Dá para conciliar segurança com agilidade?

atalho

A segurança das informações que circulam pelas corporações não pode depender de medidas isoladas como controle de acesso ou proteção das redes. É preciso muito mais do que isso, na verdade um conjunto de ações e processos que exigem vigilância constante, além de um trabalho incansável de educação das equipes e de revisão de comportamentos. Só assim, dizem profissionais de TI e executivos de empresas fornecedoras, é possível garantir às corporações o máximo de segurança, sem comprometer a agilidade na tomada de decisões e na aplicação das estratégias de negócios.

O desafio de preservar a segurança da informação em um ambiente de profundas transformações tecnológicas tem tirado o sono de muitos CIOs. Afinal, diante de tendências inexoráveis como a mobilidade, as redes sociais, a computação em nuvem, é cada vez mais decisivo para a sobrevivência e o sucesso das empresas o controle rigoroso da segurança das informações. É o que se discute nesta mesa-redonda, coordenada pelo diretor de redação do Informática Hoje, Wilson Moherdaui, e que, excepcionalmente, teve a participação não apenas de executivos de TI, mas também de representantes de empresas fornecedoras de produtos e soluções de segurança da informação: **Alberto** Lemos Araujo Filho, responsável pelas operações na América Latina da Bull, integradora de tecnologia de base francesa; André **Carraretto**, estrategista em segurança da Symantec Brasil, empresa que atua no segmento de segurança e de guarda de informações e soluções de backup; **André** Luis Carvalho, CIO para a América Latina da área agrícola da Dupont, multinacional norte-americana que atua em 13 segmentos de mercado; **Bruno** Zani, engenheiro de sistemas da McAfee do Brasil, empresa fornecedora de software de segurança; **Claudia** Ferraz, CIO para a América Latina da GE Power & Water, especificamente para a área da empresa que atua no setor de limpeza e tratamento de águas para reutilização, e utilização para bebidas; José Henrique **Guedes**, sócio-diretor da Multiedro, empresa integradora de soluções Google e de serviços de segurança da informação para o mercado corporativo; **Rodolfo** Balaniuc Dantas, superintendente de informática da Comgás, empresa responsável pela distribuição de gás natural na área de concessão do estado de São Paulo; e **Vanderlei** Ferreira, CIO do grupo EDP Energias do Brasil, que reúne 14 empresas na distribuição, comercialização e geração de energia elétrica em todo o país.

IH – Como vocês encaram a questão da segurança diante das novas ondas tecnológicas?

Rodolfo – Na Comgás, nós já temos alguns projetos que envolvem segurança na área da mobilidade: a gente está analisando ferramentas que nos possibilitem fazer o gerenciamento da utilização dos equipamentos móveis espalhados pelo campo. Sejam eles coletores de dados, PDAs ou tablets, já temos a definição de que, em paralelo a esse projeto do negócio, a área de tecnologia deve buscar a melhor alternativa para gerenciar esse novo ambiente. São cerca de 500 usuários, entre funcionários da companhia e terceiros, o que é mais uma complicação nessa equação. Além da preocupação com a segurança da informação que vai transitar, existe a de ordem física, dos equipamentos. Temos pensado numa solução para ficar na ponta que não seja muito chamativa, para evitar roubo. Até pouco tempo, tínhamos na Comgás um especialista responsável pela área de segurança de TI, que deixou a empresa e nós estamos com dificuldade para repor, porque esse mercado está bastante aquecido.

IH – Nesses casos, você costuma recorrer a terceiros?

Rodolfo – Complementamos as nossas necessidades com nossos parceiros, sim.

IH – Você considera isso uma vantagem ou uma desvantagem?

Rodolfo – Acho que é uma necessidade, porque esse negócio evolui tanto e tão rápido que é praticamente impossível uma empresa como a Comgás, cujo negócio não é tecnologia, se manter atualizada com tudo o que acontece.

IH – Esse profissional de segurança que você tem dificuldade de encontrar no mercado se reporta a você?

Rodolfo – Responde para um gestor da minha área de TI, que se reporta a mim. Nós temos no nosso portfólio ferramentas que controlam o nosso ambiente, mas nas nossas estatísticas mensais a quantidade de tentativas ou de ataques na empresa é um negócio absurdo. Como a gente até agora tem conseguido sobreviver, então acho que estamos mais ou menos suportados para tocar o nosso negócio.

Vanderlei – A segurança da informação para o grupo EDP mundialmente é a principal diretriz para o desenvolvimento de nova tecnologia. Nós montamos uma estrutura específica de segurança da informação, que responde para mim. Eu tenho um especialista de segurança da informação e uma equipe junto com ele. Nos últimos dois anos, nós elaboramos um plano estratégico de segurança da informação, com vários itens que deveriam ser implementados em dois anos. Hoje já estamos numa situação muito boa. Nós fizemos uma avaliação de custo-benefício, optamos por não comprar os equipamentos e sim fazer um outsourcing, porque o foco da empresa é gerar, distribuir e comercializar energia elétrica. Criamos algumas iniciativas, como a Semana da Segurança, porque fizemos uma pesquisa interna e detectamos que as pessoas sabem o que é segurança, mas ninguém pratica. E vem dando resultado. O órgão regulador hoje exige que o setor de energia tenha uma maior interatividade com seu cliente. Isso significa que a empresa tem agência virtual, tem seus dados circulando, então temos que tomar o máximo de cuidado para não ter as informações dos nossos consumidores expostas. Essa tem sido a nossa grande dor de cabeça. Quanto aos dispositivos móveis, num primeiro momento eu fui radical, simplesmente não deixei: se é seu, tem que estar na sua casa. Não deixei, primeiro porque eu não tinha como comprovar: no começo, todo mundo diz que é somente para ler e-mail, depois quer entrar na rede. Então eu estudei o mercado, vi o que tinha de ferramentas para fazer essa gestão, criei uma norma interna e agora, já com a monitoração instalada, vou começar a liberar gradualmente. Não foi uma decisão popular, mas deveria ser tomada, então estou tranquilo quanto a isso.

IH – Me parece que o grande dilema de vocês é entre restringir, para evitar riscos, e liberar, para os negócios fluírem. Agora, como é que você faz para impor uma restrição tão radical?

Vanderlei – Hoje a norma existe e está lá, mas eu sei que não vou sair vitorioso, é uma guerra que eu sei que vou perder. Eu não posso falar para o pessoal mais jovem não entrar no Facebook. Eles não entram no Facebook no equipamento da empresa, mas estão no Facebook o dia inteiro, no smartphone, só não estão conectados na minha rede. Eu preciso preparar a empresa para isso.

IH – O foco principal da sua restrição é a rede: você não deixa se conectar à rede nada que seja estranho.

Vanderlei – Por exemplo, na contabilidade, no planejamento estratégico, na área financeira, que hoje tem concorrência, tem leilões e promoções estratégicas, você não conecta pen drive. Quem autoriza ou não pen drive é o gestor executivo ou o diretor da área específica, solicitando que a área de segurança da informação avalie se libera ou não.

IH – Em relação aos funcionários mais jovens, deve ser ainda mais difícil impor restrições desse tipo, uma vez que os limites entre a vida profissional e a pessoal são cada vez menos visíveis para eles.

Vanderlei – Acho que isso eu consegui transmitir para eles. Nós pegamos vários relatórios e informações de intrusões que ocorreram através de equipamentos móveis, e conseguimos conscientizar o pessoal. De toda forma, minha decisão não é definitiva, é temporária, ou seja, eu preciso de um tempo para avaliar, de um lado o que o usuário quer e, do outro, o que o negócio exige. Se o negócio exige, eu vou avaliar e liberar. Mas naquele momento eu não estava preparado, então não podia liberar, já que podia colocar em risco toda a organização.

fotos hamilton pena

“Nós temos no nosso portfólio ferramentas que controlam o nosso ambiente, mas nas nossas estatísticas mensais a quantidade de tentativas ou de ataques na empresa é um negócio absurdo”.

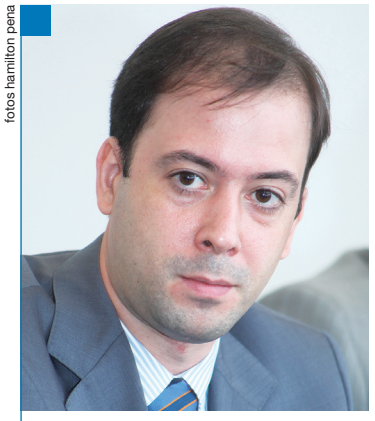
Rodolfo, da Comgás

“Quando se fala em acesso ao Facebook e outras redes sociais, acho que não se deve passar a responsabilidade para a TI: a responsabilidade é da linha de gerenciamento”.

André, da Dupont

mesa-redonda

fotos hamilton pena



“Muitas vezes, o cliente pensa que a informação só está num ponto, mas ela está copiada em outros lugares. Nesse aspecto, a nuvem é uma nova preocupação”.

Carraretto, da Symantec

IH – Eu quero propor aos fornecedores aqui presentes um desafio: qual seria o primeiro conselho que vocês dariam aos seus clientes para que eles tivessem o controle necessário sobre a informação que transita dentro da empresa e da empresa para fora?

Carraretto – O primeiro passo é você entender onde está a informação que você quer proteger. Muitas vezes as empresas têm a informação dispersa e você não sabe se ela só está naquele lugar ou se tem cópias em vários lugares. Só então você vai poder estabelecer controles que vão limitar o uso a quem precisa, ao ambiente onde aquela informação é necessária e depois vai fazer um controle mais completo.

IH – Como se faz para identificar onde a informação está sendo gerada e por onde ela está circulando?

Carraretto – A tecnologia chave para isso é a Data Loss Prevention. Hoje é a solução que ajuda muito na identificação dessa informação que é sensível. Muitas vezes, o cliente pensa que a informação só está num ponto, mas ela está copiada em outros lugares. Nesse aspecto, a nuvem é uma nova preocupação. Falando da questão dos dispositivos que podem ser conectados à rede, eu concordo com o Vanderlei em fazer o bloqueio num momento inicial, porque o usuário alega que é só o e-mail. Acontece que o e-mail é um dos mais importantes ativos de informação que a empresa tem. E se ele coloca o e-mail no tablet e é roubado no aeroporto? Então você precisa entender que informação é sensível e onde ela vai ser usada, para poder começar a estabelecer esses controles. Aí você começa a ver que é preciso realmente que o e-mail chegue aos tablets, e vai entender que tecnologia pode usar para poder proteger aquela informação.

IH – Que tipo de problema vocês têm encontrado com mais frequência?

Carraretto – Sem dúvida, na parte de mobilidade. Embora eu ache que a parte tecnológica é relativamente simples de ser resolvida, porque existem boas soluções no mercado, há outras questões não relacionadas a tecnologia com as quais a empresa tem que se preocupar antes de disponibilizar as soluções. Por exemplo: que política eu vou estabelecer para permitir que o meu usuário traga o dispositivo dele para dentro da empresa? Vou fazer um contrato com ele para que aquele dispositivo possa ser usado? Que tipo de informação eu vou permitir que ele acesse nesse dispositivo? Se ele quer acessar uma informação de nível mais sensível, eu vou precisar instalar naquele dispositivo uma solução de controle mais poderosa. A questão de política tem que ser abordada primeiro, para definir essas fronteiras e como vão ser os usos. Tem que envolver o RH, para entender se isso tem alguma violação de direito do usuário, para só então pensar na tecnologia.

Guedes – Embora eu não seja especialista em segurança, esse é um assunto que permeia o nosso dia a dia dentro da solução em nuvem. Com o acesso à Internet, a preocupação aumentou muito com o usuário móvel. O gerenciamento da infraestrutura é cada vez mais complexo, ao mesmo tempo em que há um movimento de mercado pela usabilidade, que a gente não vai conseguir parar. Imagine você ter uma estrutura 100% própria, num datacenter seu, para ter usuários móveis no mundo inteiro. Só o controle que você vai precisar ter de infraestrutura de borda para garantir esse acesso é gigantesco. E a computação em nuvem, no fundo, é só mais um tipo de terceirização: você está terceirizando toda a sua infraestrutura dentro de um provedor que tem uma escala gigantesca. Também acho interessante a ideia de tentar restringir, mas acho que é um movimento irreversível de utilização e concordo que o principal desafio é a conscientização do usuário para garantir que ele vai tratar com o devido zelo aquela informação que a área de TI tenta proteger com unhas e dentes. Qualquer celular de R$ 100,00 hoje tem câmera, então é possível tirar foto do e-mail, de qualquer informação. Aí, todo o esforço de impedir download da rede em pen drive é inútil. No final das contas, segurança, como qualquer outra coisa, é uma questão comparativa. Ou seja, nuvem é mais ou menos segura do que o quê? Na prática, a gente tem conseguido demonstrar que a segurança do seu dado dentro da nuvem é maior na maioria dos casos do que você ter o dado interno. Se a gente colocar em perspectiva, falando de detecção de intrusão, se alguém tiver interesse em roubar um dado específico e conseguir localizar o seu datacenter, tem um alvo claro para procurar o dado. Quando você está numa infraestrutura de nuvem, ele não tem mais um alvo claro para buscar a sua informação. O Google, como um dos

principais fornecedores, tem uma estrutura de segurança gigantesca. Ele nem divulga a localização dos datacenters, trata isso de forma absolutamente confidencial, e além disso tem uma política de replicação em vários datacenters em vários lugares do mundo.

Carraretto – Eu concordo em que a segurança na infraestrutura dos provedores de serviço realmente tem dimensões muito grandes. Agora, um ponto que ainda precisa de evolução é que a identificação do acesso é um dificultador para o cliente final, quando o dado vai para alguma nuvem, seja uma nuvem de CRM, de compartilhamento de arquivos, de e-mail,. Quando aquela infraestrutura estava dentro da própria empresa, a empresa tinha melhor condição de saber quem estava acessando e o que estava acessando a qualquer momento. Quando a informação vai para fora, quem tem essa visão é o fornecedor do serviço. Quem está acessando aquele serviço, é um usuário e senha? Hoje não dá para usar mais só usuário e senha, você tem que ter um fator de identificação, seja biometria ou token, para poder garantir que quem está acessando alguma informação não seja alguém que roubou a senha de outro. Eu preciso exigir uma autenticação do segundo fator, para garantir que quem está chegando é quem eu quero que chegue, já que é muito fácil hoje em dia roubar a senha de alguém. Minha primeira preocupação ao acessar um serviço na nuvem é que tipo de autenticação eu vou fazer para acessar esse serviço.

Guedes – O Google especificamente tem o segundo fator de autenticação gratuitamente, tem token para qualquer dispositivo celular. Isso entra de novo na questão da escala, é muito mais barato para o Google implementar essas ferramentas de segurança e deixar disponíveis para todo mundo, do que uma empresa individualmente fazer isso para dois usuários ou 10 mil usuários. De novo, você não tem que investir em infraestrutura. Eu concordo com você: a parte fundamental da solução de nuvem é dar para o usuário o mesmo nível de controle que ele teria internamente, mas dando o ganho da escalabilidade, da disponibilidade e da flexibilidade que a nuvem vai trazer para ele.

Claudia – Eu estou na GE há muitos anos, é uma empresa que sempre foi muito focada em segurança. Para se ter uma ideia, são 400 mil funcionários, acaba tendo escala, e ela criou uma nuvem interna, para não ter que abrir as portas para uma nuvem externa no começo, mas aos poucos ela foi se abrindo. Não tem jeito, o mercado precisa que você abra. Agora nós estamos lutando com a questão do bring your own device [traga o seu próprio dispositivo]: o RH fala que o funcionário pode processar a empresa porque mandou e-mail de casa e não recebeu hora extra. A gente conseguiu agora que o jurídico e o RH aprovassem. Mas tudo isso é muito complicado, não se sabe bem até que ponto pode abrir. Acho que o que temos que fazer é conscientizar o usuário: segurança começa no usuário e termina no usuário. Então é treinamento, campanha, publicidade, semana de segurança. A grande vantagem que a gente tem é que a segurança da GE é global, as políticas globais vêm de cima, então é mais fácil de implantar.

IH – A política de adoção de ferramentas e soluções é global, mas você se sente bem atendida?

Claudia – Além das senhas, a gente tem solução de token para conexão externa. Temos antivírus, safe boot, tudo com senha. Inclusive celular, para se conectar à rede, tem que ter senha. Mas hoje em dia a gente não se pode proibir uma pessoa de acessar o Facebook no escritório, mesmo porque ela está com o Facebook aberto no celular.

Bruno – No capítulo conscientização, é preciso lembrar que o usuário ainda vê o responsável pela segurança da informação como vilão: é aquele cara que vai monitorar o que ele está fazendo e, em última análise, pode conduzir

"Na prática, a gente tem conseguido demonstrar que a segurança do seu dado dentro da nuvem é maior, na maioria dos casos, do que você ter o dado interno".

Guedes, da Multiedro

"Acho que o que temos que fazer é conscientizar o usuário: segurança começa no usuário e termina no usuário. Então é treinamento, campanha, publicidade, semana de segurança".

Claudia, da GE Power & Water

mesa-redonda

fotos hamilton pena

“Temos que entregar segurança com controle e com performance, porque segurança não pode interferir no negócio”.

Bruno, da McAfee

uma empresa que precisa que seus usuários utilizem aplicações móveis, como e-mail e Internet, num celular ou num tablet da própria empresa. Isso é mais fácil de controlar, porque, como a empresa é dona do ativo, consegue implementar uma política e o usuário tem que cumprir normas para utilizar aquele ativo. De outro lado, há a situação em que o dispositivo móvel é do funcionário e ele quer usá-lo para acessar o e-mail corporativo. Ele vai ter que seguir algumas normas, mas a empresa não pode, por exemplo, bloquear no celular dele o acesso à câmera ou a um aplicativo qualquer. A gente tem que balancear isso. Se a gente for liberar o acesso, precisa por exemplo verificar se o celular suporta criptografia. Temos que entregar segurança com controle e com performance, porque segurança não pode interferir no negócio. Um aspecto interessante é que a segurança muitas vezes está mais ligada ao negócio do que à TI. Por exemplo, a classificação de dados: o dado é do negócio, não é de TI. A TI até cuida do dado do RH, mas não é dona do dado de RH.

a alguma punição a ele. Então, a gente precisa tentar trazer segurança para a linguagem dele. Precisa trazer o usuário para o nosso lado e aumentar o valor dele nesse processo, para que ele nos ajude. A mobilidade, de fato, é um dos maiores desafios à segurança. De um lado, a gente precisa garantir a mobilidade para

IH – Do seu ponto de vista como fornecedor, quais são as principais vulnerabilidades dos clientes que procuram vocês?

Bruno – Isso depende um pouco do tipo do cliente, mas o que a gente tem visto bastante é que a solução de segurança baseada em assinatura, que a gente conhece desde lá atrás, é uma solução bastante reativa. Praticamente todo cliente tem, mas ela acaba não sendo suficiente e aí a gente encontra alguns outros gaps. Por exemplo, eu preciso migrar alguma coisa para um datacenter novo e esse datacenter novo tem conexões de alta velocidade, só que eu não tenho soluções de segurança prontas para essa conexão de alta velocidade.

IH – Que problemas de segurança são mais frequentes nas grandes corporações?

Bruno – Em geral é a falta de integração de políticas. Pensando em tecnologia, é muito frquente encontrar empresas que compram milhares de dólares em produtos e só por isso têm uma falsa sensação de segurança. Às vezes é pior, porque na hora em que acontece o problema, alguém vai perguntar: mas você não investiu tanto nessa solução? Investiu, mas a solução não estava bem configurada ou simplesmente não funciona direito.

André – Segurança na Dupont faz parte do DNA da empresa: uma das coisas que a empresa vende é consultoria em segurança, porque ela nasceu na área de explosivos, e tinha que ter muita segurança no processo de produção. Então, ser segura é um business para a empresa. Consequentemente, a empresa coloca grande prioridade na segurança da informação, porque as duas caminham juntas. Acho que o grande dilema é atender a agilidade do negócio e ao mesmo tempo manter a informação segura. Uma das coisas que a gente tem implementado é o chamado need to know, ou seja, quem precisa saber daquela informação. Aí você começa a estratificar o que é informação pública, o que é privada e o que são as joias da coroa. Recentemente, enviamos mensagem a todos os usuários dizendo assim: “Na dúvida, não clique”. E muita gente clicou. É um bom teste. Nós temos uma política que a gente chama de record information management. É o seguinte: você precisa guardar informação, mas também não deve guardar informação. Quando se fala em acesso ao Facebook e outras redes sociais, acho que não se deve passar a responsabilidade para a TI: a responsabilidade é da linha de gerenciamento. Quem gerencia o funcionário é seu líder, não é o computador. Se o líder definiu com ele quais são os objetivos que ele tem que cumprir, não importa se ele ficou no Facebook.

IH – Você está falando em produtividade: se o funcionário entrega, não importa o tempo que ele vai dedicar a outras atividades.

André – Exatamente. Uma norma de segurança que a gente implementou recentemente é a seguinte: os e-mails, os pen drives, aquilo que você grava ou manda para um endereço de Internet, tudo é capturado mundialmente para ter rastreabilidade depois. Nós temos também uma política segundo a qual, se um funcionário vai embora, eu não posso abrir o e-mail dele: eu tenho que relatar num formulário mundial, onde coloco quais os motivos pelos quais eu quero ver aquele e-mail; esse formulário passa pelo RH e pelo jurídico mundialmente, até que eu obtenha autorização para abrir aquele e-mail. Nós também usamos muito a infraestrutura dos provedores externos, na casa deles. Se me perguntam se é seguro, costumo responder que, no Brasil, tenho que

fazer coisas como o Sped fiscal, e mandar toda a minha contabilidade, em detalhes, para o governo. Será que o governo controla essas informações direitinho? Toda a nossa força de vendas da área agrícola é terceirizada. Então nós fizemos um contrato de segurança com os terceiros, mas aí há uma dificuldade, porque eles usam os equipamentos deles. Estamos usando muito a mobilidade, especialmente na área agrícola. O pessoal do campo está superinformatizado, então eu preciso dar agilidade na ponta. E aí vem o desafio de oferecer mobilidade de forma segura. Eu não sei se os especialistas em segurança vão concordar comigo, mas quando você implementa camadas de segurança, o que acontece com a sua performance? Ela cai, porque passa por ali, passa por aqui e quando chega a resposta para o cliente, lá na frente, é tarde demais. Esse foi um dos motivos de ter ido para a nuvem com o CRM da Dupont. Mas nem tudo dá para colocar na nuvem.

IH – O que, por exemplo, não dá para colocar?

André – ERP transacional você não coloca na nuvem.

Alberto – Eu tenho umas convicções de gestão. A primeira delas é que sou absolutamente avesso à imposição de limites individuais. Desde o início, 15 anos atrás, todas as pessoas que trabalham na Bull têm total liberdade de acesso a Internet, sem nenhuma restrição. Costumo citar um caso muito simples: o funcionário que acessa sites pornográficos. Se ele acessa um site pornográfico durante o dia, o problema não é de segurança, é um problema psicológico, é um problema de gestão. Por que eu vou esconder esse problema? Isso é a essência de como nós vemos segurança, mas me custou várias discussões com o pessoal de informática, que até hoje tenta bloquear acesso a sites dentro da Bull. Eu consegui resistir a essas tentações com bons argumentos. A minha visão é muito mais técnica: não adianta investir em segurança, se você não sabe o que tem na própria empresa. Um exemplo clássico é você criar todo tipo de firewall, de barreiras, zonas desmilitarizadas, etc. De noite entra o pessoal da faxina para limpar o datacenter e faz a festa. Como 99,99% do pessoal da limpeza só faz limpeza mesmo, não é tão evidente o problema de segurança, o vazamento. Então é preciso usar uma metodologia para modelagem de segurança. Minha primeira recomendação como fornecedor sobre como tratar segurança é que se faça uma abordagem estruturada, lembrando sempre que segurança não é produto, é projeto. Não basta implementar, tem que gerenciar. É incremental, envolve cultura. Você não implementa segurança sem cultura, tem que mudar o comportamento das pessoas para a segurança. Na Bull, nós mexemos com projetos extremamente sensíveis de clientes. Todos os nossos chefes de projeto e consultores carregam informações extremamente confidenciais: um notebook perdido é uma fonte de informação brutal. Então nós impomos a criptografia como um comportamento de base, mas não basta criptografia, você precisa ter backup do que está ali dentro. E backup é cultura. Você tem que ter todo um ecossistema de segurança, que tem que estar interligado para que funcione. Eu parto do meu próprio exemplo: ando com criptografia em tudo e faço backups criptografados. Eu tenho uma nuvem interna que estoca tudo que tenho no meu notebook. Faço esses backups cada vez que me logo, remotamente ou dentro da companhia. E nós podemos falar de criptografia software e de criptografia hardware. A criptografia hardware vai tomar um lugar mais importante dentro das redes. A criptografia hardware hoje é um fator de bloqueio, um fator de atraso nos sistemas e na performance. Isso vai ser resolvido, vai ter que se resolvido e nós estamos falando de vários tipos de tecnologia hardware. Eu não sei se todos conhecem, mas existe um site na Internet, bem didático, que explica como copiar senhas. Você usa nitrogênio, congela o teclado do PC, congela a memória e copia a senha que foi digitada. Enfim, tenho uma visão que pode ser polêmica, mas acho que os departamentos de TI das organizações estão com os dias contados: vão virar departamentos de segurança em rede. As áreas usuárias vão começar a mexer com aplicação, vamos ser uma área de suporte a essas áreas usuárias, porque na verdade o principal problema das organizações é segurança em rede. Acho que a metodologia e as abordagens estruturadas de projetos de segurança vão ser um ponto chave para o sucesso das implementações. É extremamente difícil, porque exige disciplina. Eu estou tentando estabelecer como norma os backups automatizados, a criptografia automatizada. Não vai ser opção, mas obrigação.

.

> “Você cria todo tipo de firewall, de barreiras, zonas desmilitarizadas, etc. De noite entra o pessoal da faxina para limpar o datacenter e faz a festa”.
>
> Alberto, da Bull

mesa-redonda

fotos hamilton pena

“A norma existe, mas o usuário às vezes acha que a informação é importante e quer manter na base, mesmo já expirado o período estabelecido”.

Vanderlei, da EDP

IH – Uma questão pouco abordada nesse tipo de discussão é a do descarte das informações dentro das empresas. Vocês têm uma política definida para a última etapa do ciclo de vida das informações? E como compatibilizam essa política com as exigências legais de guarda de documentos e informações

André – A Dupont tem essa política implementada, o jurídico está totalmente alinhado com a política, inclusive estabelece algumas normas. Até mesmo reter um registro sem necessidade é um problema. Nós, como muitas outras empresas, enfrentamos o dilema do Sox, porque Sox é “show me the data, show me the evidence”. Muita gente passou a guardar e-mail para mostrar que tal pessoa aprovou que se fizesse determinada coisa. Aí surgiu a discussão sobre qual é o período ideal para se guardar e-mails. Dentro do próprio e-mail a gente passou a falar: esta informação precisa ficar guardada por cinco anos. Quando chega perto da expiração do prazo, o e-mail volta para que se tome a decisão de deletar ou não. Com essa política, a gente resolveu a questão cultural de ninguém se preocupar em olhar isso.

Claudia – A GE tem uma política de classificação da informação, se aquela informação é aberta ou confidencial, restrita ou classificada. E cada tipo de informação tem um tempo para ser guardada. Cada funcionário assina um termo em que se responsabiliza por aquele tipo de informação e vai guardar somente por aquele tempo.

Vanderlei – Antes da TI, eu passei pelo planejamento tributário, pela contabilidade e pelo planejamento estratégico. Nessas áreas a gente tratou muito da classificação documental e estabeleceu os prazos pelos quais deve ser guardado cada tipo de documento. A norma existe, mas o usuário às vezes acha que a informação é importante e quer manter na base, mesmo já expirado o período estabelecido. É difícil de executar, porque aquela informação sempre é importante. Acho que vou ter que montar uma estrutura para fazer esse arquivamento, porque ninguém descarta nada.

Rodolfo – A Comgás também tem o DNA de segurança, até porque, se não tiver, o nosso produto explode e mata. Então, toda reunião na empresa tem o momento da segurança. A gente tem uma política para a questão do descarte das informações estruturadas que fazem parte dos sistemas corporativos, financeiro, de RH. Mas tem uma massa enorme de dados não estruturados, de e-mails, de arquivos, que, por mais esforço que a gente tenha feito para convencer as pessoas a limpar, ninguém aperta o delete: há sempre a preocupação de perder alguma coisa importante.

IH – E vocês, fornecedores, identificam nos clientes essa preocupação com o descarte das informações?

Carraretto – Quando a parte regulatória é clara, acaba sendo mais fácil, porque é só seguir a lei. Agora, o dado sobre o qual não existe uma regulamentação clara, esse vai parar sempre na caixa “para sempre”. É aí que tem que entrar a questão da conscientização: é preciso explicar para ele que tem custo para a empresa manter aquela informação que não tem mais utilidade. Enquanto essa etapa não for cumprida, a melhor solução é fazer um armazenamento inteligente da informação, eliminar redundância, guardar uma cópia, comprimir, enfim usar todas essas tecnologias que hoje existem para você fazer uma armazenagem mais eficiente.

Bruno – De fato, quando existe regulamentação, as coisas ficam muito mais fáceis. Quando não existe, já vi até casos de clientes que usam a criptografia antes de destruir o disco. Se alguém conseguir refazer a trilha de um disco, vai remontar o dado criptografado, aí não vai ter a chave, consequentemente não vai conseguir ler. Mas acredito que o descarte de dados sempre vai depender da cultura da empresa.

Alberto – Acho que não se consegue fazer descarte de dados por obrigação. O sujeito que tem obsessão por guardar dado vai guardar o dado num HD externo na casa dele ou na gaveta dele, e talvez isso seja mais arriscado do que manter uma cópia dentro da estrutura central. Então a minha convicção é na educação, é formar o funcionário para que ele descarte e tenha responsabilidade pelo dado corporativo. Outro elemento importante nessa questão é o custo da pessoa: uma hora de um diretor tem um preço; se ele passar meio dia organizando os dados dele, prefiro dar um disco para ele copiar tudo, sai muito mais barato. Se o disco está protegido, não há problema em que ele guarde o dado.