manchete

OJE

01-04-2016

Periodicidade: Diário
Classe: Economia/Negócios
Âmbito: Nacional
Tiragem: 11000

Temática: Tecnologia
Dimensão: 1277
Imagem: S/Cor
Página (s): 18

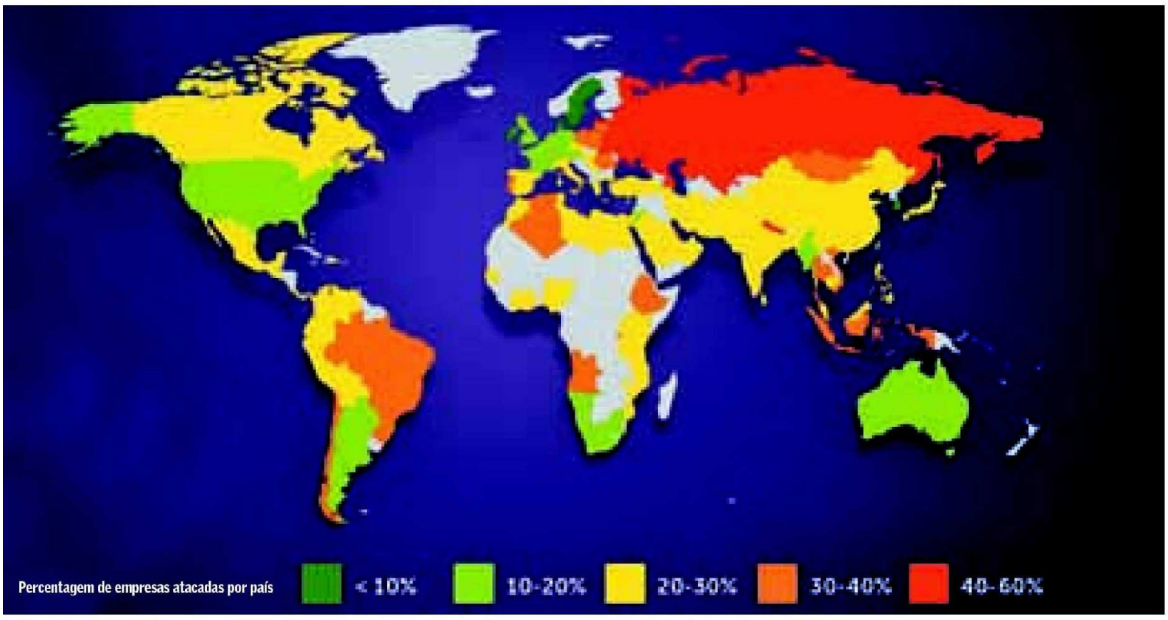
maistic

COORDENAÇÃO EDITORIAL E TEXTOS DE MAFALDA SIMÕES MONTEIRO

CIBERSEGURANÇA

A sua empresa está preparada para o ataque?

Os prejuízos provocados pelo cibercrime são avultados. O investimento em sistemas de cibersegurança também. Esta bola de neve vai continuar a crescer. A questão não é se. É quando se vai ser atacado.



Atualmente, as empresas estão melhor preparadas, têm processos e políticas mais bem definidas, mas ainda existe muita insegurança ao nível dos sistemas de informação, em particular nas empresas de menor dimensão.

De acordo com o relatório anual de segurança da Cisco, "apenas 45% das empresas confiam na sua estratégia de segurança para fazer face a ciberataques cada vez mais sofisticados, ousados e persistentes". E o panorama é tudo menos estático.

Segundo a McAfee, o número de ataques informáticos aumentou 60% em apenas dois trimestres e a Kaspersky Labs refere que, em 2015, 58% dos computadores das empresas sofreram, pelo menos uma vez, uma tentativa de infeção por malware. A Siemens estima que os custos associados ao cibercrime, rondem os 400 mil milhões de dólares (cerca de 357 mil milhões de euros).

Também o número de dispositivos móveis está a aumentar. A Cisco aponta para que, em 2020, existam 5500 milhões de utilizadores móveis à escala global, o equivalente a 70% da população mundial.

Estes dados confirmam a necessidade de proteger as infraestruturas de TI das empresas e prometem não facilitar a vida aos especialistas em segurança.

> Em finais de 2016, 70% dos departamentos de TI vão abandonar a abordagem centrada na proteção e defesa do perímetro e adotar novas abordagens de contenção e controlo
> IDC

SEGURANÇA. UMA PRIORIDADE

A segurança é "um tema cada vez mais relevante naquilo que é a realidade do digital", sublinha o diretor-geral da IDC, Gabriel Coimbra. O analista assinala que a atual "transformação digital (em curso) coloca um peso muito maior na segurança", que está por seu lado a ser alvo de uma mudança de paradigma. De acordo com as previsões da IDC, "em finais de 2016, 70% dos departamentos de TI vão abandonar a abordagem centrada na proteção e defesa do perímetro e adotar novas abordagens de contenção e controlo". Gabriel Coimbra assinala que "o cerne da questão não é propriamente defender a organização e garantir que não sofre nenhum ataque. O importante é assegurar que a organização está preparada para responder aos vários ataques que têm acontecido, vão continuar a acontecer e vão aumentar no futuro. Em síntese: o ataque é inevitável. Por isso importa saber "como é que vamos responder ou lidar com esses ataques".

Para a Siemens a segurança e o combate à pirataria informática são uma prioridade. Para o efeito a tecnológica coopera com empresas de segurança e com mais de 200 organizações ligadas à segurança a nível mundial, disse fonte da Siemens ao OJE. Em causa está a mitigação do impacto do cibercrime. Para fazer face a este problema, em 2015, a Siemens gastou cerca de 4,4 mil milhões de euros em investigação e desenvolvimento, mais 400 milhões que no ano anterior, com a maior verba dedicada a projetos da área digital. Por seu lado, fonte a OpenSoft explica que a transformação digital, em particular a mobilidade associada à tendência Bring Your Own Device (BYOD) são uma "potencial dor de cabeça para o Chief Security Officer (CSO)". A afirmação é de Ricardo Caetano, diretor de Desenvolvimento de Sistemas de Informação do integrador, que assinala que os principais fabricantes de software estão a adquirir empresas nesta área, com vista a disponibilizar rapidamente soluções abrangentes. "No entanto, do ponto de vista das arquiteturas de software, ainda não existem padrões de desenho standard para esta temática". Relativamente à segurança dos dados na cloud tudo "está mais controlado". Os service providers estão alinhados com os seus clientes e têm tanto a perder caso ocorra uma falha de segurança como quem adquire o serviço. declara Ricardo Caetano.

Proteger as redes das empresas, onde se armazena e transmite todo o tipo de informação, incluindo confidencial, "é imprescindível", explica Alfonso Ramírez, diretor-geral da Kaspersky Lab. Os estudos apontam para que os cibercriminosos se concentrem cada vez mais em alvos financeiros, obrigando as empresas a proteger-se. Todas as organizações são alvos potenciais e enfrentam riscos semelhantes, mas um estudo da Kaspersky Lab e da B2B International revela que só 19% das empresas com menos de 25 colaboradores coloca a estratégia de TI, que inclui a segurança informática, no topo das suas preocupações", refere Ramirez. "É inquestionável que as empresas mais pequenas sofrem mais com as limitações orçamentais, optando muitas vezes por adotar soluções inadequadas às suas necessidades", no entanto, estão a colocar outros em risco, pois ao descurar a segurança podem estar a ser a porta de entrada para sistemas maiores e mais complexos.

Por todos estes motivos, a cibersegurança tem de ser uma preocupação dos utilizadores de sistemas de informação: "uma vez que os sistemas de informação estão cada vez mais interligados ao exterior", explicou Rui Gaspar, diretor de Base de Dados, Tecnologia e Analytics da SAP em Portugal, responsável pela área de negócio SAP HANA e o SAP Business suite S/4HANA. Questionado sobre as principais questões de segurança colocadas pelos utilizadores das novas soluções da SAP, Rui Gaspar, explica que estas se prendem essencialmente com matérias "processuais e de governação de dados para garantir que estes não são indevidamente utilizados".

Para salvaguardar os sistemas de informação, os clientes devem recorrer a "auditorias de segurança efetuadas por uma entidade terceira", diz Ricardo Caetano, da Opensoft. O integrador de sistemas de informação explica que "uma entidade auditora competente emite relatórios compreensíveis e completos que permitem identificar qual a anomalia, a criticidade, avaliar mecanismos para colmatar falhas de segurança potenciais ou constatadas e reportar as ações efetuadas ao cliente para serem validadas em nova auditoria", explica. Ricardo Caetano.

Daqui para a frente, Gabriel Coimbra recorda que estão a desenvolver-se novas tecnologias que vão assegurar uma maior segurança na terceira plataforma de tecnologia: a encriptação e a biometria. "São duas áreas que vão mudar completamente a forma como as soluções tecnológicas de segurança são desenvolvidas", conclui.