Gestão de redes: como manter a segurança e abrir espaço para a inovação?

O desafio de fazer uma boa gestão da infraestrutura das redes corporativas é o tema desta mesa-redonda, coordenada pelo diretor de redação do Informática Hoje, Wilson Moherdaui, e da qual participaram **André** Martins, diretor de infraestrutura de TI da Serasa Experian; **Helton** Moreno, responsável por infraestrutura e sistemas da Assurant; **Ivan** Barale, gerente de operações da Porto Seguro; **Luiz Gustavo** Lins de Figueiredo, diretor de TI da Aon; **Marcelo** Maylinch Simão, superintendente de infraestrutura, arquitetura corporativa e serviços de TI da Alelo; **Márcio** Roberto da Silva, superintendente de tecnologia e serviços da Cetip; **Rodrigo** Gassi, responsável por infraestrutura e rede da América Latina da Zurich; e **Waldemar** Ruggiero Jr., diretor do departamento de processamento e comunicação de dados do Bradesco.

Informática Hoje – No caso da Porto Seguro, além de todas as pressões a que vocês estão submetidos, existem algumas especificidades, por se tratar de um conglomerado de empresas, todas com uma ênfase muito forte em mobilidade. Entre essas empresas está a Conecta, uma operadora virtual voltada aos clientes da Porto Seguro, o que deve provocar um impacto ainda maior do que a média, porque acaba sendo um fornecedor de infraestrutura para os clientes. Não é isso, Ivan?

Ivan – É verdade. A Conecta é uma empresa de telefonia virtual que utiliza o transporte da Tim. Ela atua dentro da Porto Seguro como um fornecedor e tem o desafio de ser tão competitiva quanto as empresas que hoje nos prestam serviço. O recente desafio de custos obviamente traz um ingrediente extra, um tempero adicional a tudo isso. A Porto Seguro tem um conglomerado de 28 empresas, que atuam de forma vertical, então não tem uma infraestrutura em que os processos são compartilhados entre todas as empresas. Cada diretoria geral que cuida desse conjunto de empresas tem independência de atuação, como se fosse um incentivo a empreendedorismo, e a Conecta também se encaixa nessa questão, tanto que agora eles estão concorrendo junto com outras operadoras para poder nos fornecer os links de comunicação. Então, obviamente a gente tem discussões dentro de casa, mas com a convicção de que ela vai ter que ser tão eficiente quanto em custo, performance e gerenciamento, outro grande desafio. A gente tem trabalhado nesse último ano principalmente com muitas iniciativas para reduzir custo, sem perder a capacidade de oferecer uma boa experiência de mobilidade, que é o que as pessoas estão querendo. Não adianta o funcionário estar em home office, o corretor usando um app da Porto ou um espaço de sucursal precisando de um serviço da empresa, se ele não tiver uma boa performance: ele se torna caro, independente de quanto está se pagando a ele. Hoje as pessoas não querem uma experiência diferente dependendo de onde estiverem, então o desafio é manter essa performance adequada, com disponibilidade e um custo equilibrado.

IH – Você falou que são 28 empresas que atuam verticalmente. O que significa isso do ponto de vista da gestão da infraestrutura de rede?

Ivan – A área de que eu cuido, operações, atende todas as 28 empresas,

atalho

As redes corporativas são submetidas a pressões constantes e cada vez maiores dos próprios negócios – pressões internas, da estrutura das próprias empresas, e pressões externas, da demanda dos negócios. E a cada dia mais essas redes são sobrecarregadas com novos agentes externos, com a sobrecarga brutal provocada pelas redes sociais e pelo que se convencionou chamar de Big Data. Um dos grandes desafios dos gestores das redes é evitar que a infraestrutura se torne um gargalo para a inovação

com algumas exceções, dependendo da dimensão. Mas o que traz para nós um desafio adicional é o fato de as estratégias nem sempre serem convergentes, ou seja, cada negócio tem um desafio diferente, de acordo com o cenário ou o momento do negócio. Nós temos procurado segmentar a equipe de forma a se especializar em alguns segmentos do negócio, em algumas necessidades, até porque o orçamento de cada negócio é diferente. Há empresas que ainda estão funcionando como startups, que ainda não estão totalmente integradas ou que ainda não conseguem girar por conta própria. Isso significa que a gente precisa se aproximar cada vez mais das empresas e dos negócios específicos. Embora cuide de infraestrutura, tenho participado de algumas conversas com o pessoal de negócio, para poder entender um pouco mais o desafio e as necessidades deles.

IH – E você consegue algum grau de automatização da gestão da rede em função dessas diferentes demandas e desses diferentes perfis das empresas?

Ivan – A gente consegue, sim. Apesar desse perfil diferente, em uma parte dessa rede você consegue introduzir automatização até como um diferencial para poder ser competitivo. No custeio, fica o desafio de que cada um pague só por aquela fatia do que ele usa no nosso gerenciamento. A gente tem buscado algumas soluções de mercado com empresas não tão maduras ainda, mas que têm ideias e produtos promissores. A gente tem buscado muita alternativa de provisionamento como software, tanto de rede quanto de servidores e de storage. Então, há uma camada única, para poder provisionar isso como software e poder ser mais competitivo para todos.

IH – Você pode nos contar quais são os problemas mais sérios que vocês têm tido que enfrentar?

Ivan – Acho que o grande desafio que a gente tem enfrentado é o papel consultivo da TI. O negócio hoje tem acesso a muita informação, aos próprios fornecedores, que muitas vezes vão conhecer os diretores e a gente tem sido constantemente desafiado pelo negócio a uma postura muito mais consultiva. Hoje qualquer indisponibilidade na rede tem um grau de estrago muito grande. Essa abrangência, dada a convergência das coisas, depende do que está na rede. Rede decididamente é um assunto que tira o nosso sono. Se o meu backbone central para, todos os negócios da empresa são afetados, não tem jeito. Então é um assunto que está em constante discussão e são discussões de alta temperatura sobre como a gente vai lidar com isso. Os investimentos não são baixos para poder fazer o acompanhamento de tudo isso que está convergindo: é muito streaming de vídeo, rede social, mensagens de texto, mensagens de Whatsapp, com imagens, com vídeos. Já tem 1.500 pessoas em home office e vamos chegar a 3 mil pessoas, e quem está em home office quer a mesma experiência de quem está na empresa. Então a gente tem enfrentado alguns problemas para entender o que acontece na casa do funcionário. A voz está embarcada também num aplicativo, é um softphone. Então, a experiência no Wi-Fi na casa dele tem que ser limpa e tem uma série de regras para que não haja interferência de qualquer outro elemento dentro da casa. É um tremendo desafio, porque, com a Internet das Coisas, a televisão é smart, a torradeira é smart, a geladeira é smart. Da borda para dentro da Porto, tudo bem. Mas da borda para fora, por mais que a gente tente e faça coisas pontuais, não consegue ser tão proativo como gostaria. Esse é o grande desafio.

Marcio – Você tem SLAs definidos para todos os serviços ou é tudo 100%? Se tem alguma parada, ela é entendida?

Ivan – Nós temos acordos internos com os negócios. É tudo colocado numa cesta: hoje temos 72 aplicações ou produtos que têm um SLA definido, que estão nessa cesta e a gente mede como um índice de disponibilidade da Porto Seguro. Mensalmente ou a cada bimestre é levado ao CTI, que é o conselho de tecnologia, e é apresentado para a empresa. Essa medida é feita com base no downtime, de acordo com a severidade de um incidente que parou aquele ambiente, aquele produto ou aquele segmento de negócio num horário útil, também previamente estabelecido nesse SLA. Eu tenho a conta direta do downtime. Quando é uma indisponibilidade total – parou o serviço de orçamento de automóvel, ninguém orça, cada hora de downtime é debitada. Se ele está degradado, é três para uma, ou seja, cada três horas debita uma hora do downtime. Nós temos uma reunião semanal, que a gente chama de "reza da TI" [*risos*]. Nessa reunião, nós vamos prestar contas para a diretoria, dizendo o que aconteceu e o que está sendo feito para que isso não ocorra novamente. E somos muito intolerantes quando não se sabe exatamente o que aconteceu, mais até do que a falha em si.

fotos hamilton pena

"Antigamente, muito do nosso ambiente crítico estava dentro do nosso datacenter, dentro de casa, e agora não está mais".

Marcelo, da Alelo

"Embora cuide de infraestrutura, tenho participado de algumas conversas com o pessoal de negócio, para poder entender um pouco mais o desafio e as necessidades deles".

Ivan, da Porto Seguro

fotos hamilton pena

> “A gente normalmente relata um incidente quando a redundância não funciona. Mas a gente passou a relatar os incidentes quando a redundância funciona”.
>
> Waldemar, do Bradesco

Marcelo – A gente trabalha muito com a questão do que é o ambiente crítico para o nosso negócio. Na Alelo, autorização é uma questão crítica. Ter o pessoal do atendimento, no ambiente dele, é crítico para o negócio e precisamos ter a robustez necessária. Quando alguns elementos que garantem a robustez não estão dentro da nossa casa, mas dentro da casa do colaborador, isso traz um desafio diferente. Antigamente, muito do nosso ambiente crítico estava dentro do nosso datacenter, dentro de casa, e agora não está mais. Então acho que o grande desafio é como você passa essa realidade do ambiente crítico de negócio além das nossas fronteiras e você gestiona isso para ter a disponibilidade que o negócio precisa.

André – Outro ponto que se soma a isso é que as regras têm que ficar mais flexíveis. A gente veio por anos com um ambiente muito rígido, onde havia uma separação clara do que era corporativo e do que era a vida privada. Essas coisas hoje não têm limites definidos, é difícil falar onde começa a vida privada e onde começa a vida profissional. Ele tem uma experiência em casa, por exemplo, com o Netflix, que funciona, então como falar que a banda larga dele tem um problema se ele consegue ver filmes em streaming sem problema? Então como é que a VPN dele não funciona e ele tem problema com voz? É difícil conseguir explicar esse tipo de coisa. Isso faz também com que o nosso pessoal tenha que estar preparado para outro tipo de suporte, vai ter que entender o lado do cliente, entender o que a pessoa está usando na casa dela e que tipo de infraestrutura tem ali. Antigamente, a gente podia dizer que isso não era problema nosso. Os investimentos necessários para manter a segurança de antes, quando era tudo controlado, passam a ser muito maiores e mais complexos. Talvez um dos maiores desafios seja tentar manter esses ambientes com alguma separação pelo menos lógica ou em termos de custo, onde você consegue explicar o que está sendo feito. Caso contrário, o grau de expectativa que existe dos colaboradores não é atendido.

Waldemar – Hoje a rede está muito em pé de igualdade com a segurança e com o aumento da área de compliance: são duas coisas que tiram efetivamente o sono, porque a gente tem que manter uma preocupação excessiva com essa questão da segurança, para manter a disponibilidade. Você fica muito vulnerável pela área de contato existente. Periodicamente, a rede é um pouco menos exigente quanto à atualização, comparada com a segurança, mas acho que são dois temas que fazem qualquer instituição ter um aporte financeiro grande e uma preocupação grande com a cultura dos funcionários. A gente sabe que a cultura dos funcionários, não só da TI, mas de fora da TI, tem contribuído muito para deixar os sistemas mais vulneráveis.

Helton – Hoje, as pessoas têm em casa equipamentos muito melhores do que os que têm na empresa. O sujeito tem um notebook em casa, aperta um botão e em menos de um minuto está trabalhando. Já quando liga o laptop dele da empresa, passam cinco minutos e não deu o login ainda. Ele dá o login e, até subir tudo que tem que subir, ele fala: “Como é que eu vou trabalhar nisso?”.

Luiz Gustavo – Hoje a Aon tem 1.200 funcionários, tem oito escritórios espalhados pelo Brasil. Então, qualquer estratégia que eu vá fazer para otimizar a rede, para garantir segurança e estabilidade, tem que passar por premissas básicas, que hoje são bem complexas de justificar. Por exemplo, o custo de um link para eu poder ter alta velocidade, performance e ainda redundância é muito alto, é difícil justificar para o board. Se preciso fazer upgrade nos computadores da empresa, o sujeito tem uma experiência de casa e vai dizer: “Eu compro um notebook melhor e mais barato no varejo”. Mas os notebooks que eu tenho que comprar por causa de chipset, por causa de compliance com segurança e com as diretrizes corporativas custam muito mais. Então esse é o grande desafio: conseguir mostrar o valor do investimento.

Ivan – Segurança hoje é um guarda-chuva, não é mais uma ou outra solução. Quando a gente fala em rede, eu tenho que manter minhas vulnerabilidades conhecidas, mitigadas ou resolvidas. Então a segurança é um assunto corporativo, não mais um assunto de TI, tem o comportamento de quem usa, a conscientização e a questão do equilíbrio, porque o negócio quer agilidade e velocidade. Então é um tema muito mais voltado para monitorar o comportamento, verificar os desvios e tentar atuar, porque hoje a gente não consegue mais olhar tudo. O profissional de segurança da informação tem que ser muito completo, muito antenado. O futuro é cada vez mais wireless nas empresas. Fizemos um prédio, o primeiro da América Latina, 100% wireless, um prédio que usa 5G e não tem cabo para nada, nem para telefone, nem para impressora, é totalmente wireless, e é claro que se tornou um desafio de segurança. A gente acabou quebrando um paradigma: hoje o nosso prédio mais seguro é justamente esse. É mais seguro que a rede cabeada, inclusive contra interferência. Caso ocorra uma interferência, as antenas identificam e fazem uma contramedida automaticamente.

IH – Os elementos d a rede têm a capacidade de informar automaticamente a vocês quando não estão adequados à política de segurança das empresas? Isso poderia tirar um peso tremendo das costas de vocês.

Waldemar – A gente adotou uma estratégia de arquitetura que, infelizmente, é um pouco mais cara, mas precisou ser adotada pelo tamanho e pela dimensão que o banco tem. A gente acabou segregando algumas áreas, a Internet pessoa física, a Internet pessoa jurídica e os acessos corporativos. Todas são completamente independentes. Os acessos às empresas externas que são parceiras e às empresas de desenvolvimento também são independentes. Você consegue ter uma reação tanto na questão de disponibilidade quanto na questão de SLAs e de segurança mais adequada. Cada uma dessas torres tem níveis de atualização tecnológica um pouco diferentes, porque elas não foram feitas todas ao mesmo tempo: as mais atuais têm equipamentos que permitem identificar de forma automática determinados tipos de acesso e fazer determinadas mitigações, desde a do DoS, até os ataques mais intencionais de invasão mesmo, que precisam ser olhados de uma forma que varia em todas as camadas do protocolo. Aí é onde mora o maior perigo, é um tipo de desafio de segurança que esteja numa camada mais superior, onde fica mais complexo você identificar. As informações chegam criptografadas. Como é que você faz para analisar se dentro dessas informações criptografadas tem alguma impureza ou não?

IH – Acaba sendo uma faca de dois gumes.

Waldemar – Você tem que abrir para olhar e na hora em que você abre, perde também. Trabalhando em camadas, a gente acaba conseguindo ser satisfatório nessas questões. A gente não pode falar que a segurança é 100%, nunca vai ser, mas você tem que perseguir dia a dia e evoluir principalmente na questão de preparação da equipe. A gente fala muito em processos, fala muito em atualização tecnológica, não só atualização de versões, mas ter equipamentos up-to-date. Mas o trabalho de formação de equipe é um trabalho longo e determinado. Nós no banco temos a felicidade de ter a Fundação Bradesco, que tem uma grande formação tecnológica, onde a gente pega os meninos desde o começo de carreira e faz essa formação com programas de trainee, incentivando a fazer os melhores cursos nas melhores escolas, para que a gente tenha uma estrutura tecnológica muito bem embasada. É um ponto de extrema relevância.

Helton – Existem hoje equipamentos que conseguem identificar numa rede wireless qual é o sistema operacional, que versão ele está usando, se é de um funcionário ou não. O que eu preciso fazer para chegar nisso? Preciso investir no parque tecnológico. Mas não dá para fazer isso de uma vez, então eu consigo dar essa solução no prédio administrativo, na torre 1 ou na torre 2, mas não dá para abranger tudo num primeiro momento. Por outro lado, existe um protocolo na rede, que se chama SNMP, pelo qual você consegue vasculhar tudo que acontece dentro da sua rede, e existem empresas que têm soluções para ler esse protocolo e ajudar você a tomar algumas decisões. Mas em geral começa a vir uma enxurrada de alertas e uma enxurrada de alertas não alerta nada, porque você não consegue olhar. Aí entramos no tema da capacitação: quantas pessoas capacitadas eu preciso ter para definir e priorizar os diferentes alertas e até onde elas conseguem chegar? Acho que tudo começa por uma política bem definida e aprovada pela corporação como um todo, de que algumas coisas têm que ser respeitadas, como, por exemplo, a vida útil de um equipamento. Às vezes dá dó trocar um equipamento de dois ou três anos, porque está na política e ele ainda está bom, mas a nova tecnologia está chegando. Se eu não começar a trocar agora, não consigo completar o ciclo para daqui um ou dois anos e implementar uma solução nova. Quando se fala em rede, tudo é complicado. As operadoras não entregam um bom serviço e a gente fica refém, pagando valores absurdos para ter redundância e às vezes não tem redundância nenhuma.

Luiz Gustavo – De fato, como você vai conseguir provar que tem que trocar um equipamento que ninguém vê, está lá escondido no datacenter, se o board está preocupado com receita? Você tem que dizer: se não trocar esse equipamento, vai ter um ataque de hacker. O pessoal do board vai dizer: a gente nunca passou por isso, por que vai passar agora, por que eu vou investir milhões agora em equipamento, se eu posso colocar esse dinheiro na área comercial para vender mais? A infraestrutura de TI é encarada como se fosse saneamento básico, está lá embaixo, ninguém vê, só vai ver quando explodir alguma coisa. A segurança corporativa é infinitamente mais cara do que a experiência que o usuário tem em casa. Esse é o desafio principal: como é que você prova?

> “O custo de um link para eu poder ter alta velocidade, performance e ainda redundância é muito alto, é difícil justificar para o board”.
>
> Luiz Gustavo, da Aon

IH – Para quem trabalha num banco deveria ser fácil.

Luiz Gustavo – Mas banco já tem essa cultura, vê essa inovação tecnológica há mais de 20 anos. O varejo está começando agora. O mundo de seguros está engatinhando.

Ivan – Acho importante aqui contarmos um pouco do que

mesa-redonda

fotos hamilton pena

“A gente só consegue automatizar se tem uma padronização de processos e de equipamentos”.

Helton, da Assurant

estamos fazendo, até para poder trocar experiências. A minha pergunta para o Helton é: qual é a política de troca de equipamentos vigente na sua empresa? Porque, no meu ponto de vista, isso não vai mudar, muito ao contrário. Esse é o nosso desafio. Eu tenho lá 3 mil equipamentos com seis anos de uso, que estão performando, e eu tenho que fazer uma gestão de vulnerabilidade muito mais forte. Isso não vai mudar. Não vai chegar o board agora dizendo que acabou a crise vamos trocar equipamento todo ano. Isso não tem volta.

Helton – Nós temos a política de troca a cada três anos e buscamos parceiros que oferecem tecnologia embarcada no software e não no hardware. Então a gente consegue implementar novas features sem trocar hardware. Com relação a equipamentos de usuários, a cada três anos a gente faz um leasing, troca de todo mundo.

Waldemar – Na linha do que o Ivan colocou, de compartilhar as melhores práticas, uma das coisas que a gente notou lá é como você convence o pessoal a investir mais, por exemplo, em redundância. A gente normalmente relata um incidente quando a redundância não funciona. Mas a gente passou a relatar os incidentes quando a redundância funciona. Na área de infraestrutura como um todo, que tem 2 mil funcionários, a gente reúne aproximadamente 110 pessoas todo dia, das 8h às 8h15, para compartilhar os incidentes e as ações que precisam ser tomadas imediatamente. E é relatado aquilo em que a redundância funcionou, ou seja, que não salvou, um cluster ou um link de comunicação e assim por diante. Semanalmente a gente relata para a diretoria executiva e para o conselho do banco as principais mudanças de sistema e as principais ocorrências, levando em conta também aquilo que não salvou. Isso dá uma agenda mais positiva para que a gente não seja visto só como o gastão da turma.

IH – Existe alguma incidência que seja mais recorrente, que você possa nos contar?

Waldemar – Existe. Como temos a rede distribuída pelo país todo, pelo tempo de convergência dessa rede, é cada vez mais difícil identificar o momento em que houve a falha no link. E nem sempre a aplicação está preparada para reconhecer que está havendo uma falha. Então, se na última milha aconteceu uma falha e o resto do link está todo ativo, nem sempre se percebe que está fora do ar e começa a dar erro na aplicação. O que a gente fez para melhorar isso foi uma monitoração de negócio mais pontual nos links mais críticos – não dá para ter em todos –, e aí dá para perceber um erro numa camada superior do protocolo e ter uma atuação.

IH – Mas esse monitoramento é automático?

Waldemar – Tem o monitoramento automático e tem o manual, nos links mais críticos.

André – Também em virtude da distribuição geográfica que a gente tem, o que acaba acontecendo é que um problema para o comercial é só um problema. Dois já viram uma crise. Quando você tem milhões de pontos, acaba tendo o caos praticamente todos os dias. A medição interna acaba dando uma noção inexata do que acontece, a percepção era de que estava tudo bem, o problema era que você não sabia o quanto tinha morrido na ponta e não tinha chegado a você. Foi aí que a gente começou a perceber que tinha que ter uma medição partindo da ponta. Você pode fazer curvas que demonstram que está abaixo do que deveria estar e a partir daí trazer alarmes. O que a gente começou a perceber, no caso específico de outra empresa, foi que tinha uma monitoração muito melhor do que as operadoras, especialmente de GPRS. Eu conseguia dizer para a operadora quando tinha um problema antes mesmo de ela perceber. Mas isso não vem de uma hora para outra. Primeiro tivemos que romper com aquela história de dizer que está tudo bem, porque final a gente estava medindo com a régua errada. É preciso sair para o outro lado do balcão e medir com o ponto de vista do cliente. Primeiro pensamos que medir 2 milhões de pontos seria impossível. Então a gente colocou inteligência na nossa aplicação: ela comunica o que aconteceu e você recebe uma base de dados. A gente também começou a usar o Big Data, na verdade um grande datawarehouse para infraestrutura. Além disso, é preciso fazer um trabalho grande com as operadoras. Temos uma série de reguladores que nem sempre regulam do jeito que a gente gostaria: para a Anatel, 95% é um índice bom, para a gente não é. O acordo de parceria entre as operadoras faz com que elas compartilhem infraestruturas, o que causa problemas que a gente não descobre. Quando a gente olha todo esse cenário, começa a medir a partir de outra ponta, entendendo que segurança é por camadas e tem que começar por desenho. Esse é um dos problemas que a gente tem hoje: os nossos sistemas legados não eram acessados de fora, mas de dentro, então tinham uma camada de proteção. O mundo não é amais ssim: ou você desenha pensando em segurança ou tem que colocar todas as camadas. Além disso, as formas de ataques também estão ficando mais inteligentes.

IH – Mas é possível criar uma camada de aplicação única para estabelecer essas políticas de segurança?

André – Única, não. Talvez essa seja a nossa maior falha. Toda vez que a gente procura uma bala de prata, a gente falha. Eu acho que as

soluções são de nicho, para cada problema talvez você tenha que se aproximar com as experiências do passado, mas ao mesmo tempo tem que tomar cuidado para evitar trazer todo o seu preconceito.

Marcelo – Uma coisa importante é sair um pouco da caixinha de infraestrutura. O Waldemar falou que às vezes a gente percebe o problema quando está lá no nível da monitoração de negócio. Isso tem um apelo muito grande dentro das nossas empresas, tem tido um impacto no negócio agora e no final do dia a gente percebe que tem uma questão de infraestrutura. Segurança talvez seja um dos temas que derrubam executivo de tecnologia mais rápido. Então, é preciso fazer uma abordagem mais ampla, que vai além de infraestrutura. É preciso chegar ao desenho da solução, à questão das aplicações, olhar a TI como um todo; isso nos ajuda a evoluir. Não adianta ter a infraestrutura mais segura do mundo se no final do dia a aplicação que roda sobre ela tem um monte de gaps.

IH – Ou seja, você não pode ter um olhar apurado para a infraestrutura se não tiver a dimensão do negócio para fazer a adequação. É isso?

Marcelo – Exatamente.

Helton – Acho importante lembrar que a gente só consegue automatizar se tem uma padronização de processos e de equipamentos. Então criam-se os perfis, o banco de software, e se associa ao usuário. Logo depois que ele se loga, todos os software a que ele tem direito são instalados na máquina dele. Com isso, você faz com que o seu pessoal se foque em incidentes, se foque em problemas, vá atender coisas mais pontuais. O ganho da automação é esse: você consegue usar melhor os recursos da sua estrutura.

Márcio – No segmento financeiro, grande parte das empresas é regulada, por isso nós temos a área de compliance, a área de segurança da informação e controles internos muito fortes. O que a gente tem feito diante de muitos problemas? Por exemplo, gerenciamento de rede. Hoje a gente tem acesso a roteadores das operadoras, até para conseguir saber se vai cair ou se caiu alguma coisa. O usuário traz equipamentos cada vez mais modernos, e a gente tem redes exclusivas para isso, até porque temos problemas de sinal de celular ali na região. Nós, da área de infraestrutura, somos muito cobrados para não ficar olhando para a infraestrutura: temos que estar preocupados com o negócio. No caso da Cetip, TI faz parte do negócio, faz parte da estratégia da empresa.

> “Quando você tem milhões de pontos, acaba tendo o caos praticamente todos os dias”.
>
> André, da Serasa Experian

Ivan – Márcio, o negócio também já está com essa percepção de que a TI é parceira dele?

Márcio – A TI participa de todos os projetos de desenvolvimento de produtos.

Ivan – O produto já vem embarcado na TI?

Márcio – Na hora em que vai nascer o produto, a TI está junto.

Ivan – Mas é uma característica de negócio com um produto tecnológico, um produto digital, vamos dizer assim.

Márcio – Exato. Tecnologia é a nossa fábrica.

IH – O Helton mencionou a necessidade de padronização na gestão do workplace. Isso é mais viável em empresas com foco numa única vertical. Deve ser impossível em grupos que têm mais de uma empresa, em várias verticais, não?

Luiz Gustavo – A gente está nesse caminho, de ter imagens padronizadas e o ganho é absurdo. Em 15 a nova máquina está pronta, porque tem a réplica. Mas aí também vem a contrapartida: quantas imagens e quantos padrões eu tenho que ter, porque a empresa não trocou todos os equipamentos? Um caminho interessante é a virtualização de aplicações. Ao invés de ter que padronizar todo o meu hardware, eu trabalho cada vez mais com as máquinas legadas, com os equipamentos velhos, para deixá-los como terminal burro. Então, é o caso de trocar esse equipamento para deixar o processamento dentro do datacenter, voltar para o antigo tempo do mainframe. O ganho é absurdo.

IH – Usando a nuvem?

Luiz Gustavo – Ainda não usamos muito nuvem, por causa da precariedade da infraestrutura. Por exemplo, como é que eu coloco todo o meu equipamento, todas as minhas aplicações, toda a minha empresa na nuvem hoje? A empresa é aqui no Itaim [*bairro de São Paulo*]; passa um caminhão, derruba um cabo de fibra ótica, e lá se foram a fibra e a redundância, e a empresa parou. Então eu tenho o datacenter, mas estou falando de tirar o processamento do meu client, do meu desktop, da minha mesa de escritório lá e levar para o datacenter. Aí eu consigo padronizar virtualmente. A nossa experiência tem sido muito boa.

Rodrigo – É muito comum hoje em dia ter virtualização de servidores e virtualização de aplicação. Uma nova tendência no mercado é a virtualização de rede. A infraestrutura de rede é uma atividade fixa e a virtualização roda sobre software. Quando você vai subir um novo servidor, uma nova estrutura,

fotos hamilton pena

“Nós, da área de infraestrutura, somos muito cobrados para não ficar olhando para a infraestrutura: temos que estar preocupados com o negócio”.

Marcio, da Cetip

isso tudo vai ser via software, junto com um novo servidor e uma nova aplicação. Ainda não vi cases nesse sentido, mas é uma nova tendência. A gente consultou sobre a possibilidade de fazer a monitoração dos links juntamente com a operadora, mas talvez falte confiança na operadora. Tem diversas ferramentas de monitoração para complementar a ausência de proatividade das operadoras. Em alguns países da América Latina, os links estão caindo com uma frequência muito grande. Às vezes você acha que tem redundância, mas na verdade não tem, mesmo isso estando em contrato. Neste momento, por exemplo, estou com o Chile quase totalmente indisponível, porque os dois links caíram ao mesmo tempo. E são links de operadoras diferentes, de pontos diferentes e com toda a redundância.

IH – O Ivan se referiu no início à dificuldade de gerir as restrições dos usuários nas diversas formas de acesso à rede. Vocês estabelecem essas restrições por nível hierárquico e isso funciona?

Ivan – A gente tem uma estratégia de rede sem fio, mas, independente de como ficará a rede, existem perfis. Tem uma rede visitante, para a qual tem o marco regulatório, que a gente tem que respeitar. Hoje não dá mais para você dar acesso livre, porque a pessoa pode fazer alguma ação maliciosa a partir do seu ambiente e você é responsabilizado por isso. Então, existe uma autorização e uma regulação, inclusive de tempo de uso: a banda é um pouco mais restrita e tem também um filtro de conteúdo. Para funcionários, não é por nível hierárquico, a gente tem algumas questões de conscientização. A Porto fomenta o BYOD [*bring your own device*] e o BYOA [*bring your own application*]: não permitimos só que tragam a máquina, mas a aplicação também, o aplicativo vem embarcado no smartphone, no iPad, seja lá em que dispositivo for. Eles usam a rede Wi-Fi para esses dispositivos, essa rede permite saber o que está sendo acessado, quem é, qual o tipo de device, e tem a questão do dimensionamento da rede que muda. Então, a questão de segurança é fundamental, mas também é importante o dimensionamento. Quando vai colocar uma rede Wi-Fi, a gente tem que fazer uma previsão de 2,5 dispositivos por funcionário, coisa que era impensável até pouco tempo atrás. A Porto faz um pouco de monitoramento do comportamento, monitoramento por camada. Faz gestão de vulnerabilidade de aplicação e de infraestruturas de redes. Uma empresa faz mensalmente todas as coletas e a gente vai fazendo constantes atualizações. Então a gente trabalha muito mais na linha da prevenção, mais do que da restrição, que existe, mas dentro de um limite. Você não traz um cara da geração millenium, saindo da faculdade, e diz para ele: “Esse aqui é o seu micro, essa é a sua mesa, esse é o seu telefone, pode trabalhar”.

Waldemar – Nessa questão da distribuição de direito de acesso em todos os níveis, a gente tem como ordem interna que o gestor da informação é o autorizante para dar direito de acesso ou não. A gente tem uma régua que é estabelecida tanto pela segurança corporativa, que é um par meu, quanto pela segurança lógica, que também fica comigo. A gente estabelece essa régua em comitês e isso vale para a corporação toda. A partir daí, os direitos são estabelecidos por cada um dos gestores. De tempos em tempos, a gente revê isso para verificar se não tem algo que está muito amplo na questão de acesso, no sentido de reduzir a quantidade de pessoas que têm direito de acesso a algumas informações. Acho que essa é uma política interessante, porque você consegue colocar a responsabilidade da segurança no gestor. Eu cito sempre o exemplo do nosso departamento de crédito: nas estações de trabalho desse pessoal, é proibido usar pendrive, em função da criticidade do serviço. Outros departamentos são mais abertos e a gente olha isso com uma severidade maior na questão de monitoração.

IH – A intervenção humana é mais forte.

Waldemar – Isso.

Ivan – Na Porto não é por hierarquia, é por perfil. O dono da informação é o homem que tem um programa que se chama PIS, Proteção da Informação Sensível, a identificação dos donos é pelo perfil também, para corresponsabilizá-los pelo uso da informação.

Helton – Nós implementamos BYOD na empresa em 2011 e a solução que nós demos foi a seguinte: com as operadoras, a gente só fechou o chip, então eu não tinha nenhum tipo de fidelização com a operadora, e com o funcionário existe um nível hierárquico e a partir de determinado nível ele tem cargo de confiança. A partir do momento em que ele tem o cargo de confiança, se ele tem o laptop, subentende-se que ele pode ser acionado a qualquer hora do dia e aí ele tem um subsídio para comprar um smartphone. A única coisa que a gente estabelece é que esse subsídio é dado de dois em dois anos e a gente define um modelo básico. Nós criamos uma camada de segurança dentro do aparelho, e em certas aplicações ele não consegue fazer muita coisa. O resto do que está no aparelho é dele. Com relação à rede, na Assurant funciona assim: a antena

wireless tem a capacidade de distribuir rede para diferentes públicos. A premissa é que todos os nossos sistemas fazem uso do protocolo do Single Sign-On para todo mundo. Todas as aplicações partem do pressuposto de que a pessoa logada já está autenticada. Então, a pessoa abre o laptop, e, se ela está com cabo vai pelo cabo, se ela desconecta o cabo ou tira do dock, em 40 segundos ele pega o sinal, não precisa entrar com login, ele já reconhece automaticamente, já está dentro da rede e funciona tudo com a mesma performance e experiência do cabo. Para visitantes ou para devices pessoais, o sinal é aberto, só se exige a senha da rede. A gente limita a quantidade de devices: algumas pessoas podem ter dois devices, o dela e de um visitante. A gente controla pelo tempo também: devices conhecidos são 30 dias, devices não conhecidos, aqueles eventuais, é um dia. O visitante é obrigado a ter alguém que o receba. Se alguém vai me visitar, eu sou obrigado a pôr a minha senha. O uso da Internet não é liberado 100%, passa por um filtro de conteúdo, passa por análise de tráfego. O elo mais fraco nessa corrente continua sendo as pessoas, é preciso muita conscientização, não adianta você colocar política, não adianta colocar travas.

IH – Uma questão recorrente é o impacto que as ineficiências de rede têm provocado nos processos de inovação dentro das empresas. Vocês conseguem medir ou avaliar esse impacto?

Waldemar – O impacto é significativo. O que a gente estabeleceu internamente é um SLA de resposta rápida, para tentar atender àquela necessidade. Isso vale não só para inovação, mas por exemplo, para a questão da nuvem. A gente teve que melhorar o nosso tempo de entrega de infraestrutura porque a nuvem bate à porta, oferecendo maior agilidade e melhor preço. Então, você precisa considerar e reagir a isso. Na questão de inovação, é a mesma coisa, você precisa estabelecer um processo que tenha um determinado fura-fila, sem atrapalhar aquilo que você precisa entregar. Nesse aspecto, o banco fez um trabalho muito interessante nos últimos dois anos, que, embora esteja um pouco fora da parte de rede, ajuda muito na infraestrutura: fizemos uma seleção das iniciativas corporativas que estavam sendo tomadas. O departamento de cartões ou a seguradora, por exemplo, às vezes se consideram mundos à parte. Só que existem necessidades de outras áreas também. Foi feito um projeto onde se mede a relação custo-benefício de cada uma das iniciativas de todas as áreas; os executivos sentam e estabelecem uma lista de prioridades. Isso fez com que a gente conseguisse atuar mais na padronização da infraestrutura, e aí se tem um tempo menor de atendimento e mais folga para atender às exceções dos projetos de inovação.

André – Tipicamente, alguém começava a inovação e aí nós éramos de alguma forma o gargalo ou o censor. Isso aconteceu algumas vezes e começou a dar certo na hora em que fomos tentar participar do processo de inovação, contar para eles quais são as regras que a gente tem e se ajudar. Não foi simples num primeiro momento, porque as visões eram bastante antagônicas, o que é normal. Acho que o time de infraestrutura tem a tendência de estar longe do negócio, diferente do de aplicações que está mais perto do dia a dia. O pessoal de rede é o que está até mais longe ainda. Por isso é preciso desenhar as coisas pensando em segurança de saída, não pode ser um acessório. Funcionou na maior parte das vezes, fizemos acordos, colocamos o modelo de monitoração, controle de budget, preparamos o time para isso.

Ivan – Acho que a questão da agilidade, de entregar quando precisa é só um pedaço. Tem o desafio das nuvens privada e pública, quando a gente fala no núcleo da corporação em si. A inovação por si só já preconiza experimentação e erro. Eu tenho que dar um espaço para que se consiga realmente experimentar, subir, cair, descer, enfrentar os problemas. A gente procura ter monitoração para todo mundo que está nas iniciativas: vai um mentor de cada uma das disciplinas, inclusive de segurança e o pessoal de rede, para dar um aconselhamento quando aquilo começa a ser acelerado. Eu não posso limitar a criatividade, afinal a gente criou um ambiente de desenvolvimento livre. Nesse ambiente de desenvolvimento livre, montamos uma infraestrutura virtual, em que as áreas podem criar os seus ambientes, só departamentais. Esse ambiente livre tem uma política e estão começando a consumir esse ambiente, criar máquinas virtuais, criar bancos de dados, buscar APIs, mas é tudo confinado no departamento. Então esse pessoal não consegue entrar na rede, não consegue fazer nenhum tipo de acesso. Pode ser que o que eles estão fazendo não vá dar em nada, mas eu monitoro para ver capacidade, para ver se não está tendo nenhum cracker, se não tem nada muito esquisito acontecendo ali. Se um dia quiser trazer para dentro da Porto Seguro, vai passar pelo analista de negócio que atende aquele departamento. Não somos gargalo, somos muito mais consultivos nesse aspecto e o desafio que eu tenho é provocar a equipe para ser inovadora.

“É muito comum hoje em dia ter virtualização de servidores e virtualização de aplicação. Uma nova tendência no mercado é a virtualização de rede”.

Rodrigo, da Zurich

JUNIPER NETWORKS

GRUPO BINÁRIO
Integração e Serviços

Build more than a network
Build the Future

A Juniper tem a solução de segurança SDSN (Software Defined Secure Networks) que oferece proteção por meio de todos os componentes de uma rede, indo muito além de firewalls e outros sistemas de prevenção de intrusos. É uma solução única no mercado.

Com automação, sistemas inteligentes e colaboração de diversas fontes na nuvem identifica, localiza e cataloga todas as ameaças e malwares, em tempo real e no mundo todo.

Tenha redes seguras e não mais segurança de rede.

Conheça as Soluções da Juniper Networks:

www.junipernetworks.com.br

www.binarionet.com.br

Tel.: (11) 3704-0480

SECURITY