manchete

Jornal Económico
ET CETERA
02-06-2017

Periodicidade: Semanário
Classe: Economia/Negócios
Âmbito: Nacional
Tiragem: 20000
Temática: Tecnologia
Dimensão: 3734 cm²
Imagem: N/PB
Página (s): 4 a 7

ATUALIDADE

CIBERCRIME
Como os 'hackers' estão a ameaçar a economia mundial

Os custos do cibercrime serão de 2,1 triliões de dólares até 2019, o equivalente a três por cento do PIB mundial. As consequências de um ataque cibernético para as empresas são devastadoras e, ainda há uma semana, mais de 200 mil computadores de 150 países foram afetados por um vírus. Os hackers revelam técnicas sofisticadas: estudam os mercados financeiros para conseguirem o máximo impacto negativo possível com um ataque.

ANTÓNIO SARMENTO
asarmento@jornaleconomico.pt

Kevin Mitnick, o pirata informático mais famoso do mundo, vale ouro para as empresas: passou de 'hacker' a consultor, escreve livros e palestras. Sabe quase tudo para evitar um ataque de pirataria informática. Depois de ter estado preso durante cinco anos gosta de se vestir com uma t-shirt preta onde ser pode ler "I'm not a 'hacker', I'm a security professional" – não sou um 'hacker', sou um profissional de segurança. Em 1990, conseguiu invadir os servidores de várias empresas americanas e enganou o FBI até ser capturado.

A vocação começou cedo. Nos anos 70, com 16 anos, entrou no computador da escola e alterou as suas notas. Só depois de ter caído na armadilha de Tsutomu Shimomura, especialista em segurança do Centro Nacional de Supercomputação em São Diego, Califórnia, foi detido. Shimomura trocou mensagens com Mitnick até que as autoridades norte-americanas monitorizaram a origem.

A origem do termo 'hacker' vem dos anos 50 e 60, quando o termo significava apenas uma solução inspirada ou elegante para qualquer problema. Ao longo do tempo, o nome ficou associado a programadores que começavam a ganhar espaço no Massachussetts Institute of Technology (MIT) e em outras partes do mundo. Os feitos eram admirados por combinarem conhecimento e instinto criativo.

Entretanto, estes grupos começaram a adoptar nomes como 'Legion of Doom', 'Masters of Deception', 'Neon Knights' ou 'Anonymous'. À medida que a sofisticação destes piratas informáticos foi aumentando eles começaram a entrar no radar das autoridades. Nos anos 80 e 90, foram aprovadas leis que passaram a permitir levá-los a tribunal, mas a escala dos ataques foi em crescendo.

Na semana passada, um ataque cibernético em larga escala afetou mais de 200 mil computadores em 150 países, incluindo Portugal. Várias empresas, hospitais e até mesmo agências governamentais tiveram de suspender total ou parcialmente as suas operações depois de ser infectadas pelo vírus. A gigante espanhola Telefónica foi infectada e, em Inglaterra, o Ministério Nacional de Saúde confirmou que diversos hospitais foram atacados em simultâneo, obrigando os doentes a serem transferidos para outros serviços. "É o maior ataque desta natureza que vejo nos seis anos em que trabalho para o Ministério", referiu um técnico informático ao "The Guardian".

O que os ataques fazem às empresas

Entre 2013 e 2015, os custos do cibercrime quadruplicaram e prevê-se que aumentem na mesma medida nos próximos anos. Segundo um estudo da Juniper, empresa de tecnologias de informação, a fatura deste tipo de crime deverá atingir os 2,1 triliões de dólares até 2019. Este valor equivale a perto de três por cento do PIB mundial.

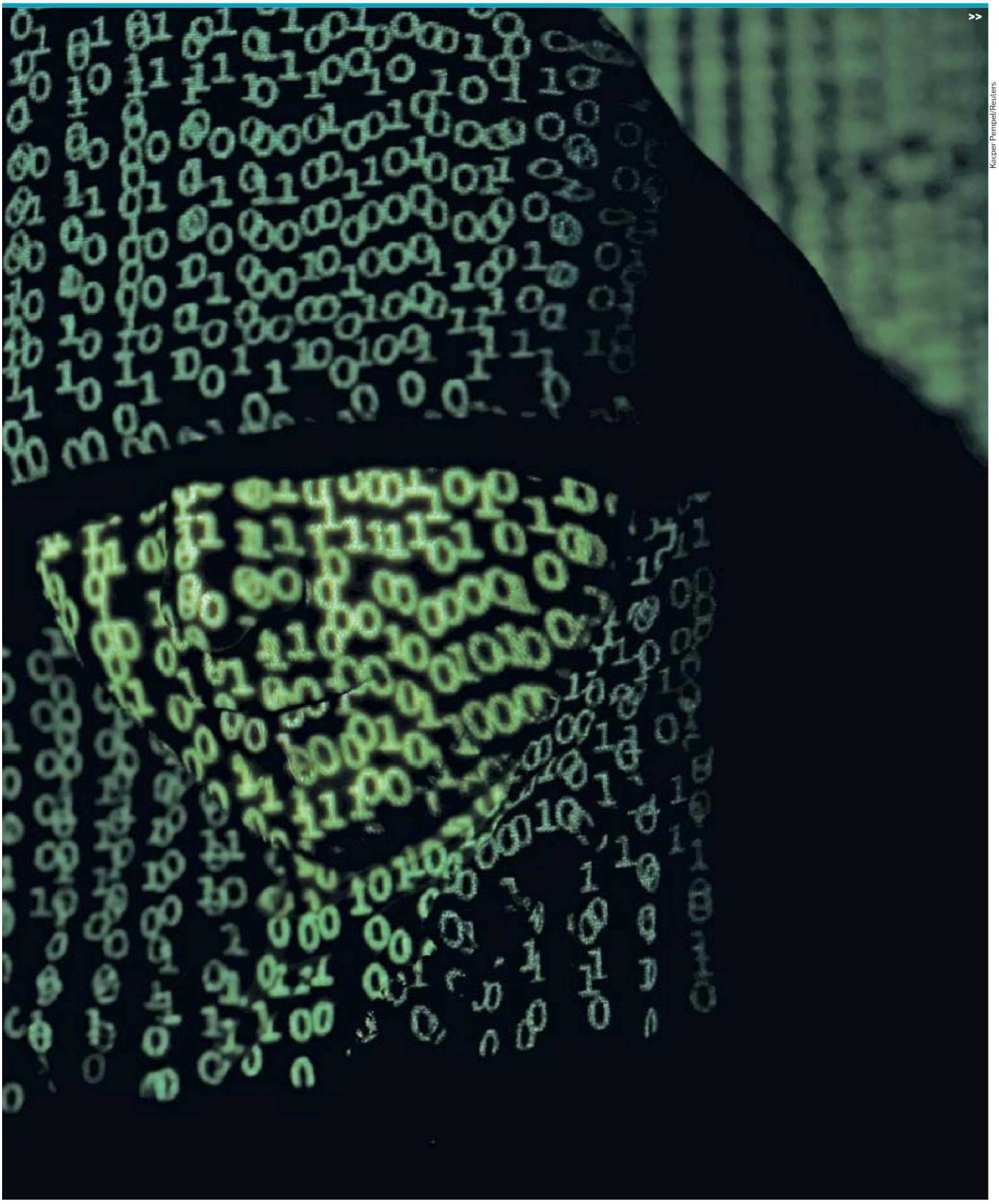
A projeção feita pela Juniper segue a linha de avaliações feitas por outras instituições. Por exemplo, a seguradora britânica Lloyds calcula o custo atual do cibercrime em 400 milhões de dólares, número que tem crescido de ano para ano. O mercado de produtos e serviços de segurança sobe também para acompanhar esta procura, passando dos 75 mil milhões de dólares em 2015 para 175 mil milhões em 2020.

Recentemente foi publicado o relatório da atividade do Gabinete Cibercrime referente ao período entre setembro 2015 e dezembro de 2016. Das informações disponibilizadas, destaque para o facto de Portugal ter feito oito mil pedidos ao Facebook, Microsoft e Google para ajudar a combater o Cibercrime. No total foram feitos 8267 pedidos pelas autoridades portuguesas aos gigantes Facebook, Microsoft e Google para conseguirem obter provas nalguns casos de suspeitas de cibercrime, como por exemplo, vendas online fraudulentas, roubos de identidade, criação de perfis falsos no Facebook ou 'phishing' bancário.

manchete

Jornal Económico
ET CETERA
02-06-2017

Periodicidade: Semanário
Classe: Economia/Negócios
Âmbito: Nacional
Tiragem: 20000
Temática: Tecnologia
Dimensão: 3734 cm²
Imagem: N/PB
Página (s): 4 a 7

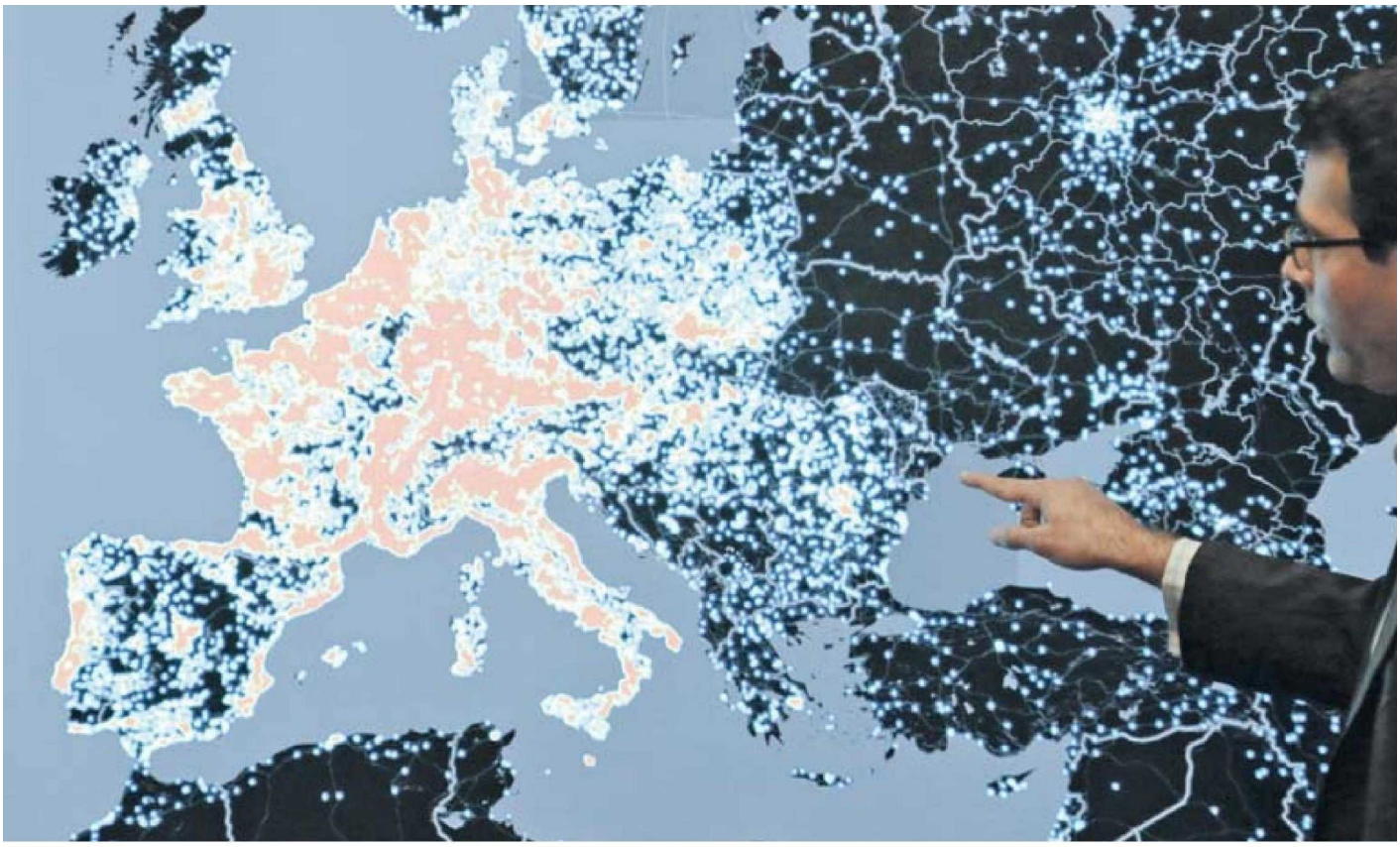


Kacper Pempel/Reuters

manchete

Jornal Económico
ET CETERA
02-06-2017

Periodicidade: Semanário
Classe: Economia/Negócios
Âmbito: Nacional
Tiragem: 20000
Temática: Tecnologia
Dimensão: 3734 cm²
Imagem: N/PB
Página (s): 4 a 7



No geral as empresas não se recusaram a colaborar mas o relatório revela que "há margem para melhorar a eficácia nos procedimentos, uma vez que nalguns casos, a percentagem de pedidos que não têm resposta satisfatória dos operadores é significativa".

Depois do ataque da semana passada, a multinacional de tecnologia Microsoft foi alvo de duras críticas ao saber-se que a empresa se terá recusado a distribuir uma reparação gratuita para as versões mais antigas do sistema operativo Windows, que poderia ter parado o ciberataque da semana passada com o vírus WannaCry. Ao invés disso, a Microsoft colocou o patch à venda por mil dólares (cerca de 900 euros) por ano.

Em declarações ao jornal britânico 'Financial Times', Michael Cherry, analista da empresa de pesquisa independente Directions on Microsoft, critica as políticas adotadas pela multinacional, que com a recusa em fornecer cibersegurança para versões mais antigas do Windows, pretende obrigar os clientes a comprarem softwares mais novos e mais seguros.

O vírus WannaCry trata-se de um 'ransomware', uma espécie de 'software' que rouba arquivos de um computador para depois pedir aos seus utilizadores o 'resgate' em dinheiro. Os computadores ficaram inacessíveis, exibindo uma mensagem a pedir resgate em 'bitcoins' no valor de 600 dólares (cerca de 540 euros).

As consequências de um ataque cibernético para as empresas são devastadores.

O vírus WannaCry trata-se de um 'ransomware', uma espécie de 'software' que rouba arquivos de um computador para depois pedir aos seus utilizadores o 'resgate' em dinheiro

"Por um lado existem os danos próprios e, portanto, o impacto financeiro devido à interrupção desse mesmo negócio e todos os custos associados à normalização da atividade. Deve recorrer-se a especialistas quer da área de IT, quer da área jurídica para travar os efeitos do mesmo", explicou Ana Marques, responsável pela área de Cyber Risks da Marsh Portugal, ao Jornal Económico.

Ao nível da prevenção, esta especialista acrescenta que "as empresas têm de colocar a cibersegurança no topo das suas agendas e têm de incluir todos os órgãos da empresa, não só o IT, mas também os administradores, departamento jurídico e departamento financeiro. As empresas têm de estar conscientes da crescente pressão do legislador europeu tanto a nível da proteção de dados como da cibersegurança".

A transferência do risco para o mercado segurador, através do qual esta solução cobrirá parte dos risco de um ataque cibernético, é uma das soluções aconselhadas.

Estudar a bolsa para atacar

A queda dos mercados bolsistas tem um impacto direto no aumento do crime económico efetuado através da internet. Em 2008, no pico da crise financeira mundial, o PandaLabs, da marca de antivírus Panda Security, lançou um alerta de segurança que revelou uma correlação directa entre a volatilidade do mercado bolsista e o aumento do aparecimento de novas ameaças.

De acordo com o PandaLabs, "ambos estão

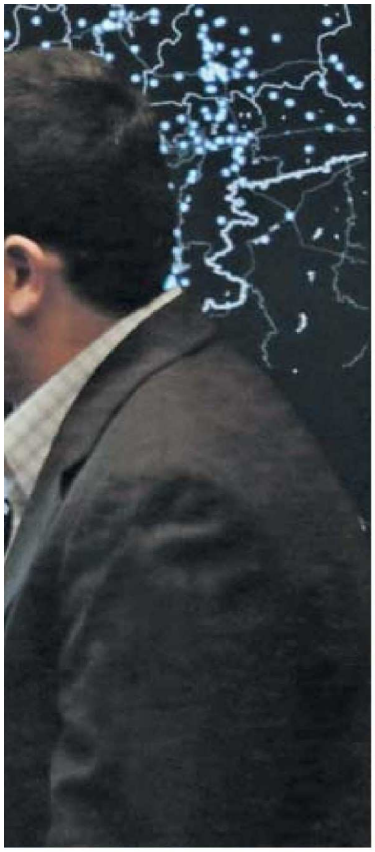
DICAS PARA EVITAR UM ATAQUE

- Ter instalado no computador um programa antivírus ou anti-spyware
- Não transportar na carteira palavras-passe ou códigos PIN, ou guardar estes dados num ficheiro desprotegido
- Não utilizar informações de fácil acesso na criação de palavras-passe, como a data de nascimento, o nome da mãe ou do animal de estimação
- Proceder às actualizações dos programas antivírus e outros instalados no computador
- Não usar ligações wi-fi grátis
- Activar as opções relacionadas com a privacidade ou manter um perfil muito acessível

manchete

Jornal Económico
ET CETERA
02-06-2017

Periodicidade: Semanário
Classe: Economia/Negócios
Âmbito: Nacional
Tiragem: 20000
Temática: Tecnologia
Dimensão: 3734 cm²
Imagem: N/PB
Página (s): 4 a 7



Jason Redmond/Reuters

muito mais interligados do que se previa e a recente instabilidade nas Bolsas acelerou o volume de ciberataques direccionados e o seu impacto relativo na economia", referiram em comunicado.

"Baseados na nossa pesquisa e análise extensivas acreditamos que as organizações criminosas observam de perto o desempenho dos mercados e adaptam-se às suas necessidades para assegurar a máxima rentabilidade".

O departamento de segurança informática da IBM publicou recentemente os resultados do estudo IBM X-Force Threat Intelligence Index, onde se revela que em 2016 houve um aumento histórico no número de dados informáticos comprometidos: qualquer coisa como 566%, uma subida de 600 milhões para quatro mil milhões. O email não desejado (spam) aumentou em 400% e os Serviços Financeiros são os mais atacados.

"Os cibercriminosos continuaram a inovar em 2016, já que vemos técnicas como o ransomware moverem-se de um incómodo para uma epidemia", afirmou Caleb Barlow, vice-presidente de Threat Intelligence da IBM Security, em comunicado.

Segundos dados divulgados também pela IBM no final de 2016, 70% dos negócios que sofrem ataques de 'ransomware' pagaram mais de 10 mil dólares para recuperarem o controlo dos seus equipamentos. Só nos primeiros três meses de 2016, o FBI estimou um lucro de 209 milhões para os atacantes, resultando num total de quase mil milhões ao fim do ano.