"A atual estratégia da Check Point contempla as PME"

A paisagem de novas ciberameaças, marcada pela prevalência dos ataques dia zero – que têm no ransomware o rosto mais conhecido – tem levado a Check Point a apostar em soluções mais sofisticadas. A oferta do fabricante contempla agora as PME, o que significa uma nova estratégia para o Canal, como nos conta Rui Duro, *sales manager* da Check Point

***IT Channel*- Que diagnóstico faz a Check Point do mercado da cibersegurança em Portugal?**

Rui Duro - Notam-se duas situações completamente antagónicas: por um lado, os clientes estão mais despertos para a necessidade de investir em soluções de cibersegurança. Os ataques que têm ocorrido ultimamente, e a sua divulgação, têm levado a que o mercado esteja mais recetivo. Por outro, não conseguimos fugir à situação financeira do País, que provoca constrangimentos enormes e leva muitas vezes a que os clientes comprem algo que lhes dá a sensação de estarem protegidos.

Se, por um lado, existem sinais positivos, por outro continua a ser bastante complicado devido aos muitos constrangimentos orçamentais.

Fotografias: Rafael Antunes

O ano 2016 está a ser mais ou menos positivo?

Este ano, em particular, está a correr significativamente bem para a Check Point. Não porque o mercado esteja melhor, mas porque temos tido bastante sucesso nas nossas ações e porque a nossa equipa cresceu. Continuamos a sentir as mesmas dificuldades que sempre sentimos. Noto, quando estou com os meus colegas europeus, que há uma grande diferença no esforço financeiro e humano que em Portugal temos de fazer para concretizar a venda face ao esforço que é necessário noutros mercados, nomeadamente no germânico ou mesmo nos nórdicos, para as mesmas soluções. Isso está claramente relacionado com o ambiente económico.

A segurança continua ter a menor fatia dos orçamentos de IT?

Sim, claramente. Diria que esta vaga de ransomware que agora aparece vem ajudar um pouco a inverter essa realidade. Era frequente dizer-se que não é possível identificar o ROI da segurança. Há dias um diretor de IT de um banco dizia-me que tinha de renovar um conjunto de firewalls e que um dos departamentos da instituição lhe pedia para justificar o retorno relacionado com cada firewall. O que não é, evidentemente, possível. O ransomware veio adicionar esse elemento: quando os dados estão todos encriptados, quando a produção parou, quando a base de dados ou o servidor da empresa está encriptado, há uma manifestação visível. Ou seja, já existe uma justificação. Notamos, no entanto, que muitas vezes é feito um investimento errado.

Porque acontece?

Às vezes a decisão é tomada pelas pessoas que não têm *know-how* ou o *empowerment* suficiente para fazer passar a sua mensagem, ficando reféns da capacidade de tornar mensurável essa necessidade. Como não conseguem fazê-lo, a decisão financeira é tomada a outro nível. É possível apontar os ganhos da aquisição de um novo servidor de base de dados para a faturação, por exemplo, mas não de um equipamento de segurança.

Este é outro aspeto: a maioria das empresas enfrentam diariamente incidentes de segurança mas simplesmente não o sabem, porque o novo malware que circula neste momento é polifórmico, ou seja, é totalmente mutável e flexível, para não ser detetado pelos sistemas tradicionais que se baseiam em assinaturas. É, também, altamente programável, isto é, consegue a qualquer momento receber um comando e transformar-se num malware completamente diferente. Isto faz com que circule dentro das empresas e não seja detetado. Muitas vezes só o é quando algo estranho acontece. O ransomware é quase um malware tradicional, porque o seu objetivo é receber dinheiro. Logo, tem de tornar-se visível. Mas há bastante malware que quer estar invisível e indetetável na rede de forma a roubar informação, a perpetrar ataques de DDOS ou a fazer spam.

Em cem por cento dos diagnósticos realizados pela Check Point em Portugal, e já fizemos centenas, detetámos *bots* na rede. O bot é um malware inteligente, muito mutável e não detetável pelos sistemas tradicionais. E verificámos que estava presente em todas as organizações, da área da saúde à banca, passando pela administração pública. Nenhum dos clientes tinha noção de que isto acontecia.

Também nas PME?

O resultado é exatamente o mesmo. A Check Point tem, neste momento, uma estratégia mais alargada, que contempla as PME. Somos conhecidos por suportar

os grandes clientes e em Portugal o cenário não é diferente. No entanto, lançámos recentemente uma nova linha de produtos e uma abordagem que nos permite ir à procura de um mercado que normalmente não era endereçado por nós. Começámos, assim, a adotar as mesmas práticas junto de clientes mais pequenos.

O que carateriza essa nova oferta?

Lançámos uma linha de hardware que tem caraterísticas próprias para este mercado. A partir de agora, uma pequena empresa consegue ter um produto *premium*, porque é vítima dos mesmos ataques que afetam as grandes organizações.

Neste momento, as pequenas empresas são o maior alvo de ransomware. Poderá também estar relacionado com o facto de as empresas de maior dimensão terem maior capacidade de resolução dos problemas. Nas empresas mais pequenas também há uma menor educação dos utilizadores.

Além do ransomware, que outras ameaças são mais prevalentes nas PME?

Identificámos muitos *bot*, que têm várias implicações, o que leva a que estas empresas participem em ações ilícitas sem o saberem, podendo vir a deparar-se com uma investigação da Polícia Judiciária. Quem ataca quer fazê-lo sem ser detetado e, para tal, recorre a vítimas. Os recursos das PME são utilizados para spam ou para ataques de *denial of service*. Estes são os ataques que mais verificamos nas PME. As pequenas empresas, e até algumas câmaras municipais, têm informação muito importante dentro de portas. A nossa experiência mostra-nos que poucas autarquias estão protegidas, e estas pequenas instituições públicas têm dados de grande valor que podem estar facilmente comprometidos por não haver orçamentos que lhes permitam melhorar as suas condições.

As soluções utilizadas pela autarquias são sempre o mínimo possível: a firewall e o antivírus de desktop, que hoje em dia são insuficientes.

Qual o *price point* da oferta da Check Point para as PME?

Posicionamo-nos em linha com a concorrência. O hardware tem outras caraterísticas, porque as necessidades são outras, pelo que conseguimos ser mais competitivos. Com esta nova oferta o cliente consegue ter a inteligência da Check Point numa solução bastante acessível e adequada às suas necessidades.

Como se reflete esta nova oferta na estratégia de Canal da Check Point?

Implica uma mudança. Até agora, e porque trabalhávamos apenas com as grandes contas, os Parceiros que tínhamos refletiam essas mesmas caraterísticas. De momento estamos a tentar chegar a outro tipo de cliente, pelo que o próprio Canal muda significativamente. É maior mas composto por empresas mais pequenas e menos especializadas. Daí que os produtos também ajudem à construção de soluções específicas.

Rui Duro, sales manager da Check Point

Atualmente estamos a iniciar campanhas de proximidade ao Canal e a ajustar a oferta. Assim que tivermos toda a mensagem transmitida, teremos um plano de formação para colocar em prática por todo o País.

Estão a recrutar novos Parceiros?

Desde maio que temos um recurso a norte, no Porto, que está a desenvolver um conjunto de ações e de contactos com novos Parceiros. Alguns trabalhavam já com a Check Point, mas não havia uma relação tão próxima. Neste momento o contacto é semanal, com alguns é até diário, e os resultados começam a aparecer. Pretendemos desenvolver este Canal com ações de formação e já realizámos duas. Vamos agora iniciar as ações de formação técnicas com estes mesmos Parceiros.

Os recursos das PME são utilizados para spam ou para ataques de denial of service

Qual o objetivo estabelecido para 2016?

Situa-se na ordem dos 20% de crescimento. Neste momento estamos em linha com os números que nos permitirão alcançar esse objetivo no final do ano. Isto leva-nos a crer que, se a situação do País fosse outra, provavelmente estaríamos ainda mais satisfeitos.

Qual é, de momento, a prioridade da Check Point em termos de portfólio?

A Check Point está muito associada à firewall. Continuamos a trabalhar ao nível das *gateways* de segurança, que colocamos no perímetro das empresas, mas existem hoje novos ataques que exigem outro tipo de soluções e, por isso, boas oportunidade de crescimento. Refiro-me ao ransomware, aos ataques dia zero, às ameaças persistentes avançadas (APTs).

Trata-se de uma oportunidade imensa porque apenas 0,1% das empresas, a nível mundial, aderiram a estas soluções. Se já não é fácil colocar antivírus ou um *anti bot* na *gateway*, mais difícil será colocar uma solução especializada de proteção de ataques dia zero. Temos de passar bem a mensagem. O ransomware, por exemplo, é um ataque dia zero, porque na maioria dos casos só é detetado quando se manifesta.

A mobilidade permanece uma prioridade?

Sim, outra área onde estamos a trabalhar ativamente diz respeito aos dispositivos móveis. O último relatório da Gartner coloca a Check Point como o único fabricante que cumpre as quatro áreas de proteção dos dispositivos móveis: análise de aplicações, avaliação comportamental dos dispositivos, segurança da rede e vulnerabilidade do próprio dispositivo.

Outra área na qual estamos também a trabalhar é cloud e virtualização. Em cloud pública trabalhamos com Azure e Amazon web Services (AWS). Depois há ainda outra área que está em grande crescimento, que são os *software defined* data centers, onde temos parcerias muito fortes, como é o caso da Cisco e da VMWare. Se um cliente tiver um sistema em Hyper V, ou em VMWare, ou KVM, conseguimos virtualizar *firewalls* na sua infraestrutura virtual.

A Check Point é hoje muito mais do que o fabricante tradicional de firewall. As oportunidades de negócio, principalmente para o Canal, são enormes.