JE MAIS TIC

Check Point anuncia proteção contra nova geração de ciberataques
| PVI e PVII

Soluções da ICG evoluem para cloud computing
| PVIII

CIBERSEGURANÇA

Ameaças diversificam-se e tornam-se mais complexas

Mais ransomware, ataques cirúrgicos, mineração não autorizada de criptomoedas, vulnerabilidades nos processadores. Será assim 2018. A cibersegurança há muito que deixou de se resumir a um software de antivírus nas suas máquinas e a uma função do departamento de IT. Toda a empresa deve estar envolvida. do topo estratégico, às bases operacionais. Pessoas, processos e tecnologias são os três pilares indissociáveis nas empresas que pretendem proteger os seus sistemas de informação. Para fazer face ao incremento da quantidade e da complexidade das ameaças, as empresas devem adotar abordagens de proteção sistémica e holística que abranja globalmente a organização. | PP. II a V

Samantha Sais/Reuters

CIBERSEGURANÇA

Ameaças diversificam-se e tornam-se mais complexas

A segurança tecnológica passou a ter de ser uma preocupação partilhada de todas a organização, do topo à base. A cibersegurança deixou de ser um problema só do departamento de TI.

MAFALDA SIMÕES MONTEIRO
mmonteiro@jornaleconomico.pt

Este ano, as empresas têm de fazer face a grandes desafios em matéria de política de segurança: adotar novas tecnologias, enfrentar ciberameaças e ter em conta os custos em que incorrer as organizações em resultado das opções tomadas.

Depois dos surtos "Wanna Cry", "Not Petya" ou "Bad Rabbit", que chamaram a atenção, de forma mais premente, para as questões da cibersegurança em 2017, o ransomware continua no topo de muitas listas de perigos na internet. Entretanto, a mineração não autorizada de criptomoedas é identificada por várias fabricantes e integradores de software de segurança como uma ameaça, enquanto a Intel e outros fabricantes de processadores publicam correções para as vulnerabilidades "Spectre" e "Meltdown" identificadas já este ano.

Se tivermos em conta a evolução dos ataques cibernéticos na última década, onde fenómenos de ransomware afetaram centenas de milhares de equipamentos à escala mundial, a perspetiva para 2018 não parece muito animadora para as organizações, diz Tiago Vieira, IMS Business Development Team Leader (Konica Minolta). "Tendencialmente, os hackers irão evo-


Kacper Pempel/Reuters

luir mais rápido que os sistemas de segurança, o que nos suscita um desafio acrescido: a prevenção. Este desafio terá em conta uma componente tecnológica, mas acima de tudo pedagógica, pois grande parte das vulnerabilidades detetadas tem por base uma ação involuntária de um determinado utilizador".

A gestão do ciber-risco começa, por isso, a entrar no léxico das empresas, que já optam por seguros de risco para mitigar possíveis prejuízos decorrentes de eventuais ataques aos sistemas informáticos. O Regulamento Geral de Proteção de Dados (RGPD) é apontado como um ponto de viragem na organização sistémica dos sistemas de informação. Afinal, as coimas são elevadas. No setor financeiro em particular, as empresas não podem ignorar a diretiva PSD2.

Mais atenção à cibersegurança

"Podemos dizer que as nossas empresas começam a olhar para este tema [da cibersegurança] com maior atenção" e começa a assistir-se a um maior "investimento em soluções de protecção, especialmente nos dois últimos anos", diz Andreia Pinto Teixeira, diretora de ciber-risco na Aon Portugal. "Não obstante, temos ainda uma percentagem considerável de empresas a subestimar as vulnerabilidades das suas áreas críticas e das responsabilidades que sobre si impendem e, por conseguinte, prevê-se o aumento dos ataques informáticos", acrescenta.

Ciberataques, fraude ou roubo de dados estão entre os cinco mais prováveis riscos mundiais para 2018 elencados pela Marsh e pelos seus parceiros no relatório dos Riscos Globais 2018, divulgado no Fórum de Davos. Carlos Figueiredo, responsável pela área de cyber risks da Marsh Portugal, recorda que as ciberameaças "estão a ganhar destaque no top dos riscos, com ciberataques em grande escala, agora posicionados em terceiro lugar em termos de probabilidade e em sexto em termos de impacto".

Da mesma opinião é Ricardo Maté, diretor-geral da Sophos Iberia: "Ao longo de 2018 prevê-se que, devido à facilidade de acesso a kits de ransomware na dark web, este tipo de ataques aumente, tanto a grandes empresas como a utilizadores particulares". O relatório "SophosLabs 2018 Malware Forecast" antecipa que essa maior quantidade de ataques ransomware se foque "nos setores mais vulneráveis como governos, infraestruturas ou saúde".

Ricardo Maté assinala também os ataques relacionados com as criptomoedas com o objetivo de "infetar os dispositivos com malware de criptomineração", que afeta o desempenho dos computadores e requer muita potência dos processadores, abrandando-os e desgastando-os. Por tudo isso, "a proteção dos dispositivos móveis pessoais e empresariais, como os smartphones ou tablets, adquire grande importância".

"Continuaremos a assistir a uma grande proliferação de malware, cujo alvo são os utilizadores finais, quer seja com a intenção de extorsão (Ransomware), de obtenção de acesso às redes corporativas, de privilégios, para danificar dados ou, até, mesmo mineirar criptomoedas", diz Nuno Cândido, senior manager da área de infraestruturas na Noesis. E acrescenta que já foram identificados cerca de 140 formas de utilização para falhas de segurança identificadas recentemente na maioria dos processadores modernos. Por isso, diz, "será uma questão de tempo até começarem a ser usadas em ataques massivos de malware".

Ciberameaças travam transformação digital

O principal entrave à transformação digital das empresas continuará a ser a preocupação com as ciberameaças. Um estudo da Cisco aponta que "60% dos diretores consideram que as suas empresas são relutantes a inovar os produtos e serviços digitais devido aos riscos de cibersegurança, e sete em cada dez afirma que as preocupações com a cibersegurança estão a retardar a inovação", assinala Eutimio Fernández, diretor de cibersegurança da Cisco para Espanha e Portugal.

Já entre os principais desafios identificadas pela consultora EY – adotar novas tecnologias, enfrentar as ciberameaças e ter em conta os custos que podem ter para as organizações cada um dos primeiros desafios –, aqueles que poderão ter maior impacto são a falta de formação das pessoas, a falta de capacidade de resposta a incidentes, o roubo/perda de informação, a eficácia da operação de segurança, incluindo antivírus, cifragem e correções, ataques de Denial of Services (DoS), malware e phishing, detalha Sérgio Sá, associate partner da EY.

As empresas enfrentam um conjunto de ameaças que começa precisamente pelo "aumento da complexidade dos ambientes de TI e das soluções de segurança adotadas", diz Sérgio Sá. Por outro lado, também os próprios ciberataques se "estão a tornar mais complexos" e com um impacto cada vez maior. Acresce a toda esta complexidade a "falta de profissionais especializados em cibersegurança", algo com "tendência a agravar-se", sublinha.

Eutimio Fernández concorda e cita um estudo que revela que "65% das organizações têm entre seis a mais de 50 soluções de segurança pontuais [não integradas entre si] que tornam os ambientes vulneráveis". O estudo revela também que "apenas 56% dos alertas de segurança são investigados pelas organizações, devido à falta de recursos ou de pessoas especializadas".

Por seu lado, a S21sec aponta para o crescimento das ameaças endereçadas aos dispositivos móveis. João Barreto, vice-presidente de marketing estratégico da empresa de cibersegurança do grupo Sonae, destaca ainda "o aumento da sofisticação dos meios usados para realização dos ataques" e a "utilização dada aos dispositivos comprometidos". Neste aspeto assinala que os ativos comprometidos serão rentabilizados de forma alinhada com a conjuntura em cada instante. "Num período de crescimento do valor das criptomoeadas, é provável que os criminosos usem os dispositivos comprometidos para minerarem criptomoeadas", diz, acrescentando acreditar também que se "intensificarão os ataques com motivações político-estratégicas, state-sponsored, o que provocará a tomada de posições extremas por alguns governos, como boicotes comerciais".

As empresas enfrentam um conjunto de ameaças que começa precisamente pelo "aumento da complexidade dos ambientes de TI e das soluções de segurança adotadas", diz Sérgio Sá, associate partner da EY

O destaque da Fujitsu para os desafios que a cibersegurança enfrenta no corrente ano vai para a Cyber Threat Intelligence (CTI), uma forma de fornecer um sistema de alerta precoce aos clientes e contextualizar as ameaças, explica Pedro Pires, consultor de cibersegurança da Fujitsu. "Em suma, ao fazer o trabalho difícil, os fornecedores podem, na prática, bloquear as ameaças antes de elas terem oportunidade de causar estragos". Outro desafio apontado por Pedro Pires, é a resposta a incidentes e, acima de tudo, a rapidez com que as organizações são capazes de responder aos incidentes vão ser cada vez mais importantes com o advento do RGPD e da legislação sobre Redes e Sistemas de Informação (NIS).

Adelino Monteiro (Sage) recomenda às empresas, uma vez que "as ameaças são globais e os eventos gerados", o investimento nos serviços de um Managed Security Services Provider (MSSP), que pode "alertar-nos para situações incomuns e que podem resultar em falhas de segurança". Finalmente, deve auditar-se regularmente todos os processos e sistemas da empresa, garantindo sempre que os mesmos obedecem a todos os requisitos legais e técnicos e de acordo com a estratégia de segurança da empresa.

Maria Antónia Saldanha, da SIBS, considera que as maiores ameaças para a área em que empresa opera deverão estar relacionadas com o crescimento nos "ataques sofisticados de fraude online", tendo em conta "os avanços tecnológicos e o desenvolvimento do comércio eletrónico". Para fazer face a esta ameaça, a diretiva PSD2 "promove a criação e atuação de novos tipos de prestadores de pagamento", impondo-lhes também "maiores responsabilidades na execução de operações de pagamento não autorizadas", mas a SIBS também está a ser proativa nesta matéria e firmou uma parceria com a IBM para o aperfeiçoamento do serviço de segurança cognitiva "Paywatch" que atua na deteção, interceção e prevenção de fraude, garantindo maior eficácia na identificação em tempo real de potenciais fraudes".

Sofisticação do cibercrime torna sistemas complexos

"O crime cibernético tornou-se cada vez mais sofisticado e as organizações têm dificuldade em detetar, prevenir e responder efetivamente a ataques", alerta João Borrego, sales consulting senior manager da Oracle Portugal. Refere que, actualmente, os executivos estão preocupados com a gestão de receitas e com a redução dos custos, mas, dentro de menos de dois anos, "a importância da segurança e conformidade será igual ou maior". Entretanto, o perímetro de segurança vai sofrendo uma erosão, à medida que temas como o "mobile, a IoT ou a cloud evoluem a uma velocidade nunca antes vista.

Esta tendência é corroborada por Mafalda Alves Dias, diretora de grandes contas e setor público da Vodafone Portugal, que cita o relatório "Strong Cyber Security drives growth & innovation", apresentado pelo Grupo Vodafone no âmbito de um estudo internacional, que revela que 89% das empresas considera a cibersegurança um fator determinante na conquista da confiança e lealdade dos seus Clientes. Sendo que mais de 85% admite aumentar os seus orçamentos alocados a ferramentas de segurança nos próximos três anos.

Melhores práticas são a solução

João Borrego assinala que "o número de dispositivos, serviços e pessoas autorizados a aceder aos dados das organizações só tem paralelo com o número de ameaças automatizadas. Para manter os sistemas seguros é necessário aplicar as melhores práticas de segurança, embora, algo que "continuará a ser um desafio", com a "falta de planeamento para aplicação de correções regulares, cifragem e mascaramento de dados insuficiente, dificuldade de manutenção de sistemas legados e cumprimento de novas normas (por exemplo, o RGPD), colocando dados e serviços em risco".

Sérgio Sá aponta que a adoção de novas tecnologias de informação está a tornar-se cada vez mais complexa devido à multiplicidade de componentes (cloud, mobile, social, Internet das Coisas - IoT, entre outros) e às questões de segurança. O consultor recomenda uma mudança na forma como a gestão é feita nas empresas, porque a adoção daquelas tecnologias "tem implicações na gestão de mais dispositivos, dados armazenados e métodos de acesso aos mesmos" e também porque "parte significativa dos responsáveis de TI e/ou segurança não acredita que o programa de segurança de informação definido pela organização responda às necessidades".

Steve Marcus/Reuters

CIBERSEGURANÇA

ESPECIALISTAS RECOMENDAM ABORDAGENS DE CIBERSEGURANÇA HOLÍSTICAS

Proteger, detetar e reagir. Para manter os sistemas de informação seguros é preciso adotar uma abordagem que abranja globalmente a organização.

MAFALDA SIMÕES MONTEIRO
mmonteiro@jornaleconomico.pt

Deve ser definido um "programa de segurança robusto que contemple como pilares pessoas, processos, tecnologias e parceiros", explica Sérgio Sá, associate partner da EY. Este programa deve ter capacidade de proteger, detetar e reagir, sendo que a "capacidade de reagir algo que poucas organizações possuem e vão necessitar de implementar".

Nas palavras de João Barreto, vice-presidente de marketing estratégico da empresa de cibersegurança S21sec, "a aproximação deve ser holísica e sistemática devendo as medidas serem, de forma geral, de três naturezas: preventivas, de monitorização e reativas". Assinala que "a prevenção é, efetivamente, a mais relevante e, na maioria dos casos, a menos executada. São, infelizmente, poucas as empresas que incluem a cibersegurança na sua prática de gestão de risco, identificando ameaças, antecipando riscos e definindo salvaguardas e medidas de monitorizar a sua concretização, idealmente ainda numa fase preparatória em que os cibercriminosos estão a ultimar ou a ativar as suas campanhas dirigidas".

Para a Cilnet, a solução passa pela definição de políticas de segurança, formação e divulgação das mesmas, bem como a implementação de ferramentas de monitorização e correlação de eventos são a base para manter a consistência, privacidade e proteção dos dados", refere Miguel Borges, administrador da empresa. "Para a implementação destas políticas de segurança deverão ser bem definidos os processos, a divulgação dos mesmos, a tecnologia adaptada a estes requisitos, nomeadamente soluções de backup, ferramentas de compliance, proteção de perímetro e de acesso", conclui.

E João Rodrigues, diretor-geral da Schneider Electric Portugal, acredita que "para evitar ciberataques, não devemos isolar as nossas organizações/sistemas. A consequência de trabalhar em sistemas isolados, ou seja, não dialogantes, é certamente pior do o risco da exposição a um ciberataque".

O responsável da Schneider menciona que "se num todo conseguimos dar respostas aos novos desafios que se impõem, a diferença poderá passar pela perceção individual face às três dimensões essenciais: pessoas, processos e tecnologias". João Rodrigues não dúvida que "as pessoas desempenham o papel mais importante na segurança. Mantê-las informadas, de uma forma constante, é um fator chave para qualquer plano de segurança de uma empresa".

Enquanto isso, Rui Ribeiro, da IBM, assinala que "transformação pode ser uma oportunidade para nos focarmos nos componentes essenciais" e, para que tudo funcione em pleno recomenda a "construção de uma cultura virada para a deteção e gestão de risco", uma vez que "as pessoas são críticas em todas as organizações e, numa perspetiva de segurança, isso é absolutamente incontornável". As empresas devem fazer uma "boa higiene de segurança". Rui Ribeiro recorda que "as campanhas de Wannacry e as variantes Petya expuseram alguma fragilidade em processos básicos como as correcções (patching) nas organizações". E assinala, "numa organização com uma cultura de gestão de risco, os controlos implementados estão associados ao risco existente, e ainda é frequente, nos controlos básicos, as organizações falharem".

Muito mais que uma responsabilidade do IT

"Não é uma tarefa fácil conciliar os

SÉRGIO SÁ
Associate partner na EY

As empresas enfrentam em 2018, um conjunto de ameaças que começa precisamente pelo "aumento da complexidade dos ambientes de TI e das soluções de segurança adotadas".

JOÃO BARRETO
Vice-presidente de marketing estratégico da S21sec

"Num período de crescimento do valor das criptomoeadas, é provável que os criminosos usem os dispositivos comprometidos para minerarem criptomoeadas em vez de cifrarem dados e pedirem um resgate (ransomware)."

CARLOS FIGUEIREDO
Responsável pela área de cyber risks da Marsh Portugal

"As empresas que estão a implementar uma gestão de risco eficiente para enfrentar os riscos cibernéticos ganham uma vantagem competitiva face à sua concorrência."

MARIA ANTÓNIA SALDANHA
Diretora de marca e comunicação da SIBS

"A nova diretiva europeia PSD2 impõe aos prestadores de serviço de pagamento maiores responsabilidades na execução de operações de pagamento não autorizadas."

ANDREIA PINTO TEIXEIRA
Diretora de ciber-risco na Aon Portugal

O RGPD "tem levado a que muitas empresas antecipem os seus planos e procedimentos de implementação para estarem em conformidade, tendo em consideração não só as sanções por incumprimento, como o dano reputacional".

RUI BARATA RIBEIRO
Responsável de vendas da IBM Security Systems

"A cibersegurança é cada vez mais um fator de suporte às atividades económicas, potenciando um modelo ágil, eficiente e global, e isso é, em si mesmo, uma oportunidade relevante".

MIGUEL BORGES
Membro da administração da Cilnet

"O facto de as empresas estarem cada vez mais móveis e com uma maior dispersão dos dados cria uma série de novos desafios de segurança tanto no ponto de vista tecnológico como nas politicas de segurança."

JOÃO RODRIGUES
Diretor-geral da Schneider Electric Portugal

"Para evitar ciberataques, não devemos isolar as nossas organizações/sistemas… A consequência de trabalhar em sistemas isolados, ou seja não dialogantes, é certamente pior do o risco da exposição a um ciberataque".

JOÃO BORREGO
Sales consulting senior manager da Oracle Portugal.

Atualmente, os executivos estão preocupados com a gestão de receitas e com a redução dos custos, mas, dentro de menos de dois anos, "a importância da segurança e conformidade será igual ou maior".

MAFALDA ALVES DIAS
diretora de grandes contas e setor público da Vodafone Portugal

O novo quadro normativo para o RGPD é um dos desafios para 2018, pois vem exigir uma adaptação dos processos das empresas.

NUNO CÂNDIDO
Senior manager da área de infraestruturas na Noesis

"Já foram cerca de 140 exploits para as recentes falhas de segurança identificadas na maioria dos processadores modernos. Será uma questão de tempo até estas vulnerabilidades começarem a ser usadas em ataques massivos de malware"

processos, tecnologia e fator humano", diz Andreia Pinto Teixeira, da Aon Portugal, que também defende uma abordagem holística no combate às ameaças. "Quando falamos de ameaças à cibersegurança precisamos de ter em consideração a multiplicidade de riscos que podem afetar uma empresa: riscos legais, operacionais, financeiros, reputacionais, entre outros", refere. Por isso, a defesa deve envolver várias áreas da empresa, desde "o IT aos recursos humanos, marketing, operações, jurídico, financeiro, colaboradores, e, não menos importante, a própria direção da empresa".

Para além da implementação de um plano de resposta interno para a eventualidade de um incidente "cibernético", uma matéria que "não deve ser da responsabilidade exclusiva dos especialistas da informática e área jurídica, mas um tema transversal aos administradores, ao departamentos de gestão de risco, de operações, recursos humanos e conformidade", Carlos Figueiredo, da Marsh Portugal, recomenda a avaliação da exposição das organizações aos ciber-riscos (ou riscos cibernéticos na designação da Marsh), nomeadamente através de um Risk Assessment. Esta avaliação permite às empresas "analisar os impactos desses riscos, a possibilidade de sofrerem uma interrupção do negócio, quantificarem as respetivas potenciais perdas e analisarem soluções de mitigação e financiamento dos riscos, ao nível, por exemplo, da privacidade, disponibilidade e integridade".

O responsável da Marsh Portugal recorda que "o reforço da proteção através de uma cobertura de riscos cibernéticos", permite "transferir prejuízos, parte das responsabilidades e de custos imputáveis às organizações para o mercado segurador e, simultaneamente, garante uma componente de assistência em situações de crise".

De volta à Aon, Andreia Pinto Teixeira recomenda o mapeamento dos riscos que podem estar relacionados com cada uma das componentes (pessoas, processos e tecnologia) e a construção de um "plano de adoção das metodologias necessárias para mitigar o seu impacto". E se, no passado, "este assunto era de imediato delegado para o departamento de IT, atualmente tem de ser visto pelas diversas áreas da empresa", pois os fatores a ter em consideração são muito vastos. Para mapear riscos, as empresas devem começar por responder às seguintes questões: (i) onde está o risco? (ii) de que forma pode afetar o negócio? (iii) qual é o plano de resposta e contingência a implementar? (iv) como difundir a cultura de prevenção do risco por toda em empresa?

Miguel Ramos, consultor sénior técnico da Evonic, salienta que é "necessário consciencializarmo-nos de que não existem sistemas 100% seguros", sendo por isso importante que as empresas sejam tão inovadoras quanto os ataques e riscos a que estão sujeitas". "A conscienciazação dos executivos de topo nas empresas para dar prioridade à segurança é fundamental, assim como a modernização das estruturas de gestão de sistemas de informação e a continua formação de todos os seus colaboradores, aplicando metodologias de gestão de informação e processos adequados", acrescenta. Atualmente, "38% das empresas já separam a gestão de segurança da gestão de IT", uma medida que, em conjunto com o investimento em mecanismos modernos e inteligentes de deteção de intrusão e processos otimizados de resposta e mitigação, "são na nossa opinião, o caminho para a redução drástica das consequências de tais eventos", defende. Para o efeito, recomenda o apoio de consultores qualificados e parceiros tecnológicos especializados "capazes de avaliar o todo na cadeia de produção, armazenamento, processamento e transmissão de dados ", conclui Miguel Ramos, da Evonic.

QUESTÕES REGULAMENTARES INFLUENCIAM PRIORIDADES DE CIBERSEGURANÇA

O RGPD (Regulamento Geral sobre Proteção de Dados) tem levado a que muitas empresas antecipem os seus planos e procedimentos de implementação para estarem em conformidade, "tendo em consideração não só as sanções por incumprimento, como o dano reputacional", refere Andreia Teixeira, diretora de ciber-risco na Aon Portugal.

O RGPD revoga a atual legislação de proteção de dados e entrou em vigor em maio de 2016. No entanto, só será aplicado na íntegra a partir de 25 de maio. Não precisa da transposição para a legislação nacional, mas requer, no entanto, legislação complementar, cuja publicação se aguarda.

Adelino Monteiro, information security na Sage Iberia, diz que este é mesmo "o principal desafio e oportunidade deste ano", obrigando as empresas a "reverem os seus processos internos de tratamento da informação, de forma a focar-se na privacidade dos dados". Será o "grande catalisador que irá sensibilizar os empresários para a importância da segurança e com ele trará muitas oportunidades a bons fornecedores de serviços de segurança, que este ano serão a grande tendência", diz.

No entanto, o panorama pode não ser ainda o melhor. "Um estudo recente da Marsh demonstra que, tendo em conta o esforço necessário, muitas organizações enfrentarão fortes dificuldades para cumprir todos os requisitos até maio. Apenas 8% dos respondentes afirmaram que as suas organizações estão totalmente em conformidade", referiu Carlos Figueiredo, da Marsh. O estudo global da EY é mais positivo, mas, ainda assim, revela que as empresas ainda não estão preparadas para cumprir o RGPD – 78% considera a conformidade em matéria de proteção dos dados e privacidade da informação uma preocupação crescente, no entanto, apenas 33% dos inquiridos tem um plano em curso. Questionado sobre qual seria o panorama em Portugal, Sérgio Sá, da EY, refere que a perceção é de que "está em linha com as conclusões do estudo da União Europeia".

Focada na deteção e prevenção anti-fraude, a SIBS considera que os desafios e oportunidades para este tipo de serviço "são cada vez maiores e em novas áreas", aponta Maria Antónia Saldanha, diretora de marca e comunicação. Em causa está, por um lado, a "pegada digital cada vez maior dos clientes – indivíduos ou empresas". Por outro, "as capacidades e a tecnologia suportam padrões de fraude e cibercrime cada vez mais complexos, sofisticados e à escala global". Destaca, ainda, a "evolução da regulação", cada vez mais exigente para os diversos players: instituições financeiras, comerciantes, organismos públicos e prestadores de serviços de pagamento.

INOVAÇÃO

Check Point anuncia proteção contra nova geração de ciberataques

Futuro passa pela "nanosegurança" embutida nos dispositivos. Empresa apresentou um novo modelo de aquisição, assente num contrato anual e baseado no número de utilizadores.

MAFALDA SIMÕES MONTEIRO *
mmonteiro@jornaleconomico.pt

A Check Point anunciou um novo modelo de subscrição de soluções de cibersegurança durante o encontro anual CPX 2018 Europa, em Barcelona, revelou a sua quinta geração de defesa e antecipa o futuro da cibersegurança que poderá, dentro de cinco anos, passar pela "nanosegurança" embutida nos dispositivos.

O novo modelo de consumo (Infinity Total Protection) permite aos clientes utilizar todas as componentes da arquitetura Check Point Infinity com "custos reduzidos" tendo por base "uma assinatura simples por utilizador e ano", explica a empresa. Nesta assinatura está incluído o acesso ao hardware e software de segurança de rede, proteção para terminais ("endpoints"), clouds e dispositivos móveis. A subscrição abrange ainda a prevenção contra ameaças de "dia zero", juntamente com uma gestão unificada e suporte 24 horas por dia, sete dias por semana. O modelo de subscrição está disponível para clientes atuais e novos.

A arquitetura Check Point Infinity protege os sistemas de informação "tanto de ataques conhecidos como desconhecidos", atuais e no futuro. Além disso, segundo a Check Point, permite também "reduzir custos através da consolidação das componentes de segurança".

A nova arquitetura e modelos de subscrição foram revelados em primeira mão pelo CEO e fundador da empresa, Gil Shwed, durante o encontro anual de clientes e parceiros, CPX 360 – Europa, em Barcelona onde se reuniram cerca de 3000 participantes. O evento repetiu-se dias depois em Las Vegas e terá lugar entre 27 de fevereiro e 1 de março em Banguecoque.

Durante a sessão de abertura, Gil Shwed explicou como funciona a nova geração de ciberataques, a quinta geração ou Gen V. Estes ataques caracterizam-se por ser "de grande dimensão e muito rápidos na forma como evoluem através de redes móveis, da cloud e das redes locais".

Para mitigar este problema, Shwed recomenda a nova solução Infinity que dá resposta "às múltiplas dimensões dos ciberataques atuais ao combinar "a prevenção de ameaças em tempo real, inteligência partilhada e a segurança mais avançada para redes, sistemas móveis e cloud". A Gen V combate os ataques para os quais a deteção estática fica aquém das expetativas, explica.

GIL SHWED
CEO e fundador da Check Point

"A quinta geração de cibersegurança está mais relacionada como o problema do que sobre a solução", disse Maya Horowitz, directora do grupo de "threat intelligence" na Check Point, à margem da conferência, ao Jornal Económico. Segundo a responsável "os ataques agora têm múltiplos vetores. Fazem o que for preciso para atingir os seus objetivos, seja por que meio for, através da cloud ou de dispositivos móveis". A especialista em segurança explica que "a quinta geração se prende com a criação da arquitetura necessária para proteger cada um dos níveis de segurança. "Para nós não é suficiente saber que bloqueamos um ataque de phishing nos PC, porque sabemos que os ataques também podem acontecer através de dispositivos móveis". Por isso, a nova arquitetura "utiliza recursos de inteligência partilhada para criar uma solução holística e mitigar os mega-ataques que surgem".

Gil Shwed aproveitou a ocasião para espreitar o futuro. Depois da atual quinta geração de ameaças, deverá surgir uma nova vaga que poderá tornar-se significativa dentro de cinco anos, antevê. Para o combate aos novos perigos, a "nanosegurança" poderá ser uma solução, integrada em qualquer "dispositivo, web ou serviço na

CPX 360

CIBERSEGURANÇA

Estragos provocados por malware “dependem da criatividade dos hackers”

Cabe a cada entidade proteger os seus sistemas. Especialista diz que um quarto dos ataques recentes explorara vulnerabilidades identificadas há mais de uma década.

nuvem, aplicações e rede, para proteger o mundo hiperligado do futuro”.

Também focado no que aí vem, o futurista e hacker Pablos Holman revelou como é que as estratégias de intrusão que utilizou para se infiltrar na tecnologia, quando se dedicava a atividades menos lícitas, podem ser aplicadas na criação de soluções para desafios globais. ●

** A jornalista viajou ao CPX 360, em Barcelona, a convite da Check Point.*

NOVA GERAÇÃO DE DEFESA

A nova geração de defesa da Check Point abrange, para além da arquitetura Infinity, três dispositivos de segurança Smart-1. Facilitam “o controlo e monitorização da cibersegurança, em toda a empresa, em tempo real, permitindo uma gestão unificada de políticas de segurança, o controlo de acessos avançado e ainda a análise de ameaças”, detalha outro comunicado da empresa.
Os novos dispositivos (Smart-1 525, Smart-1 5050 e Smart-1 5150) têm capacidade de gestão de armazenamento de até 48TB e até 100 mil registos (“logs”) por segundo, mais oito vezes que modelos anteriores, refere a empresa. Com estes dispositivos as equipas de TI têm acesso a uma única consola, holística, de gestão de segurança e conseguem correlacionar, armazenar e analisar enormes quantidades de dados, novos e históricos, de redes com milhares de dispositivos, explica a nota de imprensa.

“Mais de um quarto dos ataques estavam a explorar vulnerabilidades identificadas há mais de 10 anos”, esta é a conclusão de um levantamento realizado pela equipa de “threat intelligence” da Check Point, durante o ano passado, que correlacionou os ataques para os quais a empresa de segurança criou assinaturas, com a data em que as respetivas vulnerabilidades foram identificadas. Maya Horowitz, diretora do grupo de “threat intelligence” na Check Point, assinala que “menos de 10% dos ataques tiraram partido de vulnerabilidades descobertas nos últimos dois anos”.

Esta situação é preocupante, porque significa que as empresas não estão a fazer os trabalhos de casa na proteção dos seus sistemas de informação. “Dizemos sempre que temos de correr atrás dos maus da fita, porque estão sempre um passo à nossa frente, mas afinal estão 10 anos atrás”, ironizou a analista.

Maya alerta que é preciso trabalhar. “A maioria dos ataques que encontramos baseiam-se em vulnerabilidades antigas, em coisas que já estão cobertas por correções dos fabricantes e por soluções de segurança. Isto significa que estes ataques poderiam e deveriam ser evitados, se houvesse mais atenção e tanto particulares como empresas, investissem tempo e dinheiro para se protegerem”.

A recomendação da perita é simples: os sistemas têm de estar atualizados e os administradores de redes, atentos. Referindo-se às botnet de IoT, “os ataques têm ocorrido em câmaras ou “routers” domésticos, mas podem acontecer em qualquer dispositivo IoT. É preciso tirar tempo para proteger os sistemas”, observa. E recorda: “o mais recente ataque IoT afetou 30% das redes em todo o mundo”.

Ainda assim, a mensagem de Maya é tranquilizadora até porque, “a maioria dos ataques são simples” e de fácil resolução, pois passam “passa pela “reciclagem de ataques antigos”.

Principais vulnerabilidades de 2017

Maya recorda que em 2017, as duas principais tendências identificadas pela empresa foram o o uso sem consentimento de máquinas para extracção de criptomoedas e as já referidas botnets de IoT. Uma terceira tendência é a proliferação de ransomware, “mas isso já são notícias velhas”, referiu.

No caso da “mineração” de criptomoeda, o malware tira partido do poder de computação e dos recursos de eletricidade da vítima, através de vários métodos usando cloud computing, os browsers ou “Web Services”. De acordo com Maya Horowitz, este tipo de ataques “está a tornar-se cada vez mais complexo e sofisticado”.

Relativamente às botnets associadas a dispositivos de IoT, Horowitz refere que foram identificados “muitíssimos ataques diferentes que tiram partido de vulnerabilidades de dispositivos de IoT como câmaras e routers domésticos”. Segundo a responsável, este malware baseia-se na botnet Mirai, usada para um “ataque de negação de serviço (DDoS) de larga escala que mandou abaixo a Internet há cerca de ano e meio”. Maya refere que “o código foi publicado online” e agora “qualquer cibercriminoso o pode adaptar para fazer ataques mais sofisticados”. A ofensiva original “usava apenas as credenciais por defeito para atacar. Os novos ataques irão explorar outras vulnerabilidades o que significa que ainda se poderá propagar mais e fazer mais estragos”.

Que tipo de estragos? “Depende da criatividade dos hackers”, afirma Maya Horowits. “Como são dispositivos pequenos e com poucas funcionalidades, podem atingir todo o mundo e criar o caos, como fez a Mirai”. Mas, pode ser um DDoS “segmentado e direcionado a determinada região ou indústria”. Como vemos com o ransomware, podem ser só hospitais ou toda a Ucrânia.

MAYA HOROWITZ
Directora do grupo de “threat intelligence” na Check Point

O que faz a Checkpoint quando identifica uma vulnerabilidade?

“Assim que identificamos uma vulnerabilidade, começamos por bloquear, com a nossa ‘gateway’, os ataques nos nossos clientes. Em seguida analisamos o que se passa, que tipo de ataques estão a acontecer e adicionamos as assinaturas [de software nocivo] aos produtos da Check Point”, explica Maya. Depois “procuramos mitigar o ataque a uma escala global”.

Protegidos os clientes, a Check Point avisa e envia os dados técnicos para os fabricantes dos dispositivos vulneráveis para que possam tomar medidas. “Honestamente, alguns estão bastante relutantes em desenvolver atualizações para os seus dispositivos de [IoT]. E mesmo que o fizessem é muito difícil aos utilizadores domésticos fazer uma atualização de um dispositivo de IoT. A maioria dos utilizadores nem iria tentar”. Maya considera que, no futuro, poderá existir uma solução que passe por atualizações em segundo plano, sem o utilizador se aperceber, como já acontece com os browsers. “De outro modo, as vulnerabilidades não serão colmatadas”.

Em seguida, e após a correção por parte do fabricante, a Check Point procura “criar awareness”, divulgando informação junto dos utilizadores por diferentes meios. “A imprensa, por exemplo, é importante nesta matéria, pois pode informar as pessoas por exemplo sobre a necessidade de proteger os equipamentos de IoT”. A divulgação de casos concretos só deve ser feita após a criação das correcções. “Caso contrário, apenas estaremos a dar ideias aos hackers”, assinala Maya. ● *MSM*

O SEU SISTEMA ESTÁ A MINERAR CRIPTOMOEDAS?

A Check Point detetou um incremento no malware relacionado com a “mineração” ilegal de criptomoedas, no segundo semestre de 2017. Segundo o relatório “H2 2017 Global Threat Intelligence Trends report”, os cibercriminosos estão a virar-se cada vez mais para a cripto-mineração para criar fluxos de receitas ilegais, enquanto o ransomware (software que pede resgates para libertar os dados raptados) e o adware “malvertising” (adware que propaga malware através anúncios de publicidade, aparentemente inofensivos) continuam a ter um forte impacto nas organizações à escala mundial.
De acordo com empresa de segurança, entre julho e dezembro de 2017, uma em cada cinco organizações foi infetada com malware de “criptomineração”, ferramentas que “tomam conta” de parte da capacidade de processamento e outros recursos para extrair criptomoedas, utilizando para o efeito até 65% do poder de computação das máquinas dos utilizadores finais.

ICG

David Baltazar, fundador e CEO da ICG Portugal e Angola

EMPRESAS

Soluções da ICG evoluem para 'cloud computing'

As plataformas tradicionais da empresa do Porto, para a restauração e hotelaria, estão a ficar disponíveis "as a service" e chegam também aos dispositivos móveis.

MAFALDA SIMÕES MONTEIRO *
mmonteiro@jornaleconomico.pt

A ICG, uma empresa que acumula três décadas de experiência em soluções de software para os segmentos de restauração, retalho e hotelaria, agilizou os processos de desenvolvimento e localização da sua oferta. Está a fornecer soluções "as a Service" e assentes na mobilidade.

A empresa do Porto está a abrir um escritório em Lisboa, para poder responder com mais eficácia e eficiência às solicitações do mercado abaixo de Coimbra.

Em 2018, a empresa quer colocar no mercado novas plataformas tecnológicas, incluindo soluções cloud e assentes na mobilidade, ao mesmo tempo que apresentar uma nova política de parcerias com empresas de TI que comercializam as soluções do fabricante.

Durante 2017, a subsidiária portuguesa, incluindo a sucursal de Angola, apresentou um volume de negócios de 1,5 milhões de euros. No corrente ano, esse volume deverá aumentar 20%, disse David Baltazar, fundador e CEO da ICG Portugal e Angola, em resposta a questões colocadas pelo Jornal Económico. Cerca de 10% do volume de negócios tem como destino a investigação e desenvolvimento.

Com 18 colaboradores, a ICG Portugal vai ainda abrir um escritório em Lisboa, porque "grande parte da nossa faturação é de Coimbra para baixo" e Lisboa "ainda é um grande centro de decisão no nosso mercado alvo". A abertura das novas instalações está relacionada com "a necessidade de proximidade" e "os custos diretos e indiretos" associados, assinalou David Baltazar.

Este ano, em matéria de produtos, a empresa está a apresentar as novas plataformas ICG Hiopos Cloud, que "têm capacidade de integração com praticamente qualquer solução que possa incorporar dados de aplicações externas, que são a grande maioria", explica David Baltazar. A empresa vai também continuar a trabalhar na "evolução das plataformas tradicionais", tendo como grande aposta as tecnologias para Android. "A abertura das plataformas de pagamento também nos vai permitir abraçar outros projetos nesta área, mas a tecnologia de base será Android", acrescenta o fundador.

Agilização do desenvolvimento

Globalmente, a empresa reformulou recentemente os métodos de desenvolvimento para conseguir acompanhar a evolução do mercado, incluindo as alterações legais de cada uma das geografias em que opera. Anteriormente a ICG não conseguia dar resposta a essas alterações, o que acabava por se traduzir em atrasos no desenvolvimento e colocação no mercado das atualizações. "Os atrasos foram provocados pela estratégia de desenvolvimento toda centralizada na nossa fábrica em Lleida. A quantidade de localizações, muitas vezes em simultâneo, para as várias regiões mundiais acabava por criar um funil apertado que acabava por fazer derrapar os prazos ótimos, recorda David Baltazar. Este problema "foi completamente ultrapassado com as concessões mundiais a ficarem responsáveis pelas localizações, o que já é uma realidade". Deste modo, acrescenta, "as especificidades de cada país, sejam fiscais, prioridades operacionais ou mesmo integrações com terminais bancários, sistemas de TX FREE, etc. passaram a depender exclusivamente da representação local da marca". Neste âmbito, a ICG Portugal criou a marca Mob Youzit. A título de exemplo. David Baltazar refere que "não faz sentido que estejamos em Portugal a desenvolver verticais que por ventura já tenham sido desenvolvidos no México ou vice-versa".

RESTAURANTE "O POKE" ADOTA NOVA SOLUÇÃO DE FATURAÇÃO

"O Poke", restaurante do chef Kiko no El Corte inglés em Lisboa, adotou o software de faturação da ICG. Pedro Inácio, diretor de unidades de negócio da Comer o Mundo, explica que a empresa utilizava, até a agora, outro software e que, com a abertura de um espaço no El Corte Inglés, tomou contacto com o sistema de informação da ICG. Este sistema é parte integrante dos sistemas daquela unidade comercial pelo que o restaurante teve de adotar.

O maior problema que o restaurante enfrentou com esta mudança tecnológica foi a resistência à mudança, uma vez que a empresa sempre operou com outro sistema. Também encontraram constrangimentos na "divisão de faturas e números de contribuinte num único documento", situações que foram prontamente resolvidas pela ICG.

Para já, o único ponto de venda do chef Kiko que utiliza a solução da ICG é o "O Poke".

BREVES

SIBS e IBM unem-se no combate à fraude

A SIBS e a IBM firmaram recentemente uma parceria estratégica para o desenvolvimento de uma solução cognitiva end-to--end de monitorização, deteção, interceção e investigação de fraude em pagamentos, em tempo--real, num modelo "as-a--service", que agrega o know-how e procedimentos de segurança e anti--fraude da SIBS com a tecnologia cognitiva com base no Watson da IBM. O serviço de monitorização, prevenção e deteção de fraude Paywatch visa "detetar e evitar atividades fraudulentas sofisticadas por forma a reduzir o prejuízo decorrente de fraude e proporcionar maior confiança aos consumidores nas suas transações". As empresas pretendem com esta parceria conquistar novos clientes na Europa e em África.

RGPD: empresas desconhecem novos requisitos da lei

Faltam pouco mais de três meses para que o Regulamento Geral de Proteção de Dados seja aplicado na íntegra. No entanto, a grande maioria das empresas portuguesas não está a postos. Apenas 2,5% dos decisores considera que a sua organização está preparada para lidar com o regulamento, de acordo com um estudo da IDC/Microsoft.

A situação é menos grave nas organizações com mais de 250 colaboradores. Segundo os dados recolhidos pela IDC/Microsoft no início do mês de janeiro, neste segmento, "mais de 50% dos decisores conhece 'relativamente bem' o regulamento".

"As conclusões não são especialmente animadoras", assinala André Azevedo, diretor executivo de tecnologia da Microsoft Portugal, acrescentando que "há um longo caminho a percorrer em pouco tempo".