obsolescência e a dependência (a padrões fechados) precisam ser programadas para garantir-lhe a segurança do negócio.

No caso das drogas, é a própria fisiologia do organismo consumidor que provê essa programação, mas no caso do software essa programação precisa ser embutida no objeto de consumo.

Isto induz crescentes complexidades nesta evolução, desnecessárias à sua utilidade, que antagonizam a segurança do negócio vis a vis a segurança do usuário, contra ou através de softwares. Enquanto o esforço necessário para se corrigir vulnerabilidades cresce exponencialmente com o tamanho destes. Diz-se que o código fonte do Windows XP tem 60 milhões de linhas, muitas delas para criar 16 portas de fundo com as quais a Microsoft controla remotamente a obediência aos termos da licença. Ao passo que o GNU/Linux, de utilidade equivalente, nas distribuições mais completas não alcança 7 milhões.

Os que desdenham software gratuito e se maravilham com o maior sistema operacional já produzido, não se dão conta de que 60 milhões de linhas tornam um software praticamente indepurável, e que malfeitores tendem a descobrir como se esgueirar por tais portas de fundo. E pior, que a licença do XP é como um contrato de aluguel sem preço e prazo para as próximas prestações - a título de upgrades, fato "esquecido" em pesquisas comparativas sobre custo total de uso, como as do IDG. E que a diferença disto para extorção, quando a propriedade intelectual do XP se estente aos padrões em que são gravados os acervos dos usuários, é um verniz de legalidade.

Na alternativa do software livre, fluxos de caixa são guiados pelo mercado de suporte e serviços, enquanto a evolução do software é guiada por demanda e oferta expontâneas, o contrário e o oposto do modelo proprietário. Em vez de monopólios a traduzir a "voz do mercado" para a sociedade, uma comunidade age em seu próprio interesse utilitário, onde o modelo de licença impede a monopolização comercial: o monopólio ali é o da liberdade semiológica. Doutra parte, a lógica de produção de software proprietário aponta para um inexorável crescimento em complexidade, instabilidade e custo social, camuflados como danos colaterais na evolução "que o mercado pede": efeito manada.

Como esta camuflagem tem eficácia limitada, a única saída para a auto-preservação do modelo proprietário é a criminalização de modelos alternativos que se orientam pela segurança do usuário. A virulência dogmática do ataque orquestrado pela Microsoft ao projeto GNU e seu modelo de negócio, a licença GPL, são emblemáticos da busca por esta saída.

Vivemos em sociedades cujo poder público cede espaço ao crime organizado, ao poder da economia paralela do tráfico de drogas, de armas e de dinheiro sujo, poderes que se mesclam em situações obscuras. Mas a consciência deste fato não dará, sozinha, a eficácia desejada aos instrumentos de que dispõem para controlar riscos no convívio com tais poderes. Da mesma forma, a consciência de co-habitarmos um mundo virtual onde monopólios ditam regras de convivência e sobrevivência, não nos dará o poder de controlar os riscos desta convivência.

A economia do tráfego é sustentada pela parte dependente e viciada da sociedade vitimada, cujo nível de consciência a respeito, sozinho, só afeta o perfil e a dinâmica dos riscos, nunca os seus níveis. A sociedade só influirá nos níveis de risco na medida em que tal consciência

agir contra as dependências e vícios. Esta opinião compartilho com Paul Simons, secretário-assistente de Estado dos EUA, em matéria da Folha de São Paulo de 4/3/03. Mas talvez não a sua abrangência. Não importa se o espaço é físico, a droga é química e seu comércio é ilegal, ou se o espaço é virtual, a droga tem a forma de software e seu comércio enverniza-se de legalidade.

Revista Consultor Jurídico, 3 de abril de 2003.