

Os perigos da informática: quando os riscos se concretizarem!

FRANÇOIS SETTEMBRINO



Trata-se apenas de um bom título para atrair a atenção do leitor ou ele representa uma visão realista da situação? Estamos tão mergulhados no mundo dos computadores, em nossa relação com máquinas, contatos, e-mails e outras redes associadas, que nem nos damos conta que há uma dependência excessiva. Os médicos recomendam que nos desliguemos o mais frequentemente possível para não colocarmos nossa saúde em risco. Além disso, eles nos lembram que devemos, antes de mais nada, ser vigilantes quando estivermos trabalhando, dirigindo ou participando de interações sociais reais. A única preocupação dos médicos é permitir que nós consigamos manter um equilíbrio vital, que corre o risco de desaparecer rapidamente sem que percebamos devido à intervenção das máquinas, como mencionado acima. A zona problemática é muito mais extensa do que podemos imaginar. A seguir, faremos uma abordagem simples de alguns aspectos.

Vamos começar por uma data: 8 de abril de 2014. Não faz muito tempo, mas esse foi o dia estabelecido pela Microsoft para cortar os vínculos com o Windows XP e interromper o fornecimento de atualizações de segurança e suporte. A Microsoft não vai ficar eternamente atualizando um programa ultrapassado que foi substituído várias vezes de maneira muito mais eficiente. Será que nós ainda podemos modernizar os computadores antigos, já que a aquisição de um computador novo pode representar um rombo muito grande no orçamento de alguns usuários? Em algumas máquinas, será possível realizar um upgrade, mas isso não necessariamente facilitará o uso. Em muitos casos, se as máquinas forem fracas demais, esse upgrade será impossível e, conseqüentemente, os problemas aumentarão com o tempo. No entanto, a situação é mais grave do que parece. Muitas pessoas optaram por correr os riscos e continuar usando o XP, pois não possuem os recursos nem a vontade de comprar um novo computador. Nas empresas, isso pode ser ainda mais grave. Só na Grã-Bretanha, apenas no setor de saúde, mais de um milhão de máquinas executavam o XP... E estima-se que ao redor do mundo o mesmo aconteça na maioria dos caixas eletrônicos. É claro que, a menos que sejam confirmados, esses dados não são totalmente precisos. Além disso, é possível que a

Microsoft precise rever sua posição ou adotar uma postura mais flexível, mas isso pode ser apenas um desejo nosso, pois quanto mais o tempo passa, mais difícil se torna a situação. De qualquer forma, é bom lembrar que há mais de um bilhão e meio de PCs sendo usados no mundo todo, e mais de 90% desses PCs executam o Windows. Nem todos são XP, mas muitos deles ainda devem atender às necessidades de seus usuários. Aqueles que ainda estão em uso em empresas, principalmente em pequenas e médias empresas, lucrariam muito se fossem modernizados o mais rapidamente possível ou substituídos para manter um nível satisfatório de segurança. Talvez seja necessário pedir a ajuda de especialistas, o que não sairá de graça.

A segurança também é o que mais precisa ser protegido nas máquinas de pessoas físicas. As atividades bancárias realizadas nos PCs podem se tornar um alvo fácil para criminosos e, para se proteger, os bancos podem negar acesso aos clientes XP. As pessoas que tiverem um “guru” de informática como amigo deverão pedir a ajuda dele o quanto antes. Se nenhum amigo puder ajudar, talvez seja necessário solicitar os serviços de um profissional, o que provavelmente será caro, e a proteção nunca será completa.



QUESTÕES A SEREM CONSIDERADAS

O que mais devemos monitorar e temer ou a que mais devemos nos submeter? As considerações a seguir são apenas exemplos. Algumas são superficialmente conhecidas, em consequência de tudo o que a mídia tem divulgado com razoável competência; já outras são conhecidas com mais detalhes, graças a certas revelações (as informações fornecidas por Snowden sendo as mais recentes e também as mais graves). Tudo começa com o roubo de dados por meio de um e-mail. Menos visíveis, contratos inteiros passam pelos serviços de tradução on-line, que, sejam piratas ou suspeitos, permitem que a concorrência seja informada rapidamente sobre tudo. Dessa forma, a propriedade intelectual não tem nenhum sistema de defesa válido, e os países da Europa Ocidental não têm mais nenhum segredo; é a economia desses países que está em perigo. Para começar, não existe nenhuma regulamentação eficaz sobre dados. Quando os primeiros cartões de fidelidade começaram a proliferar nas lojas, ninguém quis enxergar que os dados pessoais dos clientes poderiam ser usados de maneira mal-intencionada e que poderia ser perigoso saber tudo sobre esses clientes. Vários elogios foram feitos sobre a proteção de dados pessoais, mas todos têm o direito de questionar e corrigir essa proteção como desejarem. Mas quantos se aventuraram? Se é cliente de uma cadeia de lojas internacional, você não tem a menor ideia de como seus dados pessoais são usados, mas sabe que eles têm um valor inestimável. Os arquivos das grandes cadeias de loja permitem restringir a parte aleatória das decisões de compra, já que o perfil do comprador é quase totalmente conhecido. Se adicionarmos tudo o que cada pessoa deixa como rastro, ou seja, vários cartões, telefonemas em que tudo é gravado, visitas a uma ou diversas redes sociais, diferentes e-mails, eventuais prontuários médicos e até mesmo o sistema GPS, tudo pode ser usado de forma enganosa. Não se esqueça também dos milhares de cookies que representam

um rastro indelével e contêm inúmeras informações sobre você. Eles permitem que você seja rastreado, que suas preferências sejam detectadas e que seus comportamentos sejam recriados. O Google não perde a oportunidade de enumerar os méritos dos cookies; contudo, ele vai substituí-los por um login anônimo, mais eficiente e mais capcioso, do qual o Google será o único proprietário.



Você não poderá nem dar sua opinião. E chegará uma hora em que os estabelecimentos comerciais e industriais que não usam o Google Chrome não poderão mais personalizar sua publicidade. Assim, indivíduos como nós não têm mais nada, nada mais nos pertence por direito ou de forma privada. Nossos dados pessoais e todos os rastros que deixamos por toda parte serão usados permanentemente, quer trate-se de uma contratação, de uma garantia, de um processo jurídico, etc. Além disso, todas essas informações são coletadas por empresas (Google e muitas outras) regidas por leis e tribunais estrangeiros e que podem fazer praticamente o que quiserem. No entanto, se quisermos ocultar algo de nossos registros, não teremos o poder de fazê-lo. É muito moderno ter um perfil no Facebook ou em qualquer outra rede social, mas antes precisamos compreender que a divulgação de nossa vida privada só poderá ter consequências negativas. E boa sorte se houver litígio e você quiser levar o caso aos tribunais, principalmente se for um tribunal americano, pois os principais favorecidos respondem às leis americanas. Não devemos esquecer também que, para se beneficiar da proteção das leis dos Estados Unidos, é necessário ser cidadão americano.

HISTORIA RECENTE

Se analisarmos a história, poderemos lembrar que foram os militares americanos que permitiram o desenvolvimento dos computadores pessoais, ou PCs. Foram eles que requisitaram e promoveram essa maravilhosa ferramenta chamada Informática. Poucas pessoas perceberam que o próprio nome não passa da justaposição de duas simples palavras: INFORmação/ autoMÁTICA. E, de fato, ao longo do tempo o enorme desenvolvimento de computadores cada vez mais potentes, de uma rapidez assustadora e dotados de memórias praticamente infinitas tornou possível quase que automaticamente a coleta de dados confidenciais, até mesmo os mais secretos, e permitiu o estabelecimento de uma vigilância quase universal. O problema é que, mais uma vez, são os militares americanos que detêm todo poder.

Porém, durante todo esse tempo, o poder de intervenção das máquinas americanas só fez crescer. Essas máquinas são capazes de invadir secretamente qualquer lugar. Os poderosos americanos podem interferir na vida de pessoas físicas como nós, através da “porta dos fundos” de nossos computadores, e também no funcionamento de qualquer organização, até mesmo da polícia. O poder das máquinas usadas por eles é surpreendente, o que lhes permite misturar

alguns parâmetros ínfimos de qualquer sistema ou rede, industrial ou militar, e torná-los obsoletos ou inoperantes. Até mesmo os sistemas de segurança deles foram criados em conjunto. Uma criptografia eficaz é uma questão para os grandes especialistas, principalmente os americanos, e somente tal criptografia pode proteger eficazmente as indústrias e os governos. Quando você compra um computador, 90% do sistema é Windows, e quem pode garantir que a proteção criptográfica pela qual você pagou caro não possui um pequeno dispositivo, conhecido apenas pelo desenvolvedor?

O título do artigo faz referência a nosso novo ambiente; o risco não é mais aleatório nesse ambiente e está sempre presente. Todos os dias, temos novas provas. Veja a seguir algumas delas:

- A receita federal do Canadá descobriu uma falha em seu software de criptografia que pode ter permitido que os dados de um grande número de pessoas tenham sido pirateados.
- Em Bélgica, o sistema de informática do SPF Finances parece ser vulnerável, apresentando falhas em todos os níveis.
- - O ING chamou a atenção do público quando propôs vender informações sobre o



comportamento de compras de seus clientes. Nesse cenário, segurança e respeito à vida pública parecem ser os grandes perdedores, pois os arquivos dos clientes são vendidos ou alugados a peso de ouro.

Esses são apenas alguns exemplos, e é muito provável que alguns tipos de uso ilícito ocorram impunemente em segredo absoluto. Nós, como usuários, somos igualmente responsáveis, pois poucas pessoas leem as letras miúdas que informam que podemos impedir que nossos dados sejam compartilhados com “parceiros” desconhecidos.

art-5-peligros-de-informatica-marzo-15 Tentamos chamar a atenção dos responsáveis políticos sobre os perigos existentes, mas nenhuma medida tem sido tomada. Nem a Europa percebe o perigo e só planeja abordar o problema em 2015. Enquanto isso, as redes coletam somas astronômicas, das quais só receberemos migalhas que nunca serão capazes de revitalizar nossa economia. Será que a situação dos responsáveis pelo Gerenciamento de risco é melhor? O famoso Instituto de gerenciamento de risco (Institute of Risk Management) de Londres aprofundou a questão do Cyber Risk, como é chamado. O resultado é assustador:

- Um total de 360 milhões de contas bancárias foram alvo de atividades criminosas e, segundo a KPMG, só em 2012 os dados de 160 milhões de pessoas foram divulgados sem autorização.
- 70% dos responsáveis pelo gerenciamento de risco não são qualificados nem têm experiência nesse campo.
- Das empresas entrevistadas, 53% não têm diretrizes sobre o assunto.
- Apenas 27% verificaram a integridade das medidas de segurança usadas por sua “cadeia de suprimentos”.
- Como se isso não fosse suficiente, 45% dos entrevistados não sabiam se sua empresa já havia sofrido ciberataques ou danos relacionados.

Há algo que nós possamos fazer? Pois o caso é urgente. Aqueles que quiserem estudar o problema em mais detalhe não podem se contentar em ler este modesto artigo. Veja a seguir duas dicas:

- Em primeiro lugar, a incrível (em francês) “la Souveraineté Numérique” de Pierre Bellanger, edições Stock, 2014, visita a questão.
- - Em seguida, sugerimos um resumo e o relatório sobre Cyber Risk do IRM (em inglês), que podem ser baixados do site do instituto (www.theirm.org). ■

CONCLUSÕES

De quem será a culpa se o risco se concretizar? Nós seremos os primeiros culpados, pois estamos envoltos por todos os tipos de perigo na rede. Em seguida, podemos apontar os profissionais de informática, que não avaliaram os riscos, ou ainda os responsáveis pelo gerenciamento de risco, que não acompanharam a evolução do problema e não reagiram. Eles deveriam ter instruído sua hierarquia e seus chefes, mas esses últimos são ainda mais responsáveis por não terem se preocupado suficientemente com o fenômeno. O mundo político não conseguiu acompanhar, quando, na verdade, deveria ter antecipado as catástrofes que nos aguardam.

Daremos a palavra final a Pierre Bellanger:

“A internet e seus serviços são controlados pelos americanos. A internet rouba nossos empregos, nossos dados, nossa prosperidade, nosso sistema tributário, nossa soberania”.

Essa é a certeza do momento atual; para merecer seu nome, o gerenciamento de risco precisa reagir, e já está mais do que na hora.