Fórum IT Channel

Cibersegurança – das ameaças às oportunidades

No mercado da cibersegurança, as oportunidades de negócio para fabricantes, distribuidores e Parceiros crescem ao mesmo ritmo das ameaças. Na primeira Mesa Redonda dedicada ao tema, debatemos o panorama do cibercrime, a perceção de risco das empresas portuguesas e o papel dos Parceiros de Canal

Vania Penedo

Proteger a informação empresarial é uma das principais vicissitudes de um mundo povoado por dispositivos cada vez mais inteligentes e conetados. Os dados são o ativo mais valioso duma organização, independentemente do seu tamanho. Não é por isso de estranhar que os cibercriminosos procurem a forma mais eficaz, e criativa, de roubar esta informação, à medida que este se torna num dos negócios mais lucrativos do mundo.

A Gartner prevê que o mercado global de segurança cresça a um ritmo anual de 7.8% até 2019. Não é difícil perceber porquê: as ameaças continuam a evoluir a um ritmo veloz e os *hackers* estão cada vez mais organizados. Há, hoje, uma indústria do cibercrime, que não para de crescer. "Começa a haver uma estratificação, uma cadeia de valor. Existem entidades responsáveis apenas por desenvolver *toolkits* e bots que disponibilizam a terceiros para determinados efeitos. Quem ataca é quem compra estas ferramentas", sublinhou Eugénio Silva, ex-*Chief Information Officer* (CIO) da TMN e do Turismo de Portugal. Assim, longe vão os tempos (e a imagem) do tradicional *hacker*, fechado num quarto a programar em frente a um computador. "Isto é preocupante porque significa que pessoas sem grandes conhecimentos tecnológicos acabam por ter acesso às ferramentas necessárias aos ciberataques".

Para ilustrar a dimensão desta indústria, Paulo Vieira, *major account manager* da Check Point, frisou que, a nível global, o ransomware movimenta mais dinheiro do que o tráfico de drogas. "Há muito dinheiro envolvido. O próprio FBI aconselha a que se paguem os resgates. Há uma indústria completa, e a crescer, em torno deste mercado".

Fotografias: Rui Jorge

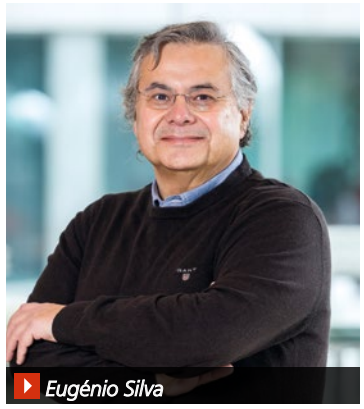
Sónia Casaca, *business unit manager - security,* na Arrow ECS, distribuidor de valor acrescentado, diz mesmo que estamos perante duas indústrias paralelas: "De um lado, os fabricantes estão a trabalhar para conseguir combater este tipo de ameaças. Do outro, a indústria do cibercrime regista uma rentabilidade financeira elevada". A responsável referiu que 2017 será de "combate" a ataques cada vez mais sofisticados, com novos tipos de soluções, para lá dos tradicionais antivírus. "Hoje simples firewall de perímetro não é suficiente, seja para as PME ou para as grandes organizações". Assim, ferramentas para combater ataques dia zero, ameaças persistentes avançadas ou ofensivas DDoS são cada vez mais a aposta dos fabricantes. Carlos Vieira, *country manager* para Portugal e Espanha da WatchGuard, realçou a complexidade da proteção da informação: "Hoje é bastante difícil ter um único dispositivo a proteger a informação, em virtude de um perímetro empresarial mais difuso – os dados estão nos dispositivos móveis, na cloud, em soluções de Software-as-a-Service, a circular por WiFi".

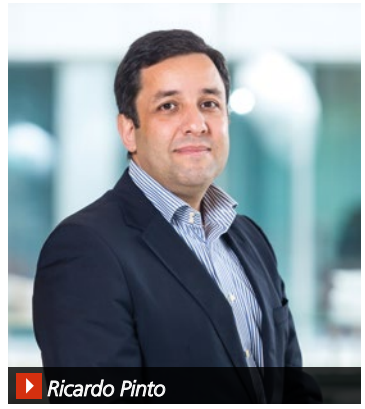
"Verificamos que, diariamente, há 8 milhões de novas infeções e que estão cada vez mais sofisticadas "

Rui Serra, product manager da AnubisNetworks

A velocidade a que hoje geramos informação beneficia os próprios cibercriminosos, que, como sublinhou Rui Pinho, *VSMB sales representative, channel sales*, da Kaspersy Lab, "começam já a utilizar eficazmente ferramentas de Big Data". A tecnologia "não vai parar", realçou, e os desafios prometem ser crescentes. Rui Serra, *product manager* da AnubisNetworks, deixou dados esclarecedores: "Verificamos que, diariamente, há oito milhões de novas infeções e que estão cada vez mais sofisticadas.


Carlos Vieira


Eugénio Silva


Ricardo Pinto

Detetámos inclusive um malware que consegue produzir um anexo, um cabeçalho e um conteúdo diferente a cada e-mail que envia".

Ransomware a crescer

Segundo o painel da primeira Mesa Redonda do *IT Channel* dedicada à cibersegurança, o ano de 2016 foi fértil em ameaças. E há um "ator" que se destaca, pelo protagonismo crescente: o ransomware. Ou "a maior dor de cabeça dos *IT managers* e o maior representante da industrialização do cibercrime", como realçou Carlos Vieira. Também Sónica Casaca indicou que o ransomware "lidera" a tendência, ao nível de ataques.

"Existem entidades responsáveis apenas por desenvolver toolkits e bots. Quem ataca é quem compra estas ferramentas"

Eugénio Silva, ex-CIO da TMN e do Turismo de Portugal

Em 2016, esta forma de malware – que, na sua essência, mais não é do que um sequestro dos dados, que ficam encriptados até ao pagamento de um resgate – tornou-se na segunda mais frequente, segundo Paulo Vieira, que classificou o crescimento de "astronómico". A prevalência do ransomware tem tido, no entanto, um efeito positivo: as empresas estão agora mais despertas para a necessidade de se protegerem. "Começamos a ver as empresas a perder muitos dados e a querer investir, para não terem este tipo de impacto negativo", destacou.

Os ataques de ransomware distinguem-se por estar alicerçados em engenharia social, outro dos traços cada vez mais prevalentes no cibercrime de hoje. "Não se tratam de ataques perpetrados através da rede ou dos servidores. Recorrem a vulnerabilidades dia zero", esclareceu Eugénio Silva. Ou seja, o *modus operandi* passa por recorrer ao e-mail de um colaborador, que ao clicar num link acaba por comprometer os dados da empresa, "o que coloca grandes desafios", segundo o ex-CIO, porque "todos os profissionais podem ser uma porta de entrada".

Esta personalização dos ataques é uma das maiores tendências. Ricardo Pinto, *business developer manager* da Forcepoint, na Ingecom, distribuidor de valor acrescentado dedicado à cibersegurança, falou mesmo em "ataques cirúrgicos, dirigidos a uma pessoa em particular". O objetivo primordial é a identificação de um alvo: "Os *hackers* procuram saber quem é, quem são os seus amigos, para induzi-los a clicar num link e, a partir daí, poder aceder à empresa. Um dos maiores veículos são as redes sociais".

Outra forma de propagação é a própria rede de contactos de uma empresa - mesmo que esteja protegida, a informação flui pelos colaboradores e pelos fornecedores. "Verificámos que quase 40% dos problemas de segurança estão relacionados com a rede de parceiros de uma empresa. Este fator também se relaciona com engenharia social, está tudo interligado", acrescentou Rui Serra. "Se receber um e-mail de um conhecido tenho um comportamento, se o receber de um fornecedor tenho outro". O *product manager* alertou para o facto das infeções serem também disseminadas pelas aplicações empresariais, "onde há cada vez mais malware":

Todos são um alvo

É errado pensar-se que os cibercriminosos estão mais focados nas grandes organizações no momento de atacar e que as PME não estão tanto no radar. "A industrialização do cibercrime levou a que entrassem neste mercado *hackers* que não diferenciam alvos", notou Eugénio Silva. Veja-se o exemplo do ransomware, que afeta igualmente PMEs e grandes empresas. "Propaga-se de forma genérica. Tanto atinge uma empresa de cinco colaboradores como uma de cinco mil. A diferença é que nesta será mais rentável e mais direcionado", alertou Rui Pinho.

O que deve ser mesmo tido em conta pelas empresas é, segundo Sónia Casaca, "a criticidade do negócio e do seu *core business*". Como exemplificou o responsável da Kaspersky Lab, "uma sociedade de cinco advogados pode ser um alvo muito apetecível se tiver uma carteira de clientes importantes".

Tudo porque o proveito dos cibercriminosos é, cada vez mais, uma questão de escala. Eugénio Silva é da opinião que uma PME ou até um indivíduo são mais fáceis de atacar, "por terem menos meios de

"O ransomware tanto atinge uma empresa de cinco colaboradores como uma de cinco mil"

Rui Pinho, VSMB sales representative, channel sales, da Kaspersky Lab

defesa". O ex-CIO falou em ataques de ransomware a pessoas, sobretudo no Brasil, em que o resgate é pouco mais de 20 dólares e que se tornam muito proveitosos por serem massivos. Do lado oposto está o maior resgate de ransomware alguma vez pago, tornado público: 17 mil dólares, nos EUA, valor acordado entre a vítima (um hospital) e os *hackers*.

Assim, e segundo este painel, o nível de preocupação deve ser igual em todas as empresas, de todos os tamanhos. "No final, haverá sempre um impacto negativo, seja ao nível das receitas ou por via da perda de dados dos clientes" apontou a responsável da Arrow ECS. Ricardo Pinto realçou, porém, que "os ataques dirigidos destinam-se sobretudo às grandes empresas, sendo muito mais complexos de mitigar".

A diferença entre uma pequena e uma grande empresa está, sobretudo, nas soluções a adotar: "Uma grande empresa terá de investir mais em soluções de gestão centralizada, tendo em conta a sua dimensão. Numa PME esse controlo é mais próximo, mas não invalida que ambas tenham as mesmas ferramentas de gestão", reforçou Rui Pinho.

Sensibilizar é preciso

Um dos maiores problemas nas PME é a consciencialização, que ainda é menor. No entanto, têm a virtude de serem "mais ágeis a agir e a colmatar o problema", segundo Paulo Vieira. "As grandes organizações são mais conservadoras, tendem a culpar a firewall". Por outro lado, realçou o *account manager* da Check Point, "preocupam-se com os dispositivos móveis, em saber se há aplicações infetadas ou se alguém está a gravar uma reunião, por exemplo, algo que nas pequenas empresas não se verifica".

"Começamos a ver as empresas a perder muitos dados e a querer investir"

Paulo Vieira, major account manager da Check Point

Mais uma vez, importa não desvalorizar o alcance do radar dos hackers. "Portugal é o terceiro país com mais máquinas infetadas com bots, por centenas de habitantes, em toda a EMEA. Observamos centenas de máquinas infetadas para roubo de informação, que são utilizadas em ataques DDoS e que estão sob o controlo de terceiras partes".

Ilustração: iStock.com/id-work

Sónia Casaca

Paulo Vieira

Vânia Penedo e Henrique Carreiro, moderadores

Consciencializar é preciso, e um papel que também cabe aos Parceiros, porque os custos indiretos de um ciberataque raramente são contemplados. Esta é mesmo a principal barreira que fabricantes e parceiros enfrentam. "Estamos perante três fases", enumerou o *country manager* da WatchGuard. "Primeiro é necessário consciencialização, depois ferramentas de backup atualizadas e posteriormente as soluções de segurança". Rui Serra falou mesmo numa "baixa preocupação com o risco", nas PME, ou "em separar a segurança do que é o IT normal".

De mãos dadas com esta despreocupação está o fator humano, unanimemente considerado "o elo mais fraco" por todos os intervenientes. "Quando se trata de pessoas, o assunto é mais complexo. Mais uma vez é preciso sensibilizar, até porque existem muitos colaboradores externos nas empresas. O ataque pode estar a ser perpetrado a partir de um colaborador, que nem sequer sabe que está a ser usado como atacante. Daí que também seja importante olhar para as aplicações internas como ponto de exposição", realçou Eugénio Silva. Como enfatizou Paulo Vieira, "o fator humano é o que os *hackers* procuram explorar ao máximo". No phishing, disse, "os atacantes preveem, em 48% das vezes, erro humano. Nos ataques de engenharia social, 38% e nos ataques dia zero 37%".

Quanto vale a informação?

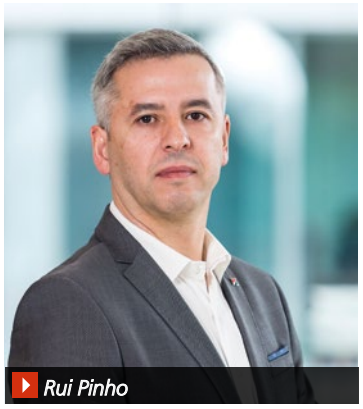
Em Portugal, as PME continuam a ter uma infraestrutura de cibersegurança obsoleta e a prestar atenção sobretudo ao fator preço. "As empresas até reconhecem que têm de ter um projeto interno de segurança, mas os orçamentos continuam a ser muito restritos. Também é comum solicitarem projetos a oito anos, o que é totalmente impossível. A mesma firewall de há quatro anos não pode ser a de hoje", frisou Sónia Casaca. "É preciso investir em infraestruturas novas", alertou. "É igualmente importante que se renovem os suportes e as atualizações. As mais pequenas, sobretudo, não entendem tão bem a necessidade do investimento".

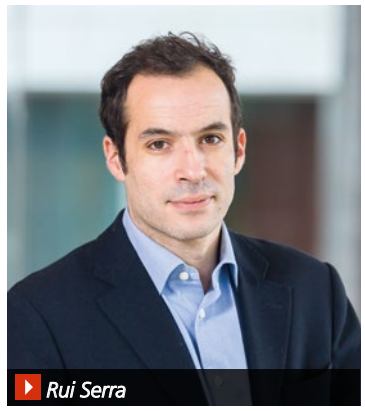
Apesar das soluções de cibersegurança ainda serem, como realçou Paulo Vieira, "o parente pobre" dos orçamentos de TI", é necessário, junto dos clientes, lançar a (metafórica) pergunta de um milhão de euros: Quanto vale a sua informação? Uma estratégia que Rui Pinho aconselha. "Coloco sempre esta questão em cima da mesa. Normalmente o cliente compara preço e não soluções". A principal falha está, como fez questão de esclarecer Ricardo Pinto, "em não avaliar-se o valor da informação ou quanto custa a uma empresa ficar parada". Na realidade, as empresas não o sabem: "Quando se fala no custo de uma solução, o cliente não tem em conta esse fator, acabando por adquirir uma solução inadequada só porque custa menos". Sobre este ponto, Carlos Vieira

"Hoje a simples firewall não é suficiente, seja para as PME ou para as grandes empresas"

Sónia Casaca, business unit manager - security na Arrow ECS

colocou o dedo na ferida: "Destina-se muito orçamento ao armazenamento de dados e ao *backup*, mas depois esquece-se a proteção desses mesmos dados". É que, realçou, o valor de um projeto de segurança tende a ser, em média, apenas 10% do valor do armazenamento. "Vale a pena relembrar que um cartão de crédito roubado vale entre 50 cêntimos a um dólar no mercado negro. O registo de uma empresa vale entre 10 a 20 dólares", disse, ilustrando o valor da informação empresarial.


Rui Pinho


Rui Serra

Nova legislação abrirá "Caixa de Pandora"

A ideia de que um ciberataque só acontece aos outros, de que os investimentos em soluções de cibersegurança podem ser relegados para segundo plano ou de que é possível gastar o menos possível e ficar bem protegido deverá ter os dias contados. Este cenário deverá mudar a partir do momento em que as empresas sejam obrigadas a comunicar às autoridades sempre que tenham sido vítimas de um ciberataque, o que acontecerá quando o novo Regulamento Geral de Proteção de Dados da União Europeia entrar em vigor, a partir do dia 25 de maio de 2018. "Vai abrir-se uma Caixa de Pandora, porque vai começar a ser noticiado na comunicação social. O custo reputacional e os danos de imagem também são relevantes", realçou Carlos Vieira. "Os

"Destina-se muito orçamento ao armazenamento e ao backup, mas depois esquece-se a proteção dos dados"

Carlos Vieira, country manager da WatchGuard para Portugal e Espanha

CEOs vão ter uma responsabilidade direta, porque com a nova legislação veremos mais empresas com a imagem danificada, mesmo as PME". A este propósito, vale a pena relembrar que toda a direção da retalhista norte-americana Target foi despedida no seguimento de um *data breach* massivo, em 2013, que expôs os dados de cartões de crédito e débito de 40 milhões de clientes. "Sobretudo a partir de 2018, o negócio da cibersegurança será bastante interessante para fabricantes, distribuidores e parceiros".

Evolução para os *managed services*

O mercado da cibersegurança é, para fabricantes, distribuidores e Parceiros de Canal, uma tremenda oportunidade, segundo o nosso painel. Carlos Vieira diz mesmo que é "a maior" e que este é "um mercado saudável" e que aporta a tão rentável componente de serviços. "Estamos no início de uma curva exponencial", disse. O ritmo de evolução das ciberameaças beneficia em muito o próprio negócio dos Parceiros, dado que no SMB os *IT managers* não têm conhecimentos suficientes para acompanhar o atual panorama do cibercrime. Eugénio Silva fala num "movimento de todo o IT", apontando que "cada vez menos as equipas internas das empresas são capazes de abordar todas as temáticas" e que "é importante que apareçam especialistas".

Os Parceiros têm a oportunidade de se posicionar com um departamento de cibersegurança externo destas empresas, o que pressupõe, no entanto, adotar um novo modelo de negócio, suportado por serviços (OPEX e já não CAPEX), e uma postura mais próxima da de um consultor. É, assim, necessário um novo perfil de Parceiros: Managed Service Providers (MSPs) e Managed Security Service Providers (MSSPs). "O Parceiro que é o intermediário só funciona até um certo ponto", observou Rui Serra. "Importa trazer valor acrescentado e isso significa serviços de cibersegurança. Aliás, estamos a ver os próprios *vendors* a avançarem para essas áreas".

Este é um modelo que os operadores de telecomunicações já adotaram há alguns anos e que deve agora ser abraçado pelos Parceiros, em nome da sua própria sustentabilidade. "É necessário que tenham *know-how*, até mesmo para conseguirem sensibilizar o cliente. O dinamismo dos ataques tem de ser acompanhado pelo dinamismo de toda a componente de serviços, sobretudo ao nível das configurações", apontou Rui Pinho. "Temos Parceiros que olham muito para as nossas soluções de antivírus como um *commodity*, que ainda não veem a segurança como uma forma de entregar valor acrescentado". O *channel manager* da Kaspersky entende que haverá sempre o revendedor, mas que este será "cada vez mais um nicho".

Em Portugal, Parceiros em que a segurança é o core business são ainda muito poucos, havendo por isso mais margem para conquistar mercado. "No SMB, começamos a encontrar Parceiros onde a segurança já é um complemento importante a nível de serviços e de venda de produtos de valor acrescentado, que são atrativos por aportarem alguma margem. Também vemos Parceiros de segurança a entregar projetos chave-na-mão, com segurança, serviços e suporte", realçou Carlos Vieira.

Do lado da distribuição, a Arrow ECS tem observado uma "grande evolução", sobretudo no número de Parceiros dedicados a cibersegurança. "Há uns anos sentíamos que não havia Parceiros suficientes nesta área. Hoje, começamos a ver Parceiros de networking, backup e storage a estabelecerem a segurança como uma área de foco para os próximos anos", revelou Sónia Casaca. Ser um integrador tradicional nesta área é algo que, advertiu, "não pode acontecer", o que implica muita formação, tanto

"O Parceiro tem de ter o papel de consultor, de olhar para a oferta disponível e entregar a melhor proposta"

Ricardo Pinto, business developer manager da Forcepoint na Ingecom

técnica como comercial, que tanto a Arrow ECS como a Ingecom se comprometem a disponibilizar. "Cabe-nos a nós, fabricantes e distribuidores, apoiar o Parceiro, que é o braço direito do cliente. É ele que olha para a oferta disponível e que tenta formar a proposta mais adequada. Tem de ter o papel de consultor, de acompanhar o projeto ao longo de toda a sua vida, assegurar configurações, monitorização e otimização. É uma relação de médio a longo prazo que se estabelece com os clientes".

A migração para o OPEX tem, no entanto, os seus 'custos'. Não é fácil para as empresas do Canal, sobretudo para as menores, diluir o fluxo financeiro por faturas mensais. "Os desafios existem mesmo do ponto de vista da logística, da própria contabilidade, além de exigir capacidade financeira. O distribuidor ainda vai funcionar mais como um banco".