JE MAIS TIC

Cibersegurança é vital para garantir a continuidade dos negócios

MAFALDA SIMÕES MONTEIRO
mmonteiro@jornaleconomico.pt

O negócio da segurança está em crescimento acelerado. Só em Portugal, segundo Gabriel Coimbra, da IDC, o valor do mercado de segurança deverá crescer cerca de 39% entre 2017 e 2022, passando de um valor de 130 milhões de euros para cerca de 181 milhões. Os serviços de segurança terão um crescimento médio anual de 9%, enquanto o crescimento médio anual (CAGR) de software e o hardware deverá rondar os 7% e 2% respetivamente.

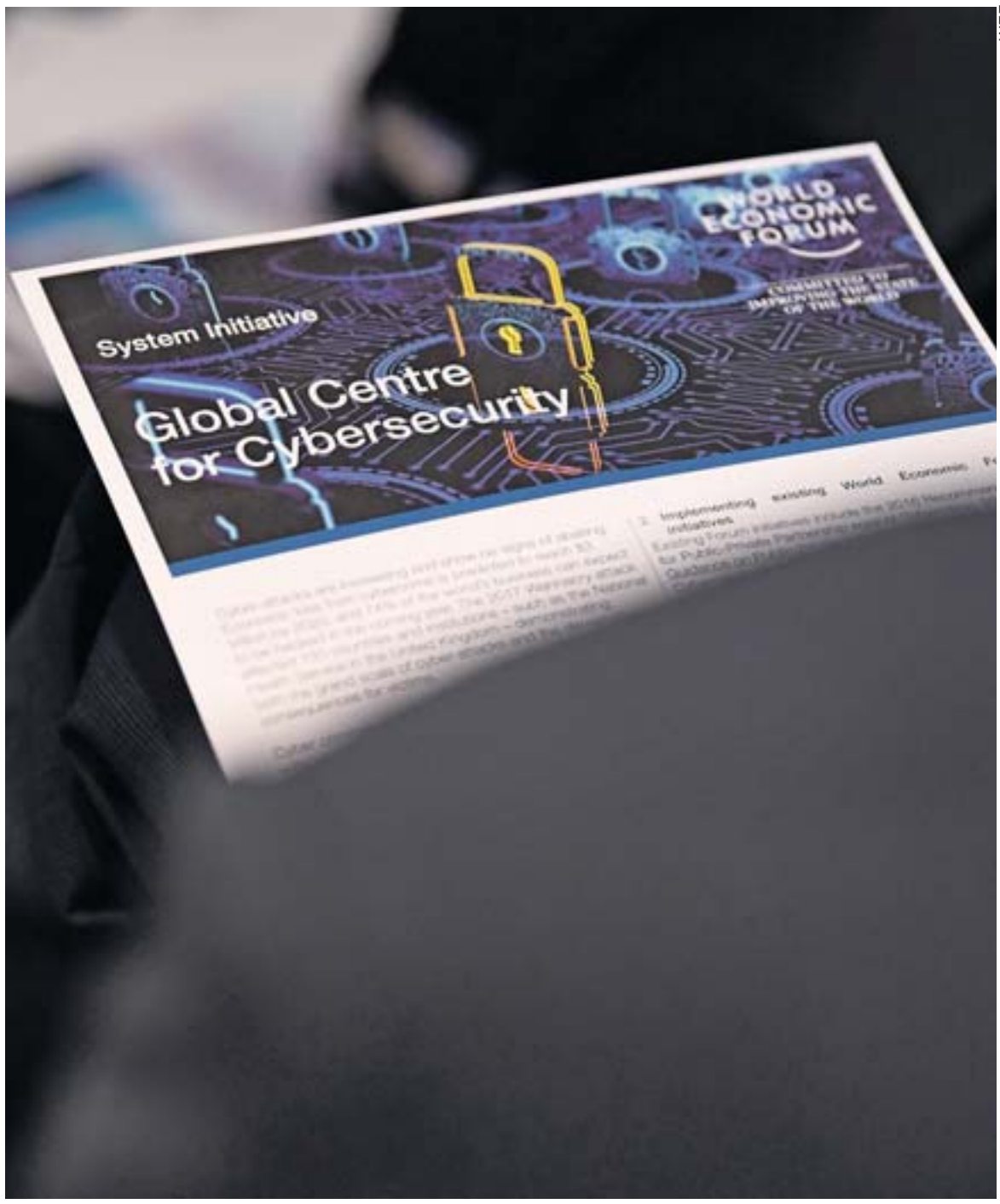
Este crescimento está relacionado, por exemplo, com a quantidade de dados existente que "é dificilmente imaginável" e cujo "crescimento é contínuo", disse Rita Mourinha da Seresco ao Jornal Económico. Nessa imensidão que é o mundo dos dados, as empresas gastam milhões para tentarem proteger-se dos ataques que chovem em catadupa e que são cada vez mais sofisticados. "Os custos associados às perdas inerentes de acesso [não autorizado] aos dados (ransomware), como à exposição da informação confidencial nos atuais quadros legais do RGPD é incalculável", explica Aragão Rio, da Dell EMC.

Alvos potenciais são todas as empresas que guardam dados pessoais ou confidenciais, como números de identificação pessoal, palavras-passe e qualquer tipo de informação sensível, mas, um pouco mais na linha da frente devido à especificidade da sua atividade, estão as empresas de comércio eletrónico. "As transações realizadas em sites de comércio eletrónico exigem a troca de dados confidenciais que podem ser comprometidos a qualquer momento se as empresas não tiverem a proteção adequada", refere Aurélio Duarte, da Amen.pt.

O risco abrange de igual modo, empresas grandes, empresas pequenas e empresas muito pequenas e todas elas deverão encará-lo da mesma forma. "Um dos desafios é que a segurança seja vista como uma prioridade e não como um custo, trazendo oportunidades a novas soluções menos complexas e mais adaptadas às necessidades das organizações", adianta Sónia Casaca, Business Unit Manager – Security da Arrow ECS.

Na linha de prioridades, o importante é encontrar o nível de proteção adequado. Como vinca João Martins, administrador da Cilnet: "conseguirmos definir diferentes níveis de proteção e de acesso à informação". Os milhões de transações realizadas por minuto em todo o mundo que vão desde uma simples compra, à folha de ordenado de qualquer um de nós, precisam ser validadas. Tal como António Espingardeiro, consultor KCS iT, Ricardo Dinis, Diretor ITS da Agap2IT evidencia a importância do uso de aprendizagem automática (ML), ramo da IA, para a automatização da deteção e resposta de ataques. O uso desta ferramenta "retira esse fardo aos humanos", sublinha.

Se para João Barreto Fernandes, da S21sec Portugal, a prioridade deve ser a gestão massiva de dados, Adelino Monteiro da Sage considera que a cibersegurança deve adaptar-se. "É crucial arquitetar uma solução de cibersegurança que se adapte dinamicamente à necessária constante mudança".



WEF

OPINIÃO

‘ML’, uma arma na identificação das ameaças

RICARDO DINIS
Diretor ITS, Agap2IT

A cibersegurança tornou-se uma prioridade para todas as organizações. O número de ataques está na ordem dos milhares de milhões e o crescimento previsto é exponencial.

Os produtos de segurança atuais focam-se em perceber como funciona um malware ou um ataque e, na sua maioria, operam na prevenção de intrusão.

Trata-se de um contexto em que os atacantes só precisam de acertar uma vez, mas as equipas de segurança das organizações têm de acertar constantemente. Na prática, as organizações estão sempre um passo atrás dos atacantes.

Nos últimos anos temos visto um crescimento nas tecnologias de inteligência artificial (IA) para as organizações, capazes de responder aos principais desafios do mundo dos negócios. A maior parte delas pode ser atribuída aos avanços no poder computacional, big-data, à computação distribuída e ao uso da Cloud.

O uso de aprendizagem automática (ML), ramo da IA que permite a emulação do cognitivo humano, para a automatização da deteção e resposta de ataques retira esse fardo aos humanos. E será, potencialmente, mais eficiente a identificar as ameaças, do que uma abordagem baseada na análise de comportamentos executada por humanos com a ajuda de software especializado.

Produtos de ciber-deteção e implementações de segurança multicamada baseados em IA, criam incerteza para os atacantes e podem, de uma forma automática, detetar, analisar e defender contra os ataques avançados detetando e enganando os invasores.

Quando se combinam profissionais de segurança com qualidade e capacidade, com tecnologias adaptativas, que mudam e ficam mais inteligentes ao longo do tempo, é criada uma oportunidade de vantagem que não existe nas tecnologias de cibersegurança de hoje em dia.

IA e ML podem oferecer vantagens na proteção de dados sensíveis e sistemas chave. Mas, como qualquer outra inovação, estas tecnologias também estão hoje em dia a ser usadas para alavancar os próprios ataques pelo lado dos hackers do mal.

E o processo de aprendizagem supervisionada, necessário à aprendizagem automática na área da segurança, é ainda suscetível ao erro humano pela possibilidade de catalogar indevidamente o código.

Cria-se uma falsa sensação de segurança, problema que tem sido contornado pelo uso de múltiplos algoritmos e conjuntos de dados, fazendo com que se um algoritmo for comprometido, os resultados dos seus pares irão evidenciar a anomalia.

O desafio primário da cibersegurança para as organizações B2B e B2C tem sido a mudança constante da escala dos ataques. A natureza desta mudança é, no entanto, previsível e segue padrões, o tipo de problema onde o uso de IA e ML se destaca e abre novas oportunidades.

Produtos de ciber--deteção e implementações de segurança multicamada baseadas em IA criam incerteza para os atacantes e podem, de uma forma automática, detetar, analisar e defender contra os ataques avançados detetando e enganando os invasores

ESTUDO DA EY

Colaboradores descuidados são fonte de vulnerabilidades mais perigosas

34% das empresas e organizações inquiridas no âmbito o EY Global Information Security Survey 2018-19 colocam os descuidos internos à cabeça das vulnerabilidades.

MAFALDA SIMÕES MONTEIRO
mmonteiro@jornaleconomico.pt

Um ano depois de várias empresas e organizações mundiais terem sido abaladas por falhas de cibersegurança à escala global, esta questão ganha importância na agenda dos decisores. No entanto, há muito caminho a percorrer, considerando o cada vez maior poderio dos ciberataques, alguns dos quais poderão até ser patrocinadas por Estados. Tudo isto é certo, mas, o EY Global Information Security Survey 2018-19 divulgado esta quarta-feira reconhece que as vulnerabilidades mais perigosas numa empresa ou organização estão relacionadas com colaboradores descuidados (34%).

Em segundo lugar surgem os controlos de segurança ultrapassados (26%), em terceiro, o acesso não autorizado (13%), seguindo-se elementos relacionados com utilização de computação em nuvem (10%).

Apenas 8% referem que as funcionalidades de segurança respondem às suas necessidades e 38% dos inquiridos assumem não conseguirem provavelmente descobrir uma violação de segurança mais sofisticada. De resto, menos

SÉRGIO MARTINS, ASSOCIATE PARTNER DA EY, COMENTA O ESTUDO

As organizações investem cada vez mais em tecnologias emergente como parte dos seus programas de transformação digital e muito embora esses programas tenham criado várias novas possibilidades, foram também responsáveis por novas vulnerabilidades e ameaças. As organizações devem ter presente que a construção de um sólido nível de segurança com os seus clientes é algo crítico para o sucesso dos seus programas de transformação. Para alcançar esta confiança, é necessário que a cibersegurança faça parte do ADN da organização, algo que começa com a sua inclusão na estratégia de negócio. (…)
Acreditamos que a confiança será o pilar do futuro digital, e é aqui que o valor para o negócio será gerado. Para conseguirmos chegar a este ponto, as organizações têm de abandonar a abordagem de pensamento em silos e pensar na cibersegurança como uma questão transversal para implementarem security-by--design.
Desta forma conseguiremos aumentar a ciber-resiliência para dotarmos as organizações da confiança necessária para aproveitarem as oportunidades emergentes e gerirem os ciber-riscos.

de 10% acreditam que têm sistemas de segurança com elevado nível de maturidade.

No entanto, muitas organizações (82%) não sabem se estão a identificar com sucesso falhas de segurança e incidentes. Entre as organizações que foram alvo de algum incidente no último ano, menos de um terço (31%) diz que o incidente foi descoberto pelo seu próprio centro de operações de segurança.

Para garantir a segurança no ciberespaço são necessários meios e estes são escassos. Segundo o EY Global Information Security Survey 2018-19 (GISS) - Is cybersecurity about more than protection?, 87% das organizações funcionam com um orçamento limitado para garantir o nível de cibersegurança e de resiliência de que necessitam. Muitas empresas admitem mesmo que a melhoria das suas práticas de cibersegurança ou o aumento do seu orçamento para este fim só sentirá um verdadeiro impulso se forem vítimas de algum tipo de violação ou incidente com consequências negativas.

Ainda assim, segundo estudo, as empresas de maior dimensão deverão ver os seus orçamentos aumentar este ano (63%) e no próximo ano (67%) quando comparadas com as empresas mais pequenas (50% e 66%, respetivamente).

O estudo foi realizado por esta empresa global em auditoria, assessoria fiscal, assessoria de transações e assessoria de gestão, através de inquérito a cerca de 1400 decisores e responsáveis de risco e cibersegurança de organizações que têm receitasentre um pouco menos de 10 milhões de dólares a mais de 10 mil milhões de dólares.

Outro sinal positivo dado pela maioria das organizações diz respeito à qualidade e sofisticação das tecnologias a que recorrem. Com efeito, o estudo revela que 77% das empresas e organizações procuram proteções de cibersegurança para além do básico e querem otimizar as suas capacidades recorrendo a tecnologias avançadas como inteligência artificial, automação de processos robotizados e analítica, entre outras.

O estudo foi realizado por inquérito a cerca de 1400 decisores e responsáveis de risco e cibersegurança de organizações com receitas entre os 10 milhões e os 10 mil milhões de dólares

"Estas organizações continuam a trabalhar nos conceitos essenciais de cibersegurança, mas estão também a repensar a sua rede e arquitetura de cibersegurança para apoiarem o negócio de forma mais eficiente", explica-se.

O estudo revela, todavia, que apenas 8% dos inquiridos indicam que as funcionalidades de segurança de informação respondem assertivamente às suas necessidades. A grande maioria (78% e 65% das empresas de maior e menor dimensão, respetivamente) dizem que as funcionalidades de segurança respondem, pelo menos, parcialmente às suas necessidades.

Significativo é igualmente o facto de todas as inquiridas dizerem estar envolvidas em projetos de transformação digital e a aumentar o orçamento dedicado a tecnologias emergentes.

Computação em nuvem (52%), analítica de cibersegurança (38%) e computação móvel (33%) são as maiores prioridades do investimento de cibersegurança em tecnologias emergentes este ano, segundo o estudo da EY para 2018--2019.

OPINIÃO

Cibersegurança é um "must have" para o seu negócio

AURÉLIO DUARTE
Marketing Executive, Amen.pt

A cibersegurança deve ser uma preocupação global e não se aplica apenas às organizações, mas também às pessoas. É necessário estarmos sensibilizados dos riscos que corremos ao termos a nossa informação online. Cada vez mais, usamos dispositivos que estão permanentemente ligados à Internet e que falam entre si (Internet das Coisas - IoT). Estes têm a capacidade de recolher uma vasta quantidade de informação sobre o utilizador, e é aqui que surgem os riscos de segurança, a partir do momento em que estamos ligados a probabilidade de sofrermos um ataque é maior.
Os fabricantes, fornecedores e parceiros associados ao seu negócio podem também aumentar o risco da violação dos seus dados. Por conseguinte, as empresas gastam milhões em soluções de segurança para combater os ciberataques.

No setor do comércio eletrónico existem centenas de milhares de sites em operação que podem beneficiar dos investimentos em segurança. As transações realizadas em sites de comércio eletrónico exigem a troca de dados confidenciais que podem ser comprometidos a qualquer momento se as empresas não tiverem a proteção adequada.

Se os dados de uma empresa forem comprometidos e os 'hackers' obtiverem informações de cartão de crédito dos clientes, a empresa será responsável pela violação de dados. Para além da falha na segurança, a empresa perde a confiança dos seus clientes, bem como as receitas.

A preocupação com os dados dos clientes não deve ser apenas das empresas de comércio eletrónico, mas de todas as empresas que guardam dados confidenciais, como números de identificação pessoal, passwords e qualquer tipo de informação sensível.

Um erro comum é pensar que as pequenas empresas são "muito pequenas" para serem alvo de ataques. Infelizmente, a maior parte dos empreendedores não percebem que as pequenas empresas correm o mesmo risco de ataques que as grandes empresas. De acordo com um relatório da Verizon, 61% dos ataques foram feitos às pequenas empresas, uma vez que são fáceis de atacar, devido a uma atitude complacente e à falta de investimento em medidas de cibersegurança.

O processo da transformação digital das empresas está mais do que nunca a colocá--las sob risco de ciberataques. A informação e os dados do negócio são os ativos mais importantes para uma empresa. É imperativo que os empreendedores comecem a ganhar consciência sobre a importância dos seus dados, uma vez que estes são vitais para o sucesso do seu negócio.

Ao termos consciência dos riscos, temos também a preocupação de proteger a informação. Os profissionais de análise de bigdata estão a usar tecnologias de prevenção, bem como serviços de deteção e resposta para fazer face ao crescendo número de ataques, causado pelo aumento de dados que são gerados diariamente. A analítica é o elemento chave para alavancar a proteção contra ciberataques.

Com o aumento dos ataques, cada vez mais sofisticados e recorrentes, cabe a cada organização tomar as devidas medidas para se proteger, tendo em consideração que um hacker só precisa de ter uma tentativa com sucesso para conseguir entrar nos sistemas. As organizações precisam de redefinir os seus conceitos de cibersegurança e mudar de direção, optando pelo paradigma PDR: Prevenção-Deteção--Resposta.

ESTUDO DA ACEPI

Vinte mercados para Portugal conquistar o mundo do comércio digital

Reino Unido, EUA, França, China, Espanha e Alemanha são os mercados alvo com maior potencial de adesão a produtos nacionais através do digital, revela um estudo da ACEPI a apresentar no Portugal Digital Week, entre 22 e 26 de outubro, no Pavilhão Carlos Lopes, em Lisboa.

MAFALDA SIMÕES MONTEIRO
mmonteiro@jornaleconomico.pt

Os seis principais parceiros de Portugal no comércio bilateral são Reino Unido, EUA, França, China, Espanha e Alemanha. Estes são, em simultâneo, países desenvolvidos e com maturidade digital sendo os mais relevantes e com maior potencial de adesão aos produtos nacionais através dos canais digitais, revela um estudo da ACEPI.

O mapa-mundo das relações digitais é traçado no estudo "Top 20 Principais Economias na área do comércio eletrónico e de maior potencial de adesão aos produtos nacionais" foi realizado no âmbito do Projeto Norte Digital da ACEPI - Associação da Economia Digital e foi comissionado à especialista em estudos de mercado IDC. O estudo vai ser detalhadamente apresentado às empresas portuguesas e à comunidade tecnológica e do e-commerce durante o Portugal Digital Week. Este conjunto de eventos, decorre entre 22 e 26 de outubro, na sua maioria no Pavilhão Carlos Lopes, em Lisboa, e conta com o Reino Unido como país convidado, justamente um dos mercados que mais potencial oferece às empresas portugueses.

As 20 economias com maior potencial de adesão a produtos nacionais através do digital reúnem vários ou, pelo menos, um de três requisitos: são relevantes no contexto atual das exportações das pequenas e médias empresas (PME) portuguesas, figuram entre as maiores economias mundiais e são países com uma maturidade digital elevada que potencia as exportações online. Em conjunto representam cerca de 80% do PIB e 55% da população mundiais.

Na lista das duas dezenas de mercados que mais oportunidade poderão proporcionar às PME no comércio digital figuram, fazem parte, além dos países atrás referidos, dois outros grandes mercados tradicionais de acolhimento de produtos portugueses: Países Baixos e Itália. Outros parceiros europeus com menos peso, mas igualmente importantes, como a Polónia, Suécia, Suíça e Turquia e Rússia surgem igualmente na lista. Facto normal, dado que 75% das exportações portuguesas de bens têm como destino o velho continente. Esta percentagem representa cerca de 50 mil milhões de euros/ano, o equivalente a 26% do PIB.

A Portugal Digital Summit tem a duração de dois dias, oferece em paralelo três sessões de debates e conta com mais de uma centena de oradores

ALEXANDRE SOARES DOS SANTOS RECEBE PRÉMIO CARREIRA ACEPI

Alexandre Soares dos Santos, líder histórico da Jerónimo Martins, dona do Pingo Doce, presidente da Sociedade Francisco Manuel dos Santos e Presidente do Conselho de Curadores da Fundação Francisco Manuel dos Santos, é o vencedor do Prémio Carreira ACEPI Navegantes XXI 2018.
A distinção é justificada pela "assinalável carreira" e "inegável contributo para o desenvolvimento da economia nacional e da sociedade portuguesa". O Galardão será entregue durante a Gala do Prémios ACEPI Navegantes XXI, dia 25 de outubro de 2018, no Pavilhão Carlos Lopes, em Lisboa. Serão também conhecidos os vencedores das vinte categorias a concurso este ano, de entre mais de uma centena de concorrentes.

Aproximação da Índia coloca-a entre 20 maiores

Apesar de países como o Canadá, a Austrália e o Japão terem um peso menos expressivo como mercados de destinos das exportações nacionais, o seu desenvolvimento e maturidade coloca-os no top 20 dos países com mais potencial para as PME nacionais.

A Índia, país que saltou diretamente para a "era digital", tem vindo a protagonizar uma grande aproximação a Portugal nos últimos dois anos. Em 2017, o primeiro-ministro Narendra Modi visitou pela primeira vez terras lusas, tendo, então, sido assinados 11 acordos de cooperação bilateral. Na altura, o primeiro-ministro, António Costa, elegeu a ciência e a cooperação entre as empresas como os dois pilares da relação com a Índia. "Se há cinco séculos foi a rota marítima que nos fez encontrar, hoje será certamente a rota digital que nos juntará para o futuro".

O Brasil, país lusófono e parceiro tradicional de Portugal, com grande desenvolvimento no e-commerce, e Marrocos, o mais importante parceiro bilateral na área do comércio de Portugal no continente africano, completam a lista dos 20 mercados.

O estudo da ACEPI, além de medir o pulso ao estado da economia digital global e identificar os mercados mais relevantes e com maior potencial para as PME portuguesas, visa igualmente ser um instrumento de apoio às empresas que pretendam apostar na economia digital e ajudá-las a selecionar os mercados alvo.

Produtos mais procurados nos destinos identificados

O estudo inventaria igualmente as diferentes categorias de produtos mais vendidos online, nos 20 países considerados, tendo em conta os seguintes domínios: Utilização da Internet, nível de compras online, meios de pagamento mais utilizados, condições de distribuição e serviços postais, utilização de tecnologias nas empresas, legislação e regulação, fiscalidade, maturidade da Economia Digital e exportação de produtos a partir de Portugal.

Os produtos elétricos e eletró-

nicos surgem à cabeça com uma fatia de 23,5%, seguido de muito perto dos produtos alimentares e bebidas, com 21,4%. O vestuário, cm 18% do negócio, o mobiliário e decoração, com 16%, e o calçado e acessórios, com uma fatia de 12%, são os produtos mais importantes. Em quinto lugar figuram os produtos têxteis, com 9,1%. Em conjunto estas cinco categorias de produtos vendidos online representam receitas superiores a 15,9 mil milhões de euros, isto é 32% do total de exportações de bens.

A apresentação do estudo é apenas um dos vários momentos altos da Portugal Digital Week, que inclui uma "round table" à porta fechada entre Portugal, país anfitrião, e o Reino Unido, país convidado na edição deste ano da iniciativa. A Portugal Digital Summit é outro marco da iniciativa. Tem a duração de dois dias e este ano surge com um novo formato (três sessões paralelas), contando com mais de uma centena de oradores (o difícil será escolher). A maioria dos temas a abordar pelos especialistas nacionais e internacionais que neles participam estão vocacionados sobretudo para as empresas e os negócios. A semana termina com o "Dia das Compras na Net". ●

ENTREVISTA ALEXANDRE NILO FONSECA presidente da ACEPI

ACEPI quer cativar empresas britânicas para vender em Portugal

Alexandre Nilo Fonseca, presidente da ACEPI - Associação da Economia Digital, explica porque era necessário fazer um estudo que identificasse os 20 principais destinos para a expansão dos negócios digitais em Portugal.

Quais são os principais objetivos e conclusões do estudo que acabaram de apresentar?
Um dos grandes desafios de Portugal no que toca ao comércio é que temos uma balança comercial digital desequilibrada. Os portugueses compram cada vez mais online e os que compram, compram mais. Além disso compram cada vez mais fora.
Não existe na mesma proporção estrangeiros a comprar em sites e operações portuguesas. A capacidade de exportação através do digital, de vender e transacionar e entregar um produto noutro país será o que muitas empresas portuguesas ambicionam.
Este estudo pretende ser uma ferramenta útil para qualquer empresário que queira identificar quais é que são os mercados mais interessantes para promover e comercializar os seus produtos utilizando a Internet enquanto plataforma.
Identificámos as 20 maiores economias em termos de digitalização, do potencial de exportação que existe para Portugal, tendo também identificado produtos e gamas de produtos que os consumidores daqueles países mais compram. Estas conclusões permitem-nos também aferir qual é o potencial que quem produz pode ter nesse país. Estou a pensar no sector do calçado, dos têxteis, do das bebidas, da alimentação. Áreas que as empresas portuguesas eventualmente já produzem e que poderão tirar partido da Internet como forma de promoção ou venda.

Quais as motivações subjacentes ao desenvolvimento deste estudo?
Achamos que este estudo vem colmatar uma lacuna que existia no mercado, que era a falta de informação para as empresas portuguesas sobre que mercados potenciais existem e em que devem apostar.
Esta ferramenta faz um diagnóstico, uma radiografia detalhada de 20 mercados inclui dados macro (população, PIB, taxas de IVA), mas também aspectos mais ligados ao digital: como o número de consumidores online, os produtos mais comprados online, os sistemas de pagamento mais utilizados, a qualidade da logística, a facilidade de fazer negócio em cada país.

> A capacidade de exportação através do digital, de vender e transacionar e entregar um produto noutro país será o que muitas empresas portuguesas ambicionam

Como escolheram o país convidado?
Para a Portugal Digital Week escolhemos um dos 20 países identificados: o Reino Unido. Esta escolha está relacionada com a relação histórica entre os dois países, incluindo em termos comerciais. Portugal compra muito no Reino Unido, mas, não obstante Inglaterra ser um dos países com maior número de compradores online, e em que cada consumidor mais consome online não é grande comprador em Portugal. Por isso é importante criar condições para que passe também a comprar em Portugal.
Para o efeito, entre outras iniciativas, será promovida, na próxima semana uma mesa redonda com 30 gestores portugueses e britânicos no Ministério da Economia para discutir não só criamos condições para criar uma maior interligação – às vezes são problemas relacionadas com logísticas, ou métodos de pagamento ou fiscais – mitigando as situações que poderão estar a condicionar a situação. ●

MAIS TIC

CIBERSEGURANÇA É CAPITAL PARA CONTINUIDADE DOS NEGÓCIOS

O mercado explica ao Jornal Económico qual a importância da cibersegurança para as empresas e quais os desafios que se colocam para salvaguardar os negócios num mundo em que bigdata, ferramentas de analítica cada vez mais complexas e dados armazenados em nuvem fazem parte do dia-a-dia.

1 QUAIS OS DESAFIOS E OPORTUNIDADES DA CIBERSEGURANÇA NUM MUNDO EM QUE OS NEGÓCIOS (B2B E B2C) TÊM DE LIDAR COM "ENORMES QUANTIDADES DE DADOS" NOS SEUS SERVIDORES OU NA CLOUD, TIRANDO PARTIDO DE FERRAMENTAS ANALÍTICAS COMPLEXAS?

SÓNIA CASACA
Business Unit Manager – Security
Arrow ECS

SEGURANÇA É UMA PRIORIDADE E UMA OPORTUNIDADE

A proteção dos dados é cada vez mais uma preocupação no mundo digital. A aplicação das novas regras, o Regulamento Geral de Proteção de Dados (RGPD), a 25 maio de 2018, foi o ponto de viragem para a proteção dos dados.
A lei veio alterar a forma como gerimos e mantemos os dados e como se encontram protegidos nas nossas infraestruturas, criando novas oportunidades na área da segurança, com soluções mais inovadoras e de nova geração.
Um dos desafios é que a segurança seja vista como uma prioridade e não como um custo, trazendo oportunidades a novas soluções menos complexas e mais adaptadas às necessidades das organizações.
É necessário inovar com a cibersegurança.
Tanto em B2B como em B2C, o RGPD veio alertar que uma fuga de dados pode pôr em causa a imagem da empresa e chamar a atenção para a importância desses mesmos dados e de como devem estar protegidos.

JOÃO MARTINS
Administrador
Cilnet

ENCONTRAR O NÍVEL DE PROTEÇÃO ADEQUADO

O grande desafio em cibersegurança é conseguirmos definir diferentes níveis de proteção e de acesso à informação, e só conseguimos essa definição com ferramentas de analítica de dados. Através destas ferramentas, conseguimos qualificar a informação crítica e sensível.
Posteriormente, a oportunidade e a diferenciação estão na forma como vamos utilizar e usar esses níveis de informação.
Num nível de informação mais crítico devemos utilizar soluções de segurança mais robustas, de maior investimento, enquanto que para a informação menos sensível e crítica devemos alocar soluções mais simples e de menor investimento.
Desta forma, conseguimos separar a criticidade da informação e o investimento necessário em segurança para os vários níveis, adotando e aplicando as melhores soluções para cada um deles. Com a quantidade de informação que as empresas hoje têm de gerir, incorreríamos em custos elevados e completamente desajustados caso não fizéssemos uma segmentação da informação, delineando a criticidade da mesma e aplicando soluções de proteção de forma eficiente.

ARAGÃO RIO
Senior Storage Systems Engineer
EMEA WER (Iberia)
Dell EMC

NECESSIDADE DE SISTEMAS DE SEGURANÇA PROATIVOS

Ao longo dos últimos tempos a área de cibersegurança tem vindo a registar uma crescente importância, tanto por parte de grandes corporações e empresas, como por PME.
O interesse neste tipo de tecnologia é imenso, pelo que os custos associados às perdas inerentes de acesso aos dados (ransomware), como à exposição da informação confidencial nos atuais quadros legais do RGPD é incalculável
A necessidade de comunicação e transações diárias entre organizações/clientes expõem de alguma forma os dados e aumentam aos riscos. Os sistemas analíticos de processamento e correlação de informação (bigdata, analítica, business intelligence) que residam em cloud privada ou publica estão expostos aos riscos, pelo que devem ser protegidos por sistemas de segurança proativos
A Dell Technologies com a Dell EMC, SecureWorks e a RSA estão na vanguardeada segurança preventiva e ativa de todos os riscos associados à perda, violação ou roubo de informação criando mecanismos end-to-end (Posto de trabalho ao datacenter (público ou privado)) para impedir os riscos existentes.

JOAO PENA GIL
Diretor de segurança
ITSector

RGPD: O NOVO DESAFIO DAS EMPRESAS

Um dos desafios mais recentes para as empresas que lidam com grandes quantidades de dados é o recém-criado Regulamento Geral de Proteção de Dados (RGPD). Este obriga as empresas a seguir uma panóplia de regras básicas de segurança e privacidade, entre as quais está a proteção de dados em repouso (em bases de dados ou ficheiros) através da aplicação de cifras criptográficas sobre os mesmos.
No entanto, quando utilizamos as bases de dados com as cifras suportadas atualmente pelos motores de BD ativas, perdemos a flexibilidade de filtrar, pesquisar e operar de modo mais complexo sobre os dados sem que estes precisem de ser decifrados. Creio que esta é uma boa oportunidade para se aumentar o investimento na investigação nos campos da cifragem antropomórfica, que permitiria mais flexibilidade na manipulação destes dados.
Outro desafio associado igualmente ao RGPD é o da autenticação do utilizador. Os sistemas devem conseguir assegurar que as entidades que têm acesso aos dados estão de facto autorizadas a fazê-lo e que o acesso não é de nenhuma forma fraudulento - algo que os sistemas podem dificultar, ou facilitar, como se viu recentemente no caso do CITIUS.

ANTONIO ESPINGARDEIRO
Consultor
KCS iT

ML: UMA MAIS VALIA PARA ASSINALAR POSSÍVEL FRAUDE

Para o mundo dos negócios, a questão da cibersegurança torna-se cada vez mais pertinente, de forma a garantir que os utilizadores naveguem na cloud e resolvam todos os seus assuntos de forma rápida e segura.
Para o consumidor, é cada vez mais comum aceder a bases de dados sensíveis como dados de contas bancárias (pagamentos), finanças, ou mesmo contas de serviços (água, eletricidade ou gás) ou de sites de comércio eletrónico na cloud. Na génese deste comportamento, está sobretudo a facilidade de acesso a plataformas digitais versus físicas e a rápida resolução de atividades para um utilizador que não quer dispor do seu tempo com questões burocráticas (ex.: atrasos/atendimento).
Ao falar em segurança informática falamos sobretudo de padrões de comportamento humano. Associado a isso está o grande volume de dados que circulam na cloud (Bigdata). Milhões de transações por minuto que necessitam de ser validadas. Dessa forma nas nossas transações de compras ou até folhas de vencimento existem padrões. Os novos sistemas de cibersegurança utilizam algoritmos de aprendizagem automática (ML) para interpretarem esses mesmos padrões.
Essencialmente trata-se de um mecanismo de estatística aplicada, onde existe um modelo matemático que define o comportamento espectável do utilizador (baseado na sua atividade).
Em termos práticos o sistema informático é treinado para "aprender" esse padrão. Uma vez treinado é então capaz de identificar através do cálculo de probabilidades eventuais desvios de comportamento que podem ou não espoletar um alerta para uma possível fraude. Hoje em dia é muito comum a utilização de localizadores de atividade, que por vezes nos notificam quando fazemos login a partir de uma localização não habitual. Da mesma forma os CRM na cloud utilizam mecanismos de tokens de autenticação que se refletem em mensagens de texto e emails com códigos de acesso para áreas de utilizador restritas.
De salientar que a cibersegurança é um novo tópico de estudo e sobretudo uma nova realidade no plano de negócios mundial. Os desafios são sem dúvida criar sistemas mais seguros e escaláveis que poderão chegar à inclusão de dados biométricos nas transações na cloud. Neste domínio existe um caminho longo a ser percorrido pelas empresas tecnológicas. A enfâse está sobretudo na criação de algoritmos de ML mais eficazes, passíveis de atuar numa filosofia preventiva.
É aqui que a criatividade pode fazer toda a diferença no sentido que o peso que se dá à localização dos logins e transações, passando pelo padrão e periodicidade das mesmas cria naturalmente combinações distintas que depois se irão revelar mais ou menos assertivas num possível indício de fraude. Neste domínio parte-se sempre de um principio de precaução, isto é, mais vale analisar falsos alarmes e clarificar toda a situação do que obter uma possível fraude associada.
Desta forma o papel do utilizador é essencial para confirmar ou não transações na sua atividade online.
Em suma a progressiva introdução de Inteligência Artificial na cloud trará sobretudo uma fusão entre o comportamento humano em conjugação com algoritmos de ML.

JOÃO BARRETO FERNANDES
VP of Strategic Marketing (CMO)
S21sec Portugal

GESTÃO MASSIVA DE DADOS DEVE SER PRIORIDADE

Enquanto disciplina que tem como objetivo a proteção do negócio das organizações, a cibersegurança deve considerar a gestão massiva de dados como prioridade devido aos enormes impactos que o comprometimento de tais dados implica. Quando tais dados são relativos a cidadãos, o tema RGPD releva ainda mais a proteção requerida.
Neste contexto os desafios são de várias naturezas, felizmente todos endereçáveis por soluções técnicas e/ou pela aplicação de processos definidos à luz de uma gestão de risco cuidada. De forma muito grosseira, os desafios podem ser sumarizados em três naturezas: a gestão rigorosa dos níveis de acesso configurados nos sistemas de informação, a proteção da informação nos vários meios em que pode estar localizada (storage, backups, vaults, etc.) e a transmissão segura de informação através de redes de dados.
Um aspeto relevante é que os riscos crescem de forma exponencial com a volumetria dos dados, a sofisticação dos sistemas que os gerem e processam, o número de entidades envolvidas e a dispersão dos meios tecnológicos usados.
Felizmente, soluções de IAM (gestão de identidades e acessos), cifra de dados "at rest" e comunicações, ratings de segurança de empresas, monitorização de dispositivos terminais, entre muitas outras, dão aos profissionais do sector a oportunidade de mostrarem que estão à altura dos desafios.

ADELINO MONTEIRO
Information Security & Risks Manager, Iberia
Sage

CIBERSEGURANÇA DEVE ADAPTAR-SE DINAMICAMENTE

A era digital permitiu às empresas reinventarem-se na forma como operam e fazem negócio. Vemos no ciberespaço uma oportunidade de disponibilizar serviços e produtos de negócio inovadores.
O uso de bigdata (grandes quantidades de dados) pode permitir melhorar os resultados de saúde, maior compromisso cívico com governos, preços mais baixos devido à transparência e uma melhor adequação entre produtos e necessidades dos consumidores.
Por outro lado, vemos uma maior inovação nas ferramentas e técnicas de hacking e ataques de segurança cada vez mais avançados. Os desafios enfrentados pelas organizações para proteção e privacidade dos dados envolvem um ambiente de TI complexo, diversas soluções bigdata fora do IT, residindo em áreas de negócios e utilizadas para experiências, maior risco do que o habitual e a anonimização dos dados nem sempre eficaz, permitindo a de-anonimização a partir de processos de re-identificação passando a ser dados pessoais (RGPD)
As empresas procuram continuamente protegerem-se contra estes ataques, mas não podem evitar o risco. É crucial arquitetar uma solução de cibersegurança que se adapte dinamicamente à necessária constante mudança.

RITA MOURINHA
Representante
Seresco em Portugal

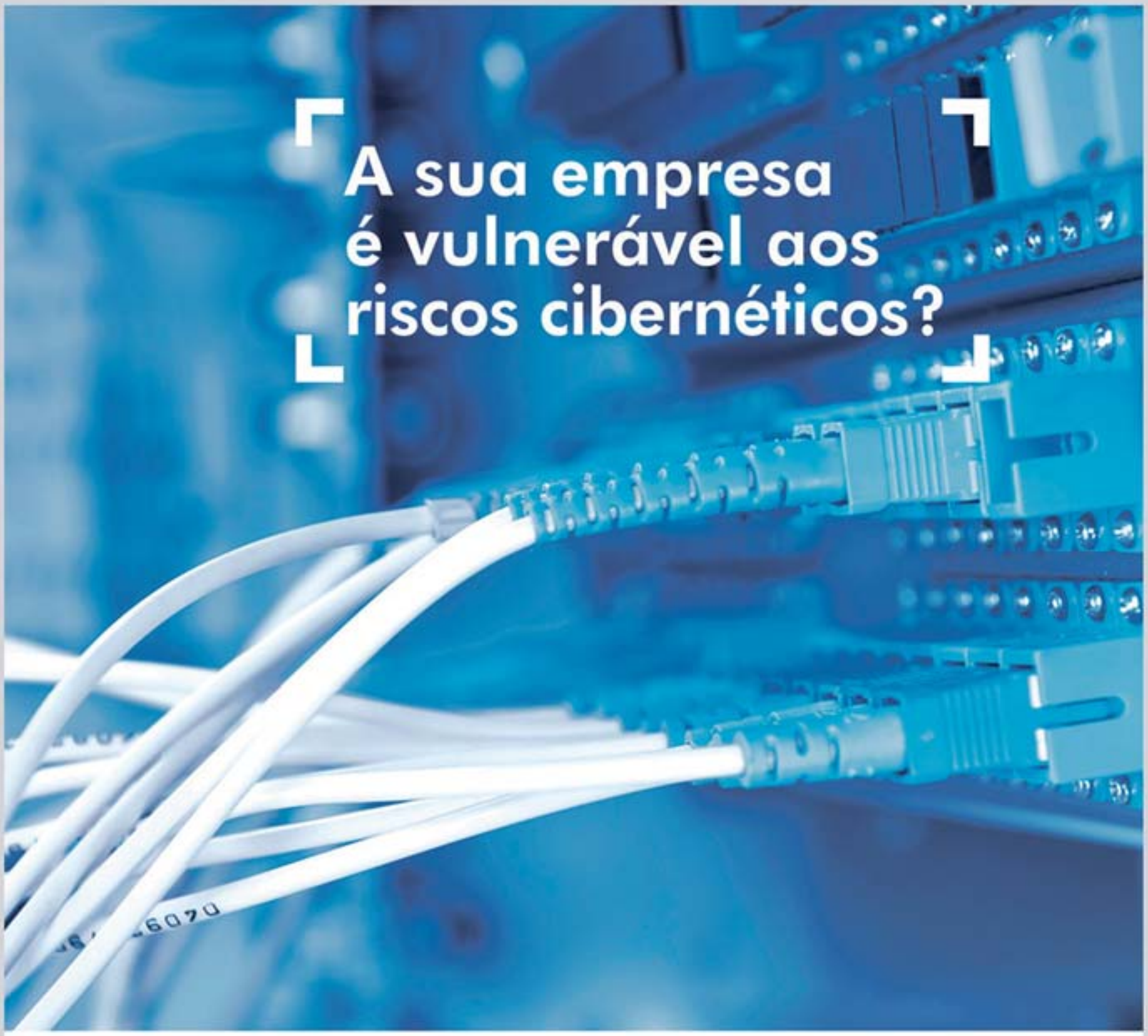
A QUANTIDADE DE DADOS EXISTENTE É DIFICILMENTE IMAGINÁVEL

O tema da bigdata não é novo. No entanto, em 2018, foi um dos hot topics, sobretudo em áreas de atividade que lidam, ao segundo, com dados pessoais como é o caso das áreas de recursos humanos e processamento salarial. Com a introdução do novo RGPD e o primeiro exercício nacional de cibersegurança, há um ano, assistimos ao crescimento da importância dos dados.
A quantidade de dados existente é dificilmente imaginável – e o seu crescimento é contínuo. Com a maior disponibilização desta informação, onde se incluem dados pessoais e intransmissíveis, como se verifica nas soluções de processamento de salários, também os desafios da cibersegurança são cada vez maiores: ciberataques externos, fugas de informação e roubos de identidade são riscos atuais a ter em conta e ameaças reais às empresas.
No entanto, o imenso volume de dados pode apresentar também grandes oportunidades, sendo uma delas o seu enorme potencial para extrair informação, insights importantes que podem ser utilizados, sobretudo na área dos recursos humanos, e também para dinamizar e fazer crescer o negócio das empresas atualmente existente.
Esta maior preocupação de cidadãos e decisores com questões de cibersegurança e a sua relevância na agenda mediática constitui também uma oportunidade para as empresas instituírem melhores regras de implementação dos procedimentos necessários para a preservação da confidencialidade, integridade e disponibilidade dos dados processados.

GABRIEL COIMBRA
Country manager
IDC Portugal

EMPRESAS PROCURAM AUTOMATIZAÇÃO DA GESTÃO DA SEGURANÇA

Em Portugal o valor do mercado de segurança deverá crescer cerca de 39% entre 2017 e 2022, passando de um valor de 130 milhões de euros para cerca de 181 milhões .
A distribuição do valor pelos segmentos está em linha com a Europa, com os Serviços a representarem 56% do mercado em 2017 e podendo chegar a 61% em 2022. Os Serviços de segurança terão um crescimento médio anual de 9%, enquanto o crescimento médio anual de Software e o Hardware deverá rondar os 7% e 2% respetivamente.
Entre 2017 e 2022 os maiores crescimentos (CAGR) verificam-se nos Managed Security Services (11,9%), seguindo-se Device Vulnerability Assessment (10,7%) e Software Vulnerability Assessment (9,5%), Forensics and Incident Investigation (7,2%), Policy and Compliance (7,2%) e Consulting Services (7,1%). Setor de Banca representa 20% do investimento, seguindo-se Governo e Indústria com 9%.
Mais de 70% das organizações nacionais reconhece que a 3ª plataforma e os aceleradores de inovação contribuíram para aumentar os riscos de segurança. O recurso a tecnologias de automatização da gestão da segurança já tem uma presença relevante nas organizações com 44% a reconhecer ter um bom balanceamento entre processos manuais e processos automatizados e mais de um terço (69%) ter a expetativa de utilização de automatização nos próximos 12 meses. As tecnologias mais utilizadas (+90%) são as Firewalls de redes (SSL, IPsec, etc.) e Redes privadas virtuais (VPN) com a Security-as-a-Service (SECaaS) a ser aquela com menos adoção entre as organizações (<15% em utilização).



Contrate o CyberEdge. Uma solução flexível para lidar com o risco cibernético - e com as seguintes consequências.

Na eventualidade de informações confidenciais serem comprometidas, as repercussões para o seu negócio podem ser graves e dispendiosas. É por isso que existe o CyberEdge. Desde à gestão de crises até às investigações legais e aos serviços de restauração de identidade, podemos ajudar a gerir e a mitigar os efeitos de uma violação, para que possa manter o foco no seu negócio.

AIG

Bring on tomorrow