IT Insight

#36 MARÇO 2022

moving to the cloud

Como lidar com *cyber-attacks*?

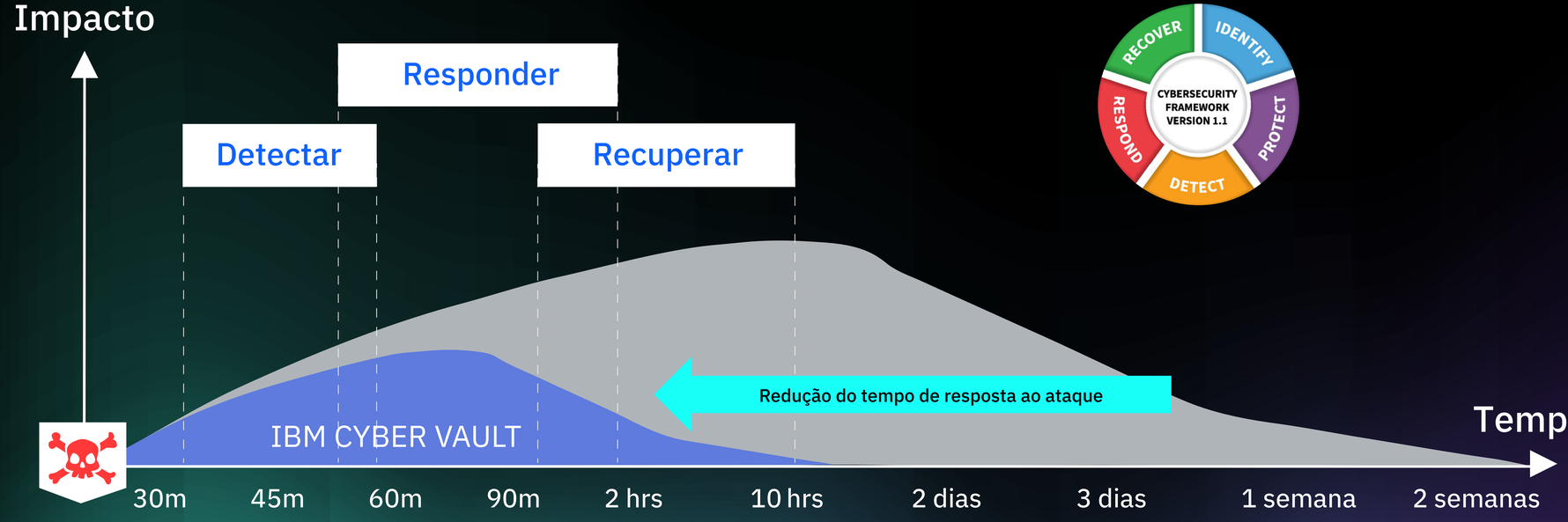
IBM pode ajudá-lo a preparar-se!

IBM FlashSystem
Cyber Vault

FlashSystem 5200

FlashSystem 7300

FlashSystem 9500



Five Years Out

Contacte-nos para mais informações:

www.arrow.com/ecs/pt
hw_ibm.ecs.pt@arrow.com

Distributor

BROWSE

IT·Insight

#36 MARÇO **2022**

Move fast. Stay safe.

Com mais de 20 anos de experiência em serviços de Cibersegurança e Training para algumas das maiores marcas do mundo, a Claranet Cyber Security reúne toda a expertise que a sua empresa necessita para se manter operacional e totalmente segura.

Visite: www.claranet.pt/cybersecurity

IT·Insight

#36 MARÇO **2022**

Security-Driven Networking, everywhere you need it.

Protect the possibilities with Secure SD-WAN.

www.fortinet.com

HENRIQUE CARREIRO

Uma nova ordem no mundo — e na cloud

QUANDO IRROMPEU a pandemia, nesse já longínquo ano de 2020, a cloud ganhou uma importância para a sociedade atual que, de certo modo, até então não era necessariamente reconhecida.

É certo que a maioria dos serviços de consumo, como o Netflix, se apoiam em serviços de cloud, mas não era tão claro então que fosse um caminho incontornável para as empresas. Mas, de súbito, tudo se alterou. Sobretudo por via das exigências relativas ao trabalho remoto, as características de acesso ubíquo da cloud impuseram-se como indispensáveis.

Em 2022, as crises são já outras e de não menor importância. A emergência de graves escaladas bélicas leva a um aumento também de ataques de outra ordem — as guerras são hoje tanto mais travadas no espaço dos CPU e dos discos de armazenamento quanto o são no terreno com armas de fogo real. As consequências são diferentes, mas ambas devastadoras de vidas e economias.

Mais uma vez, a cloud assumirá um papel de infraestrutura crucial, já pela sua maior resiliência arquitetural face aos sistemas convencionais, já pelo simples facto de os seus fornecedores contarem entre os respetivos técnicos alguns dos maiores especialistas em segurança do mundo.

O que se espera nesta fase — difícil mais uma vez — é que os fornecedores de cloud redimensionem as suas capacidades à altura dos desafios. É certo que é necessário que se desenvolvam novos serviços, já que o ambiente competitivo entre fornecedores e as necessidades do mercado não parece ter sinais de abrandamento. Mas também é necessário que as plataformas de cloud sejam capazes de continuar a aumentar os seus graus de segurança e disponibilidade, ainda que isso implique um abrandamento do ritmo de lançamento de novas características e funcionalidades.

Mais do que nunca precisamos de uma cloud robusta e sólida, numa altura em que o mundo parece especialmente assente em terrenos escorregadios, perigosos mesmo. ■

GARANTA QUE INCLUI UMA

STORAGE COM IMUTABILIDADE DE DADOS NO SEU PLANO DE CIBERSEGURANÇA!

BLOQUEIE OS ATAQUES DE RANSOMWARE COM UMA STORAGE COM IMUTABILIDADE DE DADOS

Faça do OneXafe parte da sua estratégia de segurança de TI e garanta que os seus dados estão protegidos de ciberataques ou perdas acidentais. Recupere de forma instantânea a partir de um snapshot limpo e fique seguro que vai poder responder **NÃO** a pedidos de resgate e foque-se em repor o seu negócio em produção rapidamente.

OneXafe

Complete a sua estratégia à prova de bala com uma storage com imutabilidade de dados.

arcserve.com/data-protection-solutions/onexafe-storage

arcserve®

Protect what's priceless.

DIGITALIZAÇÃO DO SETOR DE RECURSOS HUMANOS CONSOLIDA-SE EM PORTUGAL

Um novo estudo nota que a digitalização de recursos humanos em Portugal está num bom caminho, mas ainda abaixo da média europeia.

A TRANSFORMAÇÃO digital está a ter um grande impacto na gestão de Recursos Humanos (RH) nas empresas a nível global, incluindo Portugal, e as empresas procuram cada vez mais software especializado para a gestão dos RH. As conclusões proveem do novo Estudo de RH 2021 da Factorial, que refere, também, que as mudanças na forma de trabalhar conduziram a melhorias significativas na vida dos colaboradores. Neste momento, o benefício mais valorizado em todos os países inquiridos é a possibilidade de conciliar a vida profissional e pessoal.

No caso português, o nível de digitalização do setor dos RH é bastante significativo – chegando a 84,2%. Contudo, ainda é ultrapassado por grande parte dos países europeus, como o Reino Unido (96%), a Alemanha (94%), Espanha e França (ambos 91%); sendo equiparável apenas a Itália (84%). ■

REGULADOR EUROPEU LANÇA INVESTIGAÇÕES SOBRE SERVIÇOS CLOUD NO SETOR PÚBLICO

As investigações vão abranger mais de 80 organismos públicos em todo o Espaço Económico Europeu.

O COMITÉ EUROPEU para a Proteção de Dados anunciou que vai lançar investigações juntamente com 22 reguladores nacionais, incluindo a Autoridade Europeia para a Proteção de Dados, sobre a utilização de serviços baseados na cloud pelo setor público, com o intuito de verificar se cumprem as devidas condutas de privacidade.

Segundo um comunicado da instituição, as investigações vão abranger mais de 80 organismos públicos em todo o Espaço Económico Europeu, incluindo instituições da UE, abrangendo uma grande variedade de setores como a saúde, finanças, impostos, educação e fornecedores de serviços de IT.

É de notar que empresas de serviços cloud norte-americanas, como AWS, Google, Oracle e o Microsoft, têm vindo a construir data centers em toda a Europa em resposta à crescente procura por parte de organizações do setor privado e público. ■

Cumprimos a promessa da Cloud

Migre os seus serviços para a Cloud e potencie o seu negócio através de Big Data Analytics, AI - Artificial Intelligence e Machine Learning.

aws partner network
Select Consulting Partner
Public Sector Partner

aws partner network
Select Consulting Partner

Apoiamos as empresas na definição da **Estratégia de Migração para a Cloud** e fornecemos a tecnologia para implementar e operacionalizar soluções altamente escaláveis. Trabalhamos com os maiores operadores globais de telecomunicações e desenvolvemos plataformas que garantem a ligação de milhões de utilizadores. **Comece hoje connosco a sua migração para a Cloud.**

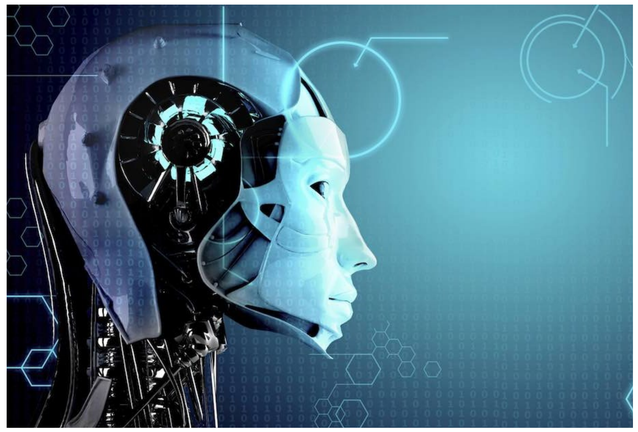
CYCLOID
Technology and Consulting

Visite-nos em https://www.cycloid.pt e contacte-nos através do e-mail: info@cycloid.pt

WE ARE STRONGER TOGETHER

EMPRESAS AUMENTAM GASTOS NO MERCADO DE IA

Os especialistas da IDC preveem que os gastos mundiais para o mercado de inteligência artificial deverão crescer 19,6% em 2022.



OS GASTOS MUNDIAIS para o mercado de Inteligência Artificial (IA) deverão crescer 19,6% em 2022, para 432,8 mil milhões de dólares. Os dados são do mais recente *Worldwide Artificial Intelligence Tracker* da IDC, que indica que o mercado deverá chegar à marca dos 500 mil milhões de dólares em 2023. "A IA surgiu como a próxima grande onda de inovação. Atualmente, as soluções de IA estão focadas em problemas dos processos de negócio e vão desde *human augmentation* até à melhoria de processos e ao planeamento e previsão, potenciando decisões e resultados superiores. Os avanços nas tecnologias de linguagem, voz e visão e soluções de IA multimodais estão a revolucionar a eficiência humana", refere Ritu Jyoti, group vice-president, Worldwide Artificial Intelligence e Automation Research da IDC. Mais, acrescenta que, "no geral, a IA mais o engenho humano é o diferenciador para as empresas escalarem e prosperarem na era da transformação digital comprimida". ■

ENISA E CERT-EU PROCURAM AUMENTAR CIBER-RESILIÊNCIA DAS ORGANIZAÇÕES

O documento "Boosting Your Organization's Cyber Resilience" aponta boas práticas de cibersegurança a serem adotadas pelas organizações.

A ENISA reportou um aumento substancial de ciberameaças contra organizações públicas e privadas em todo o território da União Europeia e menciona que esta tendência está relacionada com vários fatores. Com base neste aumento de ciberameaças contra organizações baseadas na União Europeia, a ENISA e o CERT-EU "encorajam fortemente" todas as organizações públicas e privadas a adotar o "conjunto mínimo de melhores práticas de cibersegurança" que estão disponíveis no documento "*Boost your Organisation's Cyber resilience - Joint Publication*".

Esta publicação destina-se principalmente aos decisores, tanto de IT quanto de gestão, assim como os profissionais de cibersegurança, como os CISO. Destina-se também, dizem as duas entidades, às empresas que apoiam a gestão de risco organizacional. ■

visionware

Challenging an **Unsafe** World

GERAL@VISIONWARE.PT

+351 225 323 740

VISIONWARESI

PORTO

LISBOA

VISIONWARE.PT

PROCURA POR TALENTO NA ÁREA DA SUSTENTABILIDADE CRESCE

Perante os desafios da pandemia e os objetivos definidos pela ONU, a dimensão da sustentabilidade está entre as prioridades atuais das empresas.

A SUSTENTABILIDADE está entre as principais prioridades das organizações, ganhando importância estratégica para o desenvolvimento dos seus negócios - o que se reflete nas atuais ofertas de emprego. Os dados são da Michael Page, que apresentou o eBook Talento e Sustentabilidade, no qual analisa as tendências do mercado de trabalho neste setor para este ano, no mercado português.

Os dados explicam que a atração de talento na área da sustentabilidade motivada por fatores que se prendem com a resposta ambiental, social e económica por parte das empresas perante os desafios da pandemia e dos objetivos definidos pela agenda da ONU, tem provocado uma mudança positiva na visão dos líderes face à implementação dos processos de sustentabilidade de forma transversal em todas as funções corporativas. ■

61% DOS DECISORES QUEREM ADOTAR FERRAMENTAS DE MINERAÇÃO DE PROCESSOS

A maior adoção destas ferramentas vai permitir às organizações compreender melhor o seu funcionamento interno através de dados detalhados.

A TRANSFORMAÇÃO digital aumentou, e continua a aumentar, a complexidade dos sistemas e processos das organizações, muitas vezes incapazes de compreender completamente os seus dados internos, complicando a tomada de decisões. Neste sentido, ferramentas como a mineração de processos, que fornecem uma grande quantidade de informações sobre o funcionamento da empresa, estão em expansão no ecossistema empresarial, indica uma investigação realizada pela Forrester Consulting para a Celonis.

A maior adoção destas ferramentas vai permitir às organizações compreender melhor o seu funcionamento interno através de dados detalhados sobre as suas operações e sistemas, cadeia de valor, atendimento ao cliente, planeamento de recursos empresariais, ou gestão de serviços de IT. ■

noesis
an Altia Company

Conhece as vulnerabilidades da sua organização?

Solicite um Proof of Value (PoV) de Enterprise Immune System da Darktrace:

- 4 Semanas de utilização de solução de Cyber AI, sem custos
- Proteção dos colaboradores e organização contra ameaças de segurança
- Ação imediata sobre qualquer ameaça ou vulnerabilidade
- Tecnologia líder mundial assente em Machine Learning

Saiba mais

DARKTRACE

Helping your business **grow faster**

Portugal · Espanha · Irlanda · Holanda · Brasil · EUA

www.noesis.pt

TRANSFORMAÇÃO DIGITAL GOVERNAMENTAL EXIGE COMPROMISSO COM TECNOLOGIA EMERGENTE

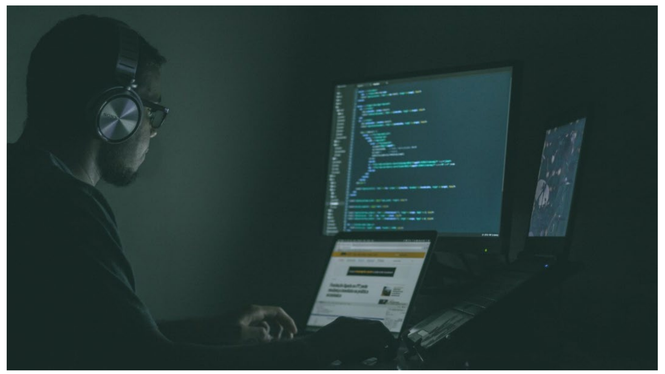
85% dos governos digitais avançados conseguiram escalar o digital de forma transversal nas suas organizações.

"**A TRANSIÇÃO** para o governo digital significa uma mudança organizacional, que pode ser difícil de alcançar às vezes", diz Dean Lacheca, Director Analyst na Gartner. Para os CIO, alcançar uma verdadeira transformação digital dentro do governo requer um compromisso total com tecnologias e capacidades emergentes que podem escalar através de uma organização, segundo a Gartner.

O relatório *Digital Transformation Divergence Across Government Sectors Survey* da Gartner explorou as diferenças de objetivos, práticas e estrutura de iniciativas digitais que levaram a implementações transformadoras bem-sucedidas. Se concentrar as suas prioridades da mesma forma, pode esperar cumprir as suas estratégias de governo digital de forma mais eficaz. No seguimento da sua investigação, a Gartner indica práticas que os governos digitalmente avançados devem adotar. ■

PROCURA POR PROFISSIONAIS DE CIBERSEGURANÇA CONTINUA A AUMENTAR

A procura por profissionais especializados em cibersegurança está a aumentar um pouco por todo o mundo e, em particular, em Portugal.



A PROCURA por profissionais especializados em cibersegurança está a aumentar em Portugal impulsionada pelo crescimento das ameaças e ataques de segurança, de acordo com a Michael Page. Com um mercado de cerca de mil/1.500 profissionais a atuar na área da cibersegurança, 600 dos quais localizados na região Norte, são necessários pelo menos mais 300 especialistas para suprir as necessidades de recrutamento atuais, bem como garantir redundância em determinadas equipas que enfrentam de momento uma situação de excesso de trabalho. Os crescentes ciberataques fazem com que vários tipos de ameaças devam estar no foco de combate e prevenção das empresas. Deste modo, o mercado de trabalho tem registado um crescimento nos últimos três anos e vai continuar a crescer, sobretudo nos principais centros urbanos do país, Lisboa e Porto. ■

Bitdefender

BUILT FOR RESILIENCE

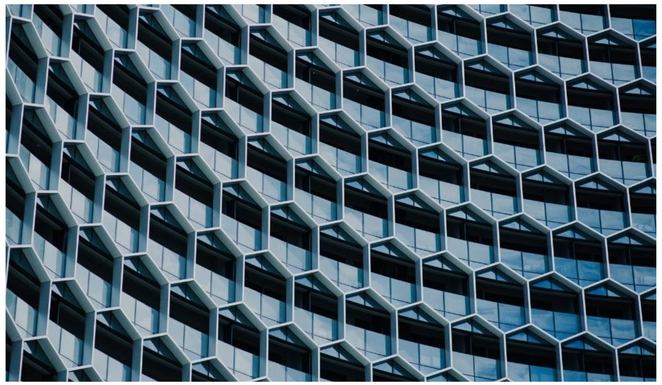
We protect your business
We protect your customers

- eXtended Endpoint Detection and Response (XEDR)
- Managed Detection and Response (MDR)
- Cloud Workload Security (CWS)

www.bitdefender.pt

REINVENÇÃO DIGITAL É FUNDAMENTAL PARA INDÚSTRIA SEGURADORA

Estudo conclui que é preciso reforçar a aposta no digital para que este setor possa crescer e ser mais resiliente.

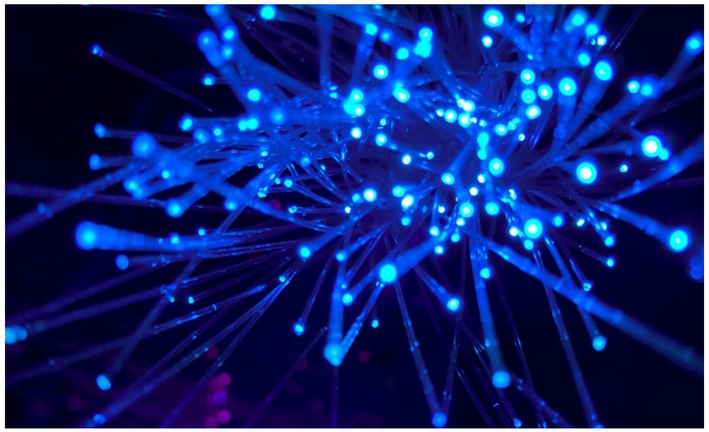


A XPAND IT lançou o estudo "Indústria Seguradora: *What's Next?*" com foco numa das maiores e mais antigas indústrias do mundo. Uma das principais conclusões deste estudo é que as seguradoras necessitam de reforçar ainda mais a aposta no digital para crescer e ser mais resilientes no futuro.

Após o período de pandemia será impossível voltar atrás. O relatório da Xpand IT aponta que o comportamento do consumidor foi bastante impactado, o que vai significar a necessidade de criar novos produtos e serviços, novos modelos de *customer engagement* e, acima de tudo, a construção de uma experiência envolvente. As seguradoras devem, por isso, construir uma experiência digital e física convincente, num contexto em que os agentes vão desempenhar um papel chave na jornada do consumidor, através de consultoria e aconselhamento. ■

IDC LANÇA BENCHMARK PARA RESILIÊNCIA DE INFRAESTRUTURAS DIGITAIS

O Digital Infrastructure Resiliency Index procura ajudar as organizações a definir as prioridades de investimento.



A IDC publicou recentemente o seu *Digital Infrastructure Resiliency Index*, uma estrutura que as empresas podem usar para avaliar seu próprio Quociente de Resiliência de Infraestrutura Digital (DRIQ, na sigla em inglês) usando uma escala de cem pontos para identificar as principais prioridades de investimento em infraestrutura digital comprovadas para melhorar significativamente os resultados de negócios digitais.

Mary Johnston Turner, vice-presidente de pesquisa do programa Future of Digital Infrastructure Agenda da IDC, explica que "o *Digital Infrastructure Resiliency Index* da IDC permite que as equipas de liderança avaliem rapidamente o nível atual de resiliência de infraestrutura digital da sua organização em relação ao setor e identifiquem áreas em que precisam rever e acelerar as prioridades de investimento na infraestrutura, para melhorar os resultados gerais dos negócios". ■

INFORMANTEM®
Keep IT Simple

WWW.INFORMANTEM.PT

POR QUANTOS ESCRITÓRIOS ESTÃO DISTRIBUÍDOS OS COLABORADORES DA SUA EMPRESA?

PROMOVEMOS A MOBILIDADE SEGURA DOS SEUS COLABORADORES:

Gestão de dispositivos móveis

Serviços Cloud

Auditoria e formação em cibersegurança

PORTUGAL • MOÇAMBIQUE • ANGOLA • CABO VERDE

LISBOA
Av. José Francisco Guerreiro Paiã Park
Edifício A2 1675-076 Pontinha

+ 351 210 127 000

PORTO
Complexo Comercial de Santana, Rua de Santana
963 - E 4465-742 S. Mamede de Infesta

+ 351 229 470 220

BUILDING THE FUTURE:

O FUTURO DA TRANSFORMAÇÃO DIGITAL COMEÇA AGORA

A quarta edição do evento da Microsoft discutiu os principais desafios e oportunidades do futuro dos negócios e da revolução digital, das pessoas e do planeta, e da educação e skilling.

MARIA BEATRIZ FERNANDES

O EVENTO PORTUGUÊS Building The Future, que decorreu entre os dias 26, 27 e 28 de janeiro, "terminou, mas a construção do futuro não para", afirmou a Microsoft Portugal na sua página de Twitter. Numa transmissão *live*, a apresentação do evento a partir do Capitólio, em Lisboa, esteve nas mãos de Filomena Cautela e o resultado foi um total de 21 mil participantes online em 66 países. Segundo Andrés Ortolá, General Manager da Microsoft Portugal, "Portugal é um país de empreendedores e de inovadores" e "ao longo destes três dias, aprofundámos a necessidade de acelerar os processos de Transformação Digital e de desenvolvimento de competências".

A TRANSFORMAÇÃO DAS PME

Muito foi discutido durante a quarta edição do evento, e, na impossibilidade de resumir as 180 sessões do Building the Future, focamo-nos em algumas das sessões que abordam o nosso mundo digital em transformação. A digitalização vai exigir investimento, competências e capacidade de ação, temas que subiram para a mesa durante o painel *SMB Transformation*.

"Aquilo que nos apanhamos nos últimos 18 meses, é quase aquilo que teríamos em alguns anos de trabalho, e o tecido empresarial português não estava pronto para esta revolução", reflete Maria Malhão, Small Medium Business Lead na Microsoft. Estela Brandão de Bastos, CEO e Owner BDM na Visual Thinking, acrescenta que, "à boa portuguesa, houve um desenrascanço, o que não quer dizer que tenha sido feito da melhor forma". "Quando uma enorme quantidade de empresas no nosso país são micro e pequenas empresas, a transformação digital é muito mais do que um projeto *one-shot*", continua. É um "tecido empresarial complexo e é difícil ter um padrão comum", pelo que cada PME tem capacidades digitais e de investimento "completamente diferentes", complementa Maria Malhão.

O panorama é moldado pelo facto de grande parte das nossas empresas terem sido fundadas "entre os anos 70 e 80 e, portanto, a geração mais velha está na liderança. A transição geracional que estamos a fazer também é complexa na questão digital", refere Alexandre Meireles, Board Member na Startup Portugal. Completa: "o ponto chave do sucesso primeiro, vender o produto – as pessoas já ouviram tanto transformação digital e estão mais do que convencidas. Depois, fazer a implementação do processo, e, depois, o acompanhamento da implementação para dar continuidade".

ROI SUSTENTÁVEL

Segundo a Microsoft, "a sustentabilidade tem, hoje, um retorno no investimento que vai muito para além do impacto direto nas reduções de carbono", pelo que impacta as marcas, os investidores, os colaboradores e "toda a cadeia de valor". Para Miguel J. Martins, Sustainable Investments Partner at Grosvenor, um ROI sustentável "implica trabalhar capitais com os quais não trabalhamos".

- Andrés Ortolá, General Manager da Microsoft Portugal -

Assim, pensar em ROI sustentável é "ir além de medir o desempenho económico ou financeiro" e "passa por medir o capital humano e o capital natural". Nesse sentido, a tecnologia representa um papel fundamental: "ajuda-nos a fazer este trajeto de transferir dados, em informação, em conhecimento e, eventualmente, em sabedoria". "A sustentabilidade é criar valor, mas, muitas vezes, aquilo que nós sentimos é que estamos a criar valor económico-financeiro, mas estamos a destruir valor natural e humano", conclui.

Existe um sistema, desde 2015, "que nos ajuda a olhar para a sustentabilidade de forma mais sistemática, qua são os SDG" – *Sustainable Development Goals* – constituídos por 17 objetivos, refere Luís Costa, Partner e membro fundador da Get2C. "Acho que podemos começar por aí e depois cada empresa e projeto deve fazer a sua análise de materialidade para perceber o que é relevante para a organização a nível de sustentabilidade, depois para quem é relevante, a nível de stakeholders", assevera.

Nesse âmbito, Miguel J. Martins refere, contudo, que é complicado convencer as organizações a aplicar este tipo de métricas e utiliza a metáfora: "o tempo das cenouras acabou, temos de entrar no tempo do chicote – que, normalmente, vem sobre a forma de regulamentação". Já Filipe Almeida, Presidente da Estrutura de Missão Portugal Inovação Social, acredita que "o chicote no nosso tempo é a realidade concreta", explicando que "já não é preciso convencer as empresas a aderirem a um conjunto de estratégias de práticas sustentáveis, porque isso é a única forma de legitimarem a continuidade da sua atividade – o chicote está aí".

A ÉTICA DA INTELIGÊNCIA ARTIFICIAL

Substituto ou auxílio? Responsável ou discriminatória? Perigosa ou uma oportunidade? Estas foram algumas das questões debatidas no painel AI Ethics no primeiro dia do Building the Future 2022.

É de notar que a CE apresentou, no ano passado, a primeira proposta de legislação para a IA e também a UNESCO adotou a primeira recomendação ética de IA. Um dos debates, embora não só no campo da IA, prende-se

com as diferentes abordagens à tecnologia entre os EUA e a Europa, que, com princípios divergentes, poderia criar constrangimentos ao processo de adoção da tecnologia. Maria Manuela Leitão Marques, deputada no Parlamento Europeu, nota que "há diferenças, mas também muitos pontos de convergência. Os dois lados estão preocupados com o ritmo da inovação e com as questões éticas relacionadas com a IA", mas a UE tem uma abordagem mais "reguladora".

Não obstante, "temos que perceber que para que a inovação seja bem sucedida, é preciso que os cidadãos confiem" e "se não houver confiança, a inovação pode ter um retrocesso, e a ética contribui para criar essa confiança", que é fundamental para poder evoluir. Já Nádia da Costa Ribeiro, Senior Consultant na PLMJ, refere que "o grande desafio para o legislador tem a ver com uma disparidade entre os conceitos jurídicos e os conceitos técnicos", que dificulta a "confluência de incorporar nos algoritmos conceitos jurídicos, para que depois respeitem princípios éticos".

Mais, discutiu-se a importância de a legislação ser acordada internacionalmente. Nádia da Costa Ribeiro refere que "se for feita por Estado, corremos o risco de ter uma fragmentação dos vários princípios e valores, para começar porque corremos o risco de misturar ética com moral", porque os Estados têm conceções diferentes da importância dos valores.

O dilema do legislador é "encontrar o equilíbrio", assegura a deputada, porque não pode ser "totalmente a favor da proteção, paralisando a inovação, nem totalmente a favor da inovação, sem nenhuma confiança por parte dos cidadãos", refere a deputada. Contudo, assegura que "as empresas estão conscientes" do tema e tem havido uma "discussão muito ativa no Parlamento".

Uma dificuldade apontada por Nádia da Costa Ribeiro é que "o regulador tem algumas dificuldades de se manter a par da evolução tecnológica", mas "cada vez mais os regulados têm vindo a interagir com os reguladores para que a regulação não fique cristalizada no tempo e se mantenha a par da atualidade". A deputada do Parlamento Europeu conclui falando da necessidade de "aproximar os cidadãos do debate", apostando "nas competências digitais, mas não apenas as competências básicas de há uns anos. Hoje, a literacia básica deve incluir, também, saber o que é um algoritmo, dados, IA, etc", completa.

UM ANO DE BALANÇO POSITIVO

A quarta edição do Building the Future contou com uma equipa de cerca de 170 pessoas na organização, 150 mil visualizações únicas, 365 oradores em 180 sessões ao longo de mais de 65 horas de transmissão online, disse a Microsoft em comunicado. Mesmo em contexto pandémico, "voltámos a fazer um evento extremamente inovador, recorrendo, inclusivamente, pela primeira vez em Portugal, a um sistema de realidade aumentada orgânica", reforçou Teresa Virgínia. Andres Ortolá conclui: "assistimos ao que de melhor se faz no país e testemunhámos como a transformação digital é o motor do futuro". ■

MANAGED DETECTION & RESPONSE

24/7 managed services to monitor, detect and act against cybersecurity incidents

SIBS®
CyberWatch

A CONTÍNUA NECESSIDADE DA CIBERSEGURANÇA

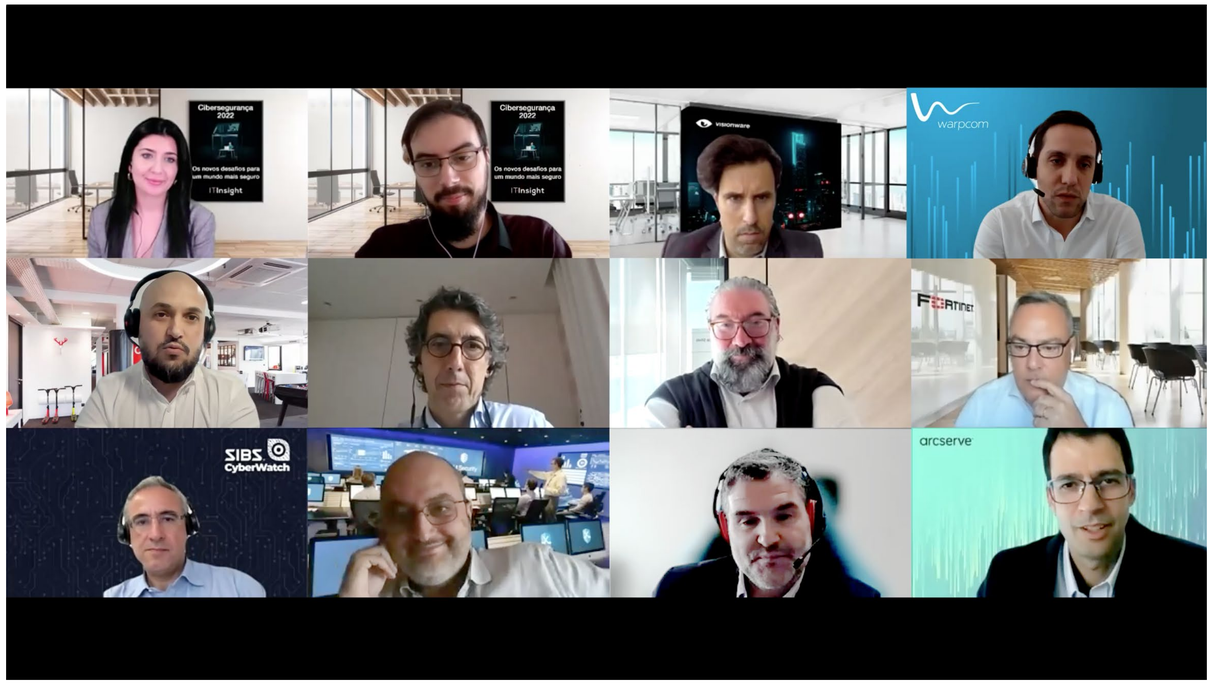
A necessidade de uma boa proteção aumentou para todas as organizações. Qualquer empresa – mesmo as mais pequenas – está em risco de ser atacada e, como tal, tem de se precaver das muitas ciberameaças existentes. Arcserve, Bitdefender, Claranet, Fortinet, IBM, Microsoft, Multicert, S21sec, VisionWare e Warpcom partilham a sua opinião sobre os desafios atuais da cibersegurança.

RUI DAMIÃO

O MUNDO MUDOU muito rapidamente desde que a pandemia chegou em 2020 e isso tem sido particularmente útil para os cibercriminosos. Trabalho em casa, digitalização contínua da sociedade e a natureza cada vez mais online das nossas vidas são sinónimos de oportunidades para cibercriminosos que conseguem explorar essas fragilidades.

À medida que avançamos em 2022, infelizmente, não há sinal de abrandamento. É por isso essencial que as organizações estejam cientes das crescentes vias de ataque, bem como do que pode ser feito para mitigar os riscos.

As principais empresas a operar no mercado de cibersegurança partilham a sua experiência para ajudar as organizações a mitigar ao máximo os ciber-riscos existentes.



- Rui Ribeiro, IBM -

- David Grave, Claranet Portugal -

O NÚMERO DE CIBERATAQUES EM PORTUGAL TEM VINDO A AUMENTAR, COM ALGUNS A TORNAREM-SE BASTANTE MEDIÁTICOS RECENTEMENTE. ESTA É UMA TENDÊNCIA QUE AS EMPRESAS PORTUGUESAS PODEM ESPERAR QUE VÁ CONTINUAR A ACONTECER?

RUI RIBEIRO, SECURITY SALES LEADER, IBM: "*Se desenharmos uma linha referente às últimas semanas, essa linha seria excessivamente alta e corresponderia a uma tendência que pode não ser a real. Mas há um conjunto de indicadores que apontam para um crescimento do número de ciberataques. Mais importante que o número de ciberataques é discutir as consequências e perceber o que pode haver como root cause de algumas destas tendências relativamente ao mercado*"

DAVID GRAVE, SENIOR CYBERSECURITY CONSULTANT, CLARANET PORTUGAL: "*A nova metodologia de ataques altamente direcionados para alvos que vão ter um elevado impacto vão garantir um maior retorno aos grupos de atacantes. Os ataques não vão diminuir porque são altamente lucrativos e o risco, neste momento, é muito diminuto. Vemos algumas organizações e algumas iniciativas para travar isto, mas neste momento ainda são iniciativas muito isoladas e limitadas no espectro*"

JOÃO MACHADO, VP SALES, S21SEC PORTUGAL: "*Na defesa, tentamos ter automatismos, mas do lado atacante começam a ter muita capacidade de automatismo e isso faz aumentar o número dos ataques. O que temos verificado é cada vez mais setores a serem atacados, com um relevo bastante grande para a componente industrial. Os ataques estão a explorar cada vez mais o OT e vão saltar para o lado das infraestruturas críticas e componentes industriais*"

BRUNO GONÇALVES, BUSINESS UNIT MANAGER CYBERSECURITY, WARPCOM: "*O mundo está altamente dependente da tecnologia. O awareness que os ciberataques têm criado junto do público em geral e dentro das organizações acaba por tornar-se num ponto relevante. Já não é algo que seria uma maior probabilidade; é algo que acontece, que as pessoas vivem e sentiram o impacto no seu dia a dia e isso é uma tomada de consciência de quão impactante e quanto estamos dependentes da tecnologia*"

PAULO PINTO, BUSINESS DEVELOPMENT MANAGER, FORTINET: "*Para inverter esta tendência, as organizações terão de lidar com situações imprevistas num futuro desconhecido. É preciso ter um conjunto de capacidades para, quando passarem por uma série de situações, estarem preparadas as ultrapassar. As organizações têm de fazer o trabalho de casa, olhar para as suas infraestruturas, para as áreas como endpoints, acessos, segurança da rede,… os elementos chave*"

AS CIBERAMEAÇAS SÃO CADA VEZ MAIORES. A CIBERSEGURANÇA É, AGORA, UM INVESTIMENTO MAIS PRIORITÁRIO? DEPOIS DESTE INÍCIO DE ANO UM POUCO MAIS ATÍPICO – PELO MENOS EM TERMOS DE MEDIATISMO – SENTEM QUE HÁ MAIS EMPRESAS A PROCURAR SOLUÇÕES DE CIBERSEGURANÇA?

PEDRO BARBOSA, CEO DA MULTICERT E HEAD OF SIBS CYBERWATCH: "*As ciberameaças têm cada vez mais impacto e, por isso, é que é um tema cada vez mais prioritário, a entrar na agenda da gestão de topo e com toda a razão. Ainda existe uma grande dificuldade e um desafio pelo caminho porque temos de passar tudo aquilo que são os valores operacionais e traduzi-los em risco de negócio e não é assim tão fácil. Observamos uma atenção maior para as áreas de cibersegurança*"

- Bruno Gonçalves, Warpcom -

- Miguel Caldas, Microsoft -

MIGUEL CALDAS, SENIOR CLOUD SOLUTION ARCHITECT, MICROSOFT: "*Desde o princípio deste ano, metade das minhas reuniões com parceiros e clientes envolve o tema de cibersegurança. Isto evidencia que as pessoas andam distraídas, porque o aumento não é só de agora. Desde que os computadores começaram a estar ligados à rede que os ciberataques aumentam. Aquilo que aumentou solidamente nos últimos tempos é a atenção que é dada pelas organizações ao tema da ciberdefesa*"

VASCO SOUSA, CHANNEL ACCOUNT MANAGER, ARCSERVE: "*Todas as empresas da área de informática conhecem concorrentes, clientes ou fornecedores que já sofreram ataques de ransomware ou outros. Perceber que uma empresa não está a operar faz as organizações começarem a pensar e a fazer as contas do que significa para si e para o negócio se sofrerem o mesmo. A superfície de ataque é cada vez maior e temos cada vez mais equipamentos a aceder a dados*"

BRUNO CASTRO, FUNDADOR E CEO, VISIONWARE: "*Grande parte das empresas – públicas ou privadas – estão à procura de soluções, quase como uma vacina mágica para o que tem acontecido, mas isso não existe, é um processo. Acredito numa abordagem na ótica de gestão de risco e procurar a solução certa – seja pessoas, procedimentos ou tecnologia – para cada caso em concreto e há uma tendência clara de procurar uma solução milagrosa que não existe*"

SERGIO BRAVO, REGIONAL SALES MANAGER IBERIA, BITDEFENDER: "*O que temos vivido nos últimos tempos com o tema da pandemia fez com que as empresas tomem mais consciência da necessidade de investir em cibersegurança porque todas as empresas têm de manter a continuidade do seu negócio. A pandemia – com todo o confinamento, teletrabalho e, agora, o voltar ao escritório – fez com que a superfície de ataque aumentasse porque o perímetro é muito distribuído*"

ATRAVÉS DOS SEUS DISPOSITIVOS, OS COLABORADORES TÊM CADA VEZ MAIS ACESSO À INFORMAÇÃO CORPORATIVA. O QUE DEVEM AS ORGANIZAÇÕES FAZER PARA PROTEGER EFICAZMENTE ESTA INFORMAÇÃO NOS DIFERENTES TERMINAIS?

PAULO PINTO, BUSINESS DEVELOPMENT MANAGER, FORTINET: "*Falamos de vetores de ataque e na capilaridade que existe na proteção da rede e isso vem, essencialmente, destes pontos móveis dos endpoints. As soluções de proteção desses endpoints são incontornáveis em qualquer arquitetura de segurança. A parte dos antivírus evoluiu e está hoje muito sofisticada, com algoritmos de inteligência artificial. Hoje, os softwares colaboram na parte da deteção e na resposta*"

- Paulo Pinto, Fortinet -

JOÃO MACHADO, VP SALES, S21SEC PORTUGAL: "*É fundamental saber, conhecer, manter e atualizar a política de segurança da empresa, qual é a informação mais crítica, como é que cada um dos seus utilizadores, departamentos e colaboradores fazem a gestão da informação. Também temos de ser capazes de implementar um conjunto de tecnologias que nos podem defender melhor, desde um simples de multifator de autenticação até toda a parte de identidade e acesso*"

DAVID GRAVE, SENIOR CYBERSECURITY CONSULTANT, CLARANET PORTUGAL: "*A migração das pessoas para fora das organizações levou a que a proteção de perímetro tenha deixado de ser a solução absoluta; não chega e não serve por as pessoas a trabalhar por VPN. Se o colaborador leva o computador para casa e se liga à organização por VPN, está a trazer para dentro da organização uma potencial panóplia de problemas de que muitas organizações não vão sequer ter visibilidade*"

SERGIO BRAVO, REGIONAL SALES MANAGER IBERIA, BITDEFENDER: "*Para que as empresas possam proteger todo este crescimento que existiu, tem de se adaptar a esta nova tendência que existe, o conceito de ciber-resiliência. O que propomos é uma tecnologia de proteção por camadas. Para além das tradicionais, são precisas camadas mais avançadas, como machine learning e inteligência artificial, para proteger o dispositivo do maior número de ameaças que estão a surgir*"

MIGUEL CALDAS, SENIOR CLOUD SOLUTION ARCHITECT, MICROSOFT: "*O aumento das soluções de segurança centradas no dispositivo vai continuar. No entanto, o zero-trust é extraordinariamente importante. Hoje, as aplicações assumem que, se um utilizador chegou ali, é porque o pode fazer. A maneira de desenvolver código tem de mudar para que uma aplicação nunca faça nada sem ter a certeza de quem é que está a mandar e que quem está a mandar tem o direito de o fazer*"

- Pedro Barbosa, SIBS Cyberwatch -

PEDRO BARBOSA, CEO DA MULTICERT E HEAD OF SIBS CYBERWATCH: "*Há medidas que são mais demoradas de implementar e têm estratégias, mas há outras que, num determinado nível de realidade, acabam por ser quick wins ou fáceis de implementar. A autenticação de dois fatores é importante uma vez que uma parte considerável das ameaças entram via endpoint/colaborador e de diferentes técnicas. Se não conseguimos prevenir tudo, temos de ser muito rápidos a detetar e a defender*"

BRUNO CASTRO, FUNDADOR E CEO, VISIONWARE: "*Vemos imensa tecnologia disponível, alguma mais ou menos implementada, que dá uma sensação de conforto – no meu entender – falsa. Todos os que têm tecnologia implementada têm de testar vezes sem conta a componente de proteção, de deteção, de recuperação. É fundamental testar a tecnologia, as pessoas e os processos numa única visão. Há empresas que investem e continuam a sofrer ciberataques*"

É UMA QUESTÃO DE TEMPO ATÉ QUE A ORGANIZAÇÃO SEJA ATACADA E QUE ESSE CIBERATAQUE TENHA ALGUM TIPO DE SUCESSO. QUAL É A IMPORTÂNCIA ATUAL DO BACKUP, DA RESTAURAÇÃO DO BACKUP/DADOS E DOS PLANOS DE DISASTER RECOVERY?

VASCO SOUSA, CHANNEL ACCOUNT MANAGER, ARCSERVE: "*A perceção de que é uma questão de tempo está a ficar cada vez mais visível. Os backups eram uma coisa ultra desinteressante e, hoje, há consciência de que são estratégicos para qualquer empresa. O backup é a última linha de defesa; não é a única. Não é por poderem ser ultrapassadas diversas camadas que vamos descurá-las; não é por sabermos que as portas podem ser arrombadas que vamos deixar de ter uma porta em casa*"

- Vasco Sousa, Arcserve -

RUI RIBEIRO, SECURITY SALES LEADER, IBM: "*Reforço que há uma necessidade de cibersegurança na ciber-resiliência e a importância da bidirecionalidade destas duas disciplinas. Organizacionalmente, separou-se estas duas componentes e tudo o que é backup e recovery fica, tipicamente, do lado do IT, e tudo o que é operações de segurança fica, tipicamente, do lado da segurança. Não é incomum ver isto no mercado, mas é preciso ver este tema de forma integrada*"

BRUNO GONÇALVES, BUSINESS UNIT MANAGER CYBERSECURITY, WARPCOM: "*A organização não pode olhar para o backup como uma salvaguarda em caso de um ataque. O plano de disaster recovery é essencial; não basta ter backups, é preciso testá-los, perceber se de facto o tipo de abordagem é adequado à organização e como é que a informação está a ser salvaguardada para, no momento em que preciso, tenho, de facto, a informação que é fundamental para garantir a operação*"

A FIGURA DO CISO, OU DE UM QUADRO DEDICADO EQUIVALENTE NAS ORGANIZAÇÕES, TEM VINDO A CRESCER ASSIM COMO EQUIPAS INTERNAS DEDICADAS. FACE À ESCASSEZ DE TALENTOS, E RACIONALIZAÇÃO DE CUSTOS, QUAL O PAPEL QUE O SECURITY-AS-A-SERVICE (SECAAS) E OUTRAS FORMAS DE EXTERNALIZAÇÃO PODEM DESEMPENHAR E COMO ESCOLHER O PARCEIRO CERTO?

DAVID GRAVE, SENIOR CYBERSECURITY CONSULTANT, CLARANET PORTUGAL: "*Deparamo-nos todos os dias com as questões da cibersegurança a caírem exclusivamente na equipa de IT. O mindset da cibersegurança é diferente do mindset de montar a operação. As equipas devem ter dentro de casa alguém que tenha o know-how de cibersegurança e que possa servir como um CISO ou um ponto de contacto, mas a externalização acelera a adoção de tecnologia e suporte necessário para estes temas*"

PEDRO BARBOSA, CEO DA MULTICERT E HEAD OF SIBS CYBERWATCH: "*Se recuarmos uns nove anos, quando esta indústria começou a acontecer, o que observámos foi que existiam milhões de postos de trabalho por preencher. O acelerar da transformação digital acabou por trazer muitas mais necessidades. O papel dos fornecedores especializados nesta área tem particular relevância para endereçar áreas que são cada vez mais fulcrais para as organizações se tornarem mais ciber-resilientes*"

- João Machado, S21sec Portugal -

JOÃO MACHADO, VP SALES, S21SEC PORTUGAL: "*Todos nós, enquanto empresas nesta área, sentimos a falta de recursos e vamos continuar a sentir falta. Mesmo com a criação de automatismos para libertar pessoas de tarefas mais rotineiras para níveis de especialização um bocadinho maiores, é preciso tempo para preparar realmente cada uma destas pessoas. Assim, este gap vai continuar a existir e temos de estar preparados para viver com ele*"

BRUNO GONÇALVES, BUSINESS UNIT MANAGER CYBERSECURITY, WARPCOM: "*Há um ponto fundamental: na cibersegurança, a questão do 24/7, garantir que a organização tem permanentemente alguém ou um serviço que garanta a monitorização e uma capacidade de reação a qualquer momento torna ainda mais evidente a escassez de talento. É impossível pensar que vamos ter todas as organizações com uma capacidade de resposta através de equipas internas que garantam esta prestação de serviços*"

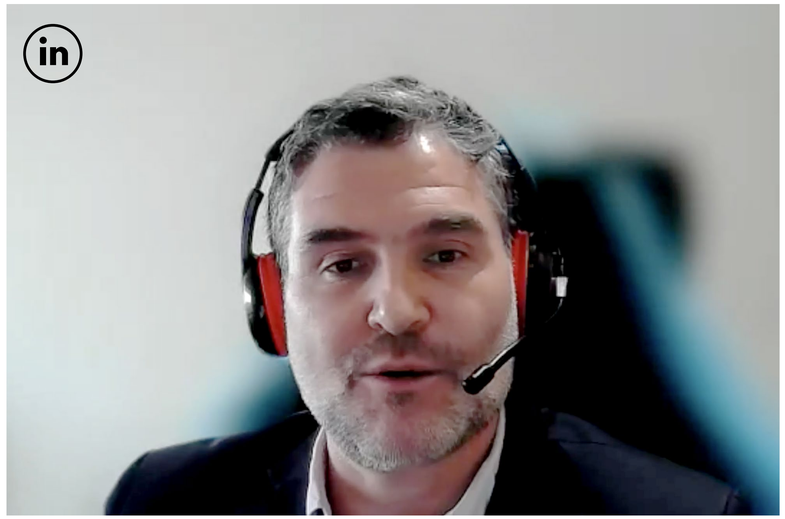
BRUNO CASTRO, FUNDADOR E CEO, VISIONWARE: "*No mercado de outsourcing, temos de estar disponíveis 24/7. Encontrar alguém com experiência, disponibilidade e conhecimento é muito difícil e é uma variável muito valiosa que não há. O mercado mudou e vai ter de escolher as empresas com quem vai querer trabalhar. É preciso passar por um enquadramento estranho em que é necessário dizer a um potencial cliente que não vamos porque não temos man power para isso*"

- Bruno Castro, VisionWare -

EM TERMOS DE CIBERAMEAÇAS, QUAIS SÃO AS TENDÊNCIAS A QUE AS ORGANIZAÇÕES DEVEM TER ESPECIAL ATENÇÃO E PROTEGER-SE E QUAIS SÃO AS SOLUÇÕES MAIS PROCURADAS?

RUI RIBEIRO, SECURITY SALES LEADER, IBM: "*É preciso repensar o que se tem do ponto de vista de parque tecnológico face ao que se pretende ter, que são resultados concretos. Nem sempre a lógica de comprar uma nova tecnologia para cumprir mais uma caixinha de requisitos funciona; há coisas onde se pode reutilizar o que tenho e outras onde se pode deitar fora. Outra tendência que vejo é a perceção de que é, de facto, uma questão de tempo até ser atacado*"

SERGIO BRAVO, REGIONAL SALES MANAGER IBERIA, BITDEFENDER: "*O ransomware já se profissionalizou e, como tal, já é possível contratar este tipo de ataques para atingir uma organização. Temos assistido a uma evolução dentro do que é tipo de ransomware, a reutilização de código em diferentes grupos de cibercriminosos que desaparecem e reaparecem, se associam entre si para cada um atacar a sua parte. No final, a verdade é que é um negócio*"



- Sergio Bravo, Bitdefender -

MIGUEL CALDAS, SENIOR CLOUD SOLUTION ARCHITECT, MICROSOFT: "*O CISO ou o Security-as-a-Service nem são uma solução para uma empresa que tem cinco ou dez trabalhadores; não têm um departamento de IT. Tem de ser a tecnologia a fornecer a melhor solução possível dentro do budget disponível nessas organizações, que não conseguem contratar as empresas que fornecem serviços de elevadíssima qualidade, mas não suprem as necessidades de alguém que tem 20 trabalhadores*"

VASCO SOUSA, CHANNEL ACCOUNT MANAGER, ARCSERVE: "*Na proteção de dados, a solução que se pretende é que os dados estejam acessíveis e disponibilizados. Antes, falava-se em sistemas WORM – Write Once, Read Many. Hoje, fala-se mais em imutabilidade de dados; isto significa que, depois de escrito os dados, não podem ser nem alterados nem apagados. Isto responde à tal situação em que os dados são apagados ou encriptados e é possível chegar a isso de diferentes formas*"

PAULO PINTO, BUSINESS DEVELOPMENT MANAGER, FORTINET: "*Há uma coisa que me preocupa que é a questão legislativa. O facto de ter saído uma legislação com uma área de aplicabilidade muito grande, para empresas que não têm ainda um grau de maturidade elevado, vai desfocá-las. Tem poucos recursos e vão querer cumprir com a legislação e o compliance, então vão fazer um esforço enorme para analisar os pontos todos, mas não têm essa capacidade*" ■

arcserve®

POR FLORIAN MALECKI,
Vice President International Marketing
da Arcserve

4 TENDÊNCIAS DE PROTEÇÃO DE DADOS PARA TER EM ATENÇÃO EM 2022

Na economia digital dos nossos dias, é mais importante do que nunca proteger os dados empresariais contra danos, destruições ou ataques e a viabilidade de qualquer empresa depende do acesso constante aos respetivos sistemas e dados fundamentais.

ISSO IMPLICA MONITORIZAR permanentemente o panorama de dados e prestar atenção aos novos desafios e ferramentas, bem como de estar a par das normas de privacidade e das ameaças de segurança. Apresentamos aqui quatro tendências emergentes que irão moldar a forma como as empresas irão abordar a proteção e gestão de dados em 2022.

1: A SUPERFÍCIE DE ATAQUE CONTINUARÁ A EXPANDIR-SE COM AS NOVAS FORMAS DE TRABALHO.

A sua superfície de ataque inclui todas as formas possíveis de que um atacante dispõe para aceder aos dispositivos e redes da sua empresa e bloquear ou extrair os seus dados. Assim sendo, é essencial reduzi-la ao mínimo possível. O problema é que a superfície de ataque está em constante crescimento e mutação, à medida que cada vez mais pessoas trabalham remotamente em múltiplos dispositivos e criam cada vez mais pontos de entrada que permitem concretizar ciberataques. O próprio controlo de terminais é cada vez mais complexo, à medida que os colaboradores saem das organizações e a recuperação de equipamentos fica mais difícil.

Em suma, as falhas de segurança serão inevitavelmente uma realidade. Assim, no próximo ano, as empresas terão de reconhecer eventuais falhas de segurança, por forma

- Florian Malecki -
Vice President International Marketing da Arcserve

a conseguirem libertar-se das ameaças. À medida que a superfície de ataque aumenta, as estratégias devem ser mais minuciosas e abranger, não só os dados do data center interno, mas também os dados da nuvem, da linha da frente e de tudo o resto.

2: A SOBERANIA DOS DADOS IRÁ PROVOCAR UMA COMPLEXIDADE AINDA MAIOR AO NÍVEL DA GESTÃO DE DADOS.

Como as empresas têm crescido a nível mundial e têm ficado cada vez mais interligadas, as regras relativas à privacidade de dados tornaram-se muito mais complexas. Por exemplo, uma empresa com sede na Alemanha pode utilizar uma empresa sediada nos EUA, como a Amazon ou a Google, para armazenar e enviar dados. A questão que se coloca prende-se com a localização legal dos dados da empresa da Alemanha e as leis pelas quais são regidos. As respostas a estas questões são complexas e pouco claras.

Atualmente, a maior parte dos dados reside na cloud, ou seja, distribuída a nível mundial. Assim, os fornecedores de serviços na cloud terão de gerir com os clientes as questões de soberania e conformidade com as várias normas e jurisdições.

3: OS PROBLEMAS DA CADEIA DE ABASTECIMENTO GLOBAL TRANSFORMAR-SE-ÃO NUM PROBLEMA DE PROTEÇÃO DE DADOS.

Os problemas da cadeia de abastecimento estão a provocar interrupções significativas na economia mundial, sendo que a oferta é escassa em todos os setores e ao que tudo indica, estes problemas irão persistir ao longo de 2022.

Os ciberataques irão provocar ainda mais perturbações na cadeia de abastecimento global no próximo ano. Em 2021, o ataque de ransomware ao Colonial Pipeline desativou o maior oleoduto dos EUA e originou faltas de combustível ao longo de toda a Costa Leste. A empresa pagou um resgate aos piratas informáticos de, aproximadamente, 5 milhões de dólares.

Em 2022 as organizações terão de garantir que os ciberataques não comprometem ainda mais as cadeias de abastecimento e que os dados permanecem sempre disponíveis, podendo ser recuperados de imediato.

4: O ENCARREGADO DA PROTEÇÃO DE DADOS TERÁ IMPORTÂNCIA ESTRATÉGICA.

Os Encarregados da Proteção de Dados são responsáveis por possuir conhecimentos especializados sobre as leis e práticas de proteção de dados, enquanto supervisionam a estratégia de proteção de dados da empresa e asseguram a conformidade com os requisitos do RGPD.

O papel do DPO prepara-se para crescer em termos de importância estratégica, em especial à medida que as responsabilidades dos DPO passam a englobar uma visão holística da privacidade de dados, da segurança e da educação.

À medida que as empresas armazenam cada vez mais dados em sistemas híbridos, de terceiros, nas instalações ou na cloud, e à medida que os regulamentos de dados crescem e se multiplicam, as empresas devem manter-se no topo do panorama de dados em permanente evolução, ou arriscam afundar-se por completo. ■

Bitdefender
BUILT FOR RESILIENCE

POR SERGIO BRAVO,
Diretor de Vendas da Bitdefender

APT, UMA AMEAÇA CIBERNÉTICA CADA VEZ MAIS DIFUNDIDA

De acordo com um relatório do Identity Theft Resource Center, o número de incidentes de segurança nos primeiros nove meses de 2021 foi 17% superior ao registado durante todo o ano de 2020.

NUM CENÁRIO COMO ESTE, as organizações devem analisar cuidadosamente as suas capacidades de deteção e resposta face a possíveis ameaças, e tudo indica que o início do ano é o momento em que muitos deles optam por reavaliar as suas estratégias de cibersegurança, adotando decisões focadas na redução de riscos e na capacidade de se defenderem melhor.

Normalmente, ao estabelecer prioridades de segurança, **são tidos em conta fatores como o orçamento disponível, a situação da empresa no que respeita à tolerância ao risco ou ao cumprimento de diferentes regulamentos**. Além disso, se o estado das diferentes ameaças for cuidadosamente analisado, verificar-se-á que este ano, além de considerar as modalidades de ransomware, *phishing* e vulnerabilidades de zero-day, as empresas também devem estar atentas à evolução de ameaças persistentes avançadas (APT).

Até relativamente recentemente, as APT eram uma prática muito sofisticada, que para se desenvolver adequadamente necessitava de ter os recursos de um Estado ou de um grupo muito poderoso de cibercriminosos. Ultimamente, estamos a ver como este tipo de ataque *está a generalizar-se em todo o mundo.*

Geralmente, as APT são concebidas para atingir metas com implicações a nível nacional: espionagem política, roubo de propriedade intelectual, boicotes de infraestruturas críticas... Muitos ataques têm-se centrado na compilação de informações, afetando infraestruturas públicas críticas, em que os cibercriminosos são responsáveis pela exploração de vulnerabilidades que lhes permitem maximizar a recolha de dados confidenciais com o mínimo de esforço.

Tudo indica que campanhas de *hacking* que anteriormente exigiam meses de planeamento e competências informáticas de alto nível para superar defesas e mover-se através de redes sem serem detetadas já não são reservadas para atores apoiados pelo Estado.

Hoje, estes recursos estão disponíveis para qualquer um. Podem ser comprados e vendidos na Dark Web como um produto ou serviço. Não é que as APT tenham mudado, é que agora é mais simples para qualquer cibercriminoso aceder às ferramentas básicas para levar a cabo uma iniciativa deste tipo.

A evolução da tecnologia, com cada vez mais empresas a moverem dados sensíveis para a cloud e a incorporarem dispositivos conectados nas suas operações, faz com que a superfície de ataque seja maior e mais atrativa para este tipo de ameaças.

Os organismos públicos e as grandes empresas sempre foram um alvo claro dos grupos de APT. No entanto, as PME estão agora também no centro das atenções, uma vez que os cibercriminosos provaram que são um bom ponto de entrada para atingir objetivos maiores.

PROTEÇÃO CONTRA APT

Quando se trata de se protegerem, há uma série de passos que todas as organizações teriam de considerar.

Em primeiro lugar, é essencial que cada empresa conheça e compreenda o seu próprio estado de segurança, identificando os fatores que a podem colocar em risco.

A partir daí, precisam de desenvolver as suas capacidades de proteção. Na maioria dos casos, implementar uma solução de Deteção e Resposta Alargada (XDR) pode ajudar os responsáveis de segurança a identificar ameaças e padrões. Além disso, quando não tiver recursos internos suficientes, a contratação de um serviço de deteção e resposta gerido (MDR) será essencial para poder ter suporte de segurança, gestão do ambiente e pesquisa de ameaças 24 horas por dia, incorporando uma abordagem mais automatizada e analítica às suas próprias capacidades de segurança.

Para se proteger das APT, tem de ser proativo. É necessário alcançar um orçamento equilibrado para poder integrar tecnologias de prevenção, deteção e resposta, mas deixar claro que não é conveniente confiar tudo à tecnologia. Também é bom ter recursos qualificados e conhecer a rede em profundidade para ser capaz de analisar e determinar o que a empresa precisa em todos os momentos. Se uma infraestrutura robusta for desenvolvida, os incidentes de segurança podem ser geridos mais facilmente. ■

claranet

POR DAVID GRAVE,
Senior Cybersecurity Consultant,
Claranet Portugal

A CIBERSEGURANÇA COMO RESPONSABILIDADE PARTILHADA

Os ciberataques com elevado impacto nas organizações e na sociedade estão longe de ser novidade e tendem a aumentar. É tempo, por isso mesmo, de partilhar responsabilidades na resposta às novas ciberameaças.

EM DEZ ANOS O MUNDO MUDOU de forma significativa e, mesmo que seja um cliché usado neste contexto, a verdade é que toda a nossa vida pessoal e profissional passou a ter uma enorme dependência da Internet, ficando à mercê de serviços ou tecnologias dos quais dependemos para executar muitas tarefas diárias.

Ao tornarmo-nos mais dependentes da tecnologia, tornámo-nos também mais vulneráveis ao cibercrime, à fraude nas redes sociais e ao *phishing*. O trabalho remoto acabou por reforçar esta dependência e, sobretudo, expôs o problema real: a falta de consciencialização dos utilizadores sobre cibersegurança.

A *cibersegurança* é agora uma responsabilidade partilhada, em que cada um de nós precisa de desempenhar um papel. As organizações já começaram a perceber que podem ser a próxima vítima e que basta um único computador infetado para comprometer toda a organização, potenciando um ataque com prejuízos avultados.

Neste contexto, todos devemos tomar medidas básicas de cibersegurança que possam melhorar a proteção individual, coletiva e organizacional.

NOVA TIPOLOGIA DE ATAQUES

À medida que a tecnologia avança, avançam também as técnicas que os cibecriminosos usam. Esta-

- David Grave -
Senior Cybersecurity Consultant da Claranet Portugal

mos atualmente a testemunhar o fim da primeira vaga de cibercrime, onde os ataques eram vastamente indiscriminados e os valores pedidos significativos, mas transversais. Entramos agora a grande velocidade numa segunda vaga, mais profissional e organizada, com uma atuação multinível: há grupos especializados na identificação dos alvos e na sua exploração inicial e, após esse trabalho, outros grupos assumem a responsabilidade pela concretização do ataque, usando ferramentas altamente sofisticadas - muitas vezes desenvolvidas por um terceiro grupo -, partilhando depois entre si os resultados da ofensiva.

Os ataques são agora mais direcionados e os valores pedidos têm em conta o poder financeiro das organizações, assim como as perdas diárias que estejam a sofrer. Muitos atacantes passaram a exigir valores baseados numa complexa equação entre o lucro que conseguem e o custo real para a empresa, mantendo esses valores baixos o suficiente para que as organizações ponderem o seu pagamento face aos valores que irão perder no negócio – atendendo ao tempo que irão demorar até ter os seus sistemas estáveis, operacionais e seguros novamente.

O ciberataque à Vodafone esteve longe de ser o primeiro contacto com um ataque em grande escala a uma infraestrutura crítica, mas foi o que teve as repercussões socioeconómicas mais visíveis em Portugal. Infelizmente, esta categoria de ataques já não é uma novidade - é o chamado "novo normal". Quanto ao panorama nacional, apesar de todas as dificuldades no setor público e no privado, ambos com as suas peculiaridades, vemos uma evolução positiva tanto na consciencialização do C-Level, como no empenho dos profissionais. A cibersegurança é agora uma prioridade emergente.

A FORMAÇÃO COMO SOLUÇÃO

Não existem propriamente soluções mágicas para nos proteger de todas as categorias de ciberameaças. Mesmo que os investimentos tecnológicos sejam importantes, é necessário continuar a investir na *formação dos colaboradores*. Até porque as soluções tecnológicas requerem técnicos altamente especializados - que são escassos, dada a elevada procura -, e um seguro de ciber-risco, por si só, dificilmente nos protege de danos reputacionais. A cibersegurança é um processo cíclico e metódico. Assim, é fundamental sabermos onde estamos e qual o objetivo que pretendemos atingir. Para isso é necessário escolher as referências adequadas à nossa indústria, usar boas práticas como um guia prescritivo e investir em serviços que nos deem garantias de qualidade e capacidade de resposta. E, claro está, testar, testar, testar! *Testar*: esse é o mote que as organizações deverão seguir para garantir a segurança das aplicações, das infraestruturas e da cloud – incluindo os *backups* –, sem esquecer as equipas, as soluções de cibersegurança e os processos. É cada vez mais importante garantir uma *resposta a incidentes* como forma de dar continuidade aos negócios.

Só assim conseguiremos saber em que medida estamos preparados para lidar com este “novo” desafio e, desta forma, detetar, mitigar e recuperar dos seus impactos. ■

FORTINET

POR JOHN MADDISON

AS VANTAGENS DA SEGURANÇA INTEGRADA COM A FORTINET LAN EDGE

De um modo geral a lan apresenta-se como um potencial alvo para ataques de cibercriminosos. Muitas das soluções no mercado não têm segurança integrada, sendo necessário adicionar soluções extra que aumentam a complexidade e os custos.

Os utilizadores querem conexões de Internet e WI-FI mais rápidas; o IT quer soluções seguras e que, idealmente, reduzam a complexidade para se focarem em iniciativas estratégicas e perderem o mínimo de tempo possível com problemas comuns.

A segurança não está habitualmente integrada no *LAN edge*, o que pode levar a que as configurações não fiquem bem feitas e possam ser uma porta de entrada para ciberataques. Quando se trata de gerir o LAN edge, as organizações enfrentam vários desafios:

- Manter sincronizadas diferentes configurações;
- Ter visibilidade de toda a rede;
- Gerir diferentes níveis de acesso;
- Lidar com um alto Total Cost of Ownership (TCO).

Para endereçar esses desafios e gerir melhor uma rede segura, cada vez mais organizações estão a considerar abordagens de plataforma integrada ou uma arquitetura *meshed* de cibersegurança.

TRÊS VANTAGENS NA CONVERGÊNCIA DE REDE E SEGURANÇA

1. Configuração Simples – Em redes de grande dimensão, fazer uma pequena mudança pode ter um efeito em cascata e interromper outras áreas da rede. A equipa de IT tem de ter a certeza de que quaisquer alterações ou atualizações podem ser seguidas e geridas, para que todas as áreas da rede permaneçam operacionais. O trabalho necessário para instalar e supervisionar um padrão comum em muitos locais remotos e tipologias diferentes pode esgotar rapidamente os recursos de IT. As *soluções de rede integradas orientadas para segurança* são mais fáceis de dimensionar e crescer, sem sacrificar a segurança das mesmas.

2. Melhor visibilidade para uma gestão mais fácil – As redes atuais estão a mudar constantemente com dispositivos de colaboradores e convidados a entrar e a sair da rede em todos os momentos. A visibilidade típica do LAN edge pode fornecer detalhes sobre as conexões do dispositivo, mas pode faltar o contexto do dispositivo da camada superior. O número cada vez maior de dispositivos de *Internet das Coisas (IoT)* é um desafio particular em termos de visibilidade uma vez que, à medida que aparecem na rede, as aplicações devem ser autorizadas sem colocar em risco a segurança geral da rede. Em locais sem equipa de IT, lidar com dispositivos IoT pode ser ainda mais desafiador já que as informações na interface da camada de acesso são as únicas fornecidas.

3. Menor TCO – Mesmo que as soluções possam fornecer a visibilidade e a gestão que uma organização precisa, os custos cumulativos de licenciamento, ativação e subscrição de recursos vão aumentar progressivamente. As organizações devem seguir cuidadosamente a quantidade de sistemas e soluções que precisam de ser adquiridos para que tudo funcione como esperado. É necessário determinar quantas licenças precisam e se os vários recursos precisam de assinaturas recorrentes. O cálculo do custo de propriedade também precisa de ter em consideração o tempo da equipa. O tempo necessário para implementar e fazer a manutenção das operações também pode variar bastante entre as soluções, o que torna importante perceber o quão complicado é gerir uma determinada solução e se precisa de produtos adicionais para funcionar corretamente. A consolidação de soluções com uma abordagem de plataforma *mesh* de alto desempenho pode simplificar drasticamente o licenciamento e reduzir os custos.

SEGURANÇA INTEGRADA PARA REDUZIR A COMPLEXIDADE

As soluções integradas permitem simplificar a arquitetura de rede e podem aliviar o trabalho de configuração e gestão da equipa de IT. Isto aplica-se não só à LAN, mas também a *SD-WAN* e *ZTNA*. Ao implementar uma plataforma adaptável e integrada, as organizações podem eliminar a expansão de dispositivos, configuração e licenciamento. Esta abordagem economiza tempo e dinheiro para que as organizações possam cumprir os seus objetivos de negócios, mantendo a gestão diária da rede simples. ■

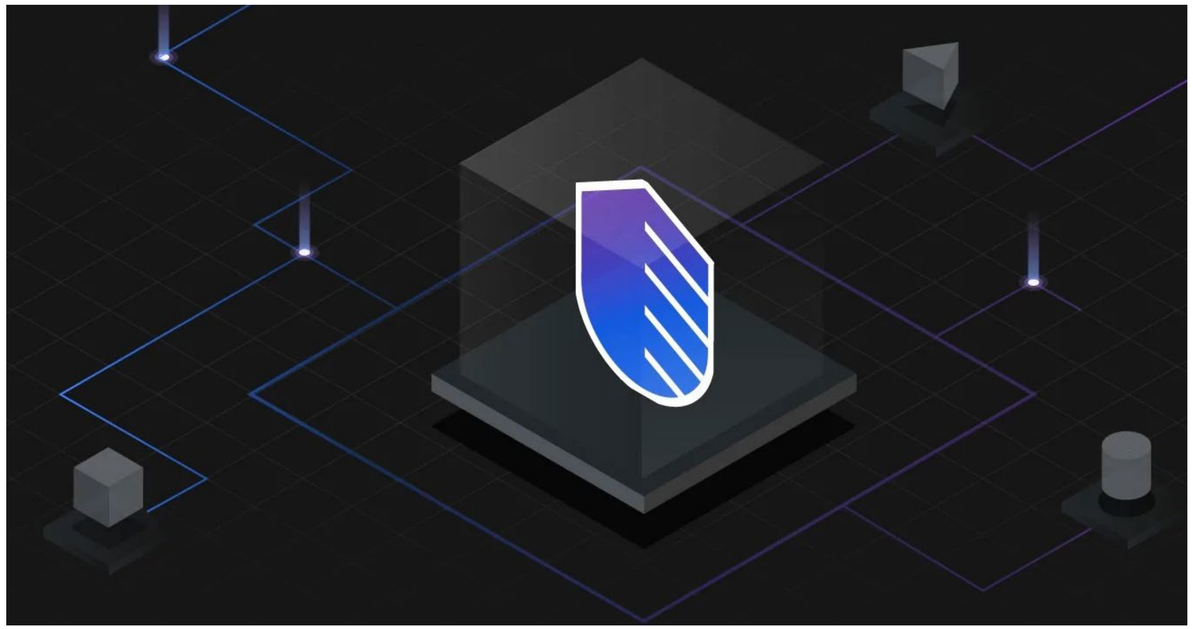
IBM

IBM CLOUD PAK FOR SECURITY

Modernizar a sua segurança com uma plataforma aberta e multicloud.

À MEDIDA QUE AS ORGANIZAÇÕES movem o seu negócio para a cloud, os dados são frequentemente espalhados por diferentes ferramentas e locais, quer seja na cloud ou *on-premises*. Isto cria lacunas que permitem que não se encontrem ameaças — que muitas vezes são resolvidas através de integrações complexas e dispendiosas.

O IBM Cloud Pak® for Security fornece uma plataforma para ajudar a integrar rapidamente as ferramentas de segurança existentes, de forma a gerar *insights* mais profundos sobre ameaças e riscos em ambientes híbridos e multicloud. Utilizando um ambiente de operação comum independente das infraestruturas que correm em qualquer lugar, é possível procurar rapidamente por ameaças, orquestrar ações e automatizar respostas - tudo ao mesmo tempo que deixa os seus dados onde estão.



– **Descubra as ameaças ocultas mais rapidamente**, conectando e procurando em todas as fontes de dados para uma visão mais completa do seu ambiente;

– **Reduzir o custo dos dados de segurança** ligando-se às ferramentas de segurança existentes através de padrões abertos, sem mover os dados;

– **Reduzir o tempo de resposta** automatizando tarefas manuais e repetitivas e impulsionando investigações através de integrações de terceiros;

– Corre em qualquer lugar – *on-premises*, cloud pública ou privada - com software contentorizado pré-integrado com Red Hat OpenShift;
– Aumentar a visibilidade da segurança através de uma solução que se liga a um ecossistema aberto da IBM e de conectores de dados de terceiros;
– Expandir as capacidades da sua equipa com competências adicionais, desde consultoria a pedido até ao desenvolvimento personalizado;

IBM CLOUD PAK FOR SECURITY PLATFORM

O IBM Cloud Pak for Security é uma plataforma integrada que reúne ferramentas, equipas e dados com uma experiência unificada e fluxos de trabalho ininterruptos. Diferentes funções de segurança, como o centro de operações de segurança (SOC) e a segurança de dados, são tradicionalmente separadas umas das outras, o que diminui a visibilidade e colaboração em toda a empresa. O IBM Cloud Pak for Security conecta estas equipas anteriormente isoladas, permitindo que o SOC e analistas de segurança de dados partilhem incidentes e artefactos através das capacidades da plataforma central.
Os líderes e analistas de segurança podem obter visibilidade nas suas operações de segurança com dashboards pré-construídos e personalizados que exibem métricas e análises detalhadas e de alto nível em toda a plataforma.
Com tecnologia de software livre e padrões abertos incorporados no IBM Cloud Pak for Security, a plataforma pode conectar-se a uma variedade de ferramentas de segurança e soluções em cloud IBM e de terceiros.

Como funciona

A plataforma IBM Cloud Pak for Security é composta por produtos e soluções modulares para as equipas de segurança aproveitarem. Os produtos e soluções estão ligados para uma experiência unificada do utilizador e gestão de casos centrais para fornecer aos analistas fluxos de trabalho integrados ininterruptos em toda a plataforma. Além disso, o licenciamento flexível e os preços não baseados em volume permitem que as organizações escolham as capacidades de que necessitam e facilmente adicionem mais, à medida que as suas necessidades mudam.

IBM CLOUD PAK FOR SECURITY PRODUCTS AND SOLUTIONS

Informações de Inteligência de Ameaça de Segurança da IBM

O Threat Intelligence Insights oferece informações detalhadas e atuais de ameaças que ajudam os analistas de segurança a identificar e priorizar as ameaças mais relevantes para a sua organização, com base no seu perfil organizacional. É possível obter informações de segurança adicionais alavancando a X-Force Threat Intelligence e verificar todas as fontes de dados conectadas para ver se uma ameaça está a afetar o seu ambiente.

Explorador de dados de segurança IBM

O Data Explorer permite que os analistas realizem investigações federadas através da IBM e de fontes de dados de terceiros. Podem ligar *insights* de ferramentas de segurança, tais como Security Information and Event Management (SIEM), Endpoint Detection and Response (EDR), e dados armazenados em data lakes, como o Elastic. Além disso, os analistas podem obter insights de ambientes multicloud que ferramentas SIEM como QRadar e Splunk estão a monitorizar.

IBM Security SOAR

O SOAR capacita os analistas de segurança através da automatização de operações de segurança comuns e processos de resposta a incidentes (IR), orientando-os através das medidas necessárias para resolver casos complexos. Podem aceder rapidamente a informações de segurança importantes com o contexto relevante do incidente, permitindo uma tomada de decisão precisa e uma ação decisiva.

IBM Security QRadar

O QRadar unifica a visibilidade com mais de 500 integrações validadas para segurança e ecossistemas de TI com suporte *out-of-the-box* para centenas de casos de uso de segurança, incluindo ameaça interna, ameaça avançada, segurança na cloud e muito mais. Os analistas de SOC podem obter *insights* centralizados entre utilizadores, *endpoints*, clouds, aplicações e redes. O motor de análise do QRadar usa uma gama de análises para identificar comportamentos anormais e atividades anómalas que indicam ameaças conhecidas e desconhecidas.

IBM Security Guardium Insights

O Guardium Insights é um centro de segurança de dados construído para simplificar a arquitetura de dados de uma organização, fornecendo uma visão unificada através de fontes de dados, armazenando registos de conformidade e auditoria a longo prazo, e empregando análises avançadas e machine learning (ML) para descobrir ameaças ocultas e comportamento anómalo.

Gestor de Risco de Segurança IBM

O Risk Manager proporciona aos líderes de segurança visibilidade na postura de risco de segurança das suas organizações, contextualizando dados de risco de todo o ambiente de TI e correlacionando *insights* entre vetores de risco e a criticidade dos ativos. ■

Microsoft

conteúdo produzido por
Microsoft Portugal

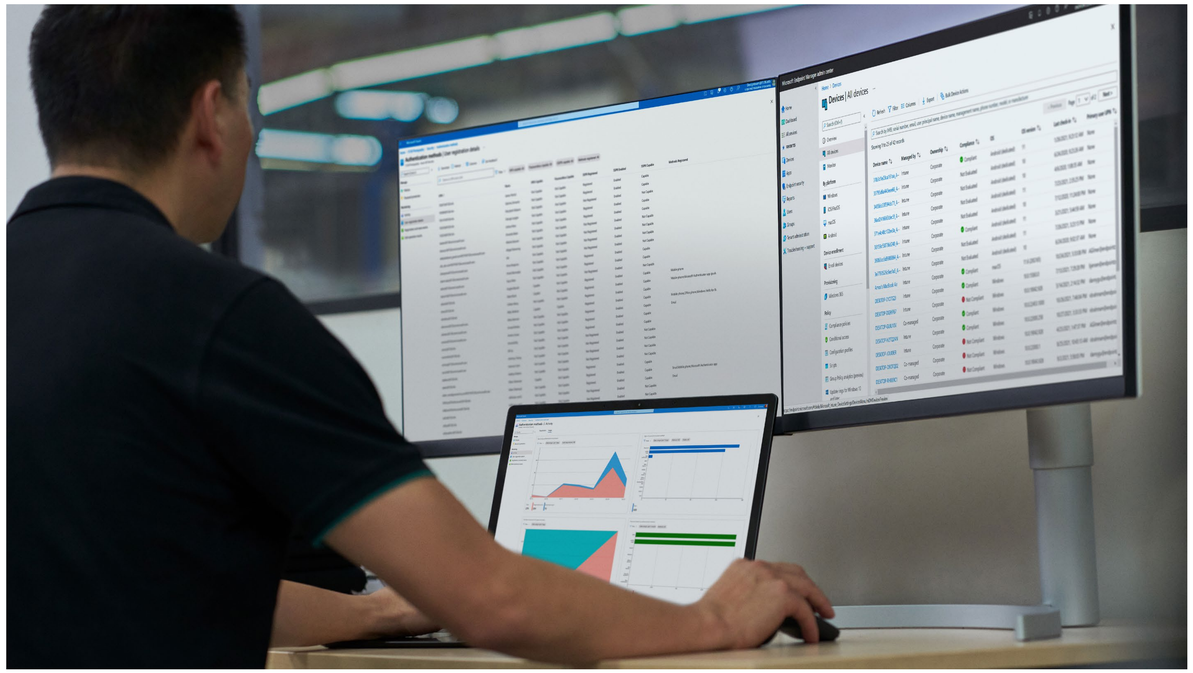
CYBER SIGNALS:

DEFENDER-SE CONTRA AMEAÇAS CIBERNÉTICAS COM AS MAIS RECENTES PESQUISAS, INSIGHTS E TENDÊNCIAS

A Microsoft lança o Cyber Signals, um resumo sobre inteligência das ameaças cibernéticas com base nos dados e investigações mais recentes da tecnológica.

ESTE CONTEÚDO, que será lançado trimestralmente, oferece uma perspetiva especializada sobre o cenário de ameaças atual, focando táticas, técnicas e estratégias de tendências usadas pelos atores de ameaças mais sofisticadas do mundo. Como tal, é um recurso valioso para os Diretores de Segurança da Informação, Diretores de Informação, Diretores de Privacidade, e as suas equipas, à medida que continuam a desenvolver tecnologias, políticas e processos perante o cenário de ameaças em constante mudança. A Microsoft, acredita que a segurança é um trabalho de equipa e que quando partilhamos o que aprendemos, podemos tornar o mundo um lugar mais seguro.

O Cyber Signals reúne *insights* das equipas de investigação e segurança na linha da frente, incluindo a análise a 24 mil milhões de sinais de seguran-



ça combinados com inteligência, monitorizados em mais de 40 grupos de estado-nação e mais de 140 grupos de ameaças. Nesta primeira edição, é abordado o tema da identidade. As identidades são compostas por tudo o que dizemos e fazemos nas nossas vidas, registados como dados que se estendem por muitas *apps* e serviços. Embora isto proporcione grande utilidade, se não mantivermos uma boa higiene de segurança, as nossas identidades estão em risco. E no último ano, vimos a identidade a tornar-se o fator preponderante para a segurança.

Embora as ameaças tenham vindo a aumentar rapidamente nos últimos dois anos, tem havido uma baixa adoção de autenticação forte de identidade, como a *autenticação multifator* (MFA) e *soluções sem palavra-passe*. Dados da Microsoft de dezembro de 2021 mostram que, em todos os setores, apenas 22% dos utilizadores da solução de cloud de identidade da Microsoft, o Azure Active Directory (AAD), implementaram uma forte proteção de autenticação de identidade. Estas soluções são cruciais na prevenção de uma variedade de ameaças e a Microsoft está empenhada em apoiar os clientes e parceiros com soluções como estas para uma maior proteção das comunidades.

Só em 2021, a Microsoft intercetou 35,7 mil milhões de e-mails de *phishing* com o Microsoft Defender para Office 365 e bloqueou mais de 25,6 mil milhões de ataques de autenticação de força bruta do AAD. Com uma equipa de mais de 8.500 especialistas de segurança, dedicados a proteger as plataformas, ferramentas, serviços e *endpoints*, a Microsoft reconhece o seu papel em ajudar a defender o nosso ativo digital mais valioso, a identidade. Para garantir que as pessoas são quem dizem ser quando acedem às contas e serviços, a Microsoft verifica a sua identidade — confiar numa única palavra-passe para autenticar os utilizadores pode criar pontos de risco atraentes para os *hackers*. A Microsoft continuará a investir de forma significativa nesta área, que inclui o reforço de 20 mil milhões de dólares nos próximos 5 anos.

As ameaças online estão a aumentar em volume, velocidade e sofisticação. Da IoT à atividade do Estado-nação, novas táticas de ransomware a *insights* sobre a economia do cibercrime, o Cyber Signals fornece uma análise das tendências e orientação prática para fortalecer a primeira linha de defesa digital. Com o número crescente de pessoas a trabalhar remotamente e a aceder a aplicações e dados de negócios a partir de várias localizações, incluindo escritórios em casa, espaços de *coworking* e outros locais remotos, a importância da autenticação segura – para proteção das empresas, dados pessoais, dispositivos, identidades, plataformas e clouds – aumenta.

Para mais informações sobre as soluções de segurança da Microsoft, aceda a *www.microsoft.com/security*. Acompanhe também as notícias e atualizações sobre segurança cibernética no Twitter da *@MSFTSecurity*. ■

multicert

POR PEDRO BARBOSA,
CEO da Multicert,
Head SIBS Cyberwatch

MAIS QUE CIBERSEGURANÇA, É HOJE FUNDAMENTAL FALARMOS DE CIBER-RESILIÊNCIA NAS ORGANIZAÇÕES

Ciber-resiliência, ou seja, a capacidade de uma organização suster ciberataques, minimizando disrupções no seu negócio ou marca, tornou-se, nos últimos 2 anos, um fator crítico para os decisores, para a continuidade de negócio e para o fator confiança, por parte de consumidores e organizações.

É JÁ UM CLICHÉ dizermos que hoje não é uma questão de se, mas quando, vamos ser atacados. Mas… e quando acontecer, como estamos preparados para reagir? **Qual o nível de maturidade da ciber-resiliência da nossa organização** e, acima de tudo, o que podemos fazer, para melhorar?

Foi neste sentido que a **SIBS Cyberwatch**, que presta serviços de cibersegurança 24x7 a empresas e organizações, nacionais e internacionais, identificou um conjunto de **10 medidas fundamentais** para trabalhar a ciber-resiliência, nas suas diferentes vertentes:

1 – **Seguir uma Framework de referência.** Porquê? Permite abordar o tema de uma forma estruturada e assegurar que, quando opta por um conjunto de medidas, cobre as diferentes vertentes de forma holística e avalia a sua progressão de maturidade.

2 – **Gestão de Ativos e a sua exposição.** Conhecer os ativos pertencentes à infraestrutura de IT da sua organização e a correspondente superfície de ataque, é fundamental.

3 – **Gestão de Vulnerabilidades.** Um processo de gestão de vulnerabilidades fornece diretrizes estruturadas para identificar, prio-

- Pedro Barbosa, CEO da Multicert, Head SIBS Cyberwatch -

ritizar, mitigar e validar as vulnerabilidades de segurança.

4 – **Testes de Intrusão.** Aplicações que não tenham nenhuma vulnerabilidade são a exceção. A realização de testes de segurança recorrentes, é fundamental para a deteção de vulnerabilidades de segurança e atuação atempada sobre as mesmas.

5 – **Gestão de Identidades.** Gerir as identidades dos utilizadores dentro de um sistema e controlar o seu acesso aos recursos disponíveis nesse sistema. Crítico para melhorar os perfis de segurança, simplificar a gestão dos utilizadores numa organização, auditar e iniciar o caminho para uma arquitetura *zero-trust*.

6 – **Autenticação de dois fatores.** A autenticação multifator (MFA) é de longe a melhor defesa contra uma vaga crescente de ataques relacionados com *logins*, incluindo *brute-force*, *credential stuffing* e *password spraying*. Se tem que começar por algum lado, considere esta medida uma prioridade.

7 – **Sensibilização de colaboradores.** Sabemos que é outro dos clichés mais ouvidos: "O elemento humano é o elo mais fraco na Cibersegurança". Como combater isto? Com um processo de consciencialização dos utilizadores para os perigos a que estes estão expostos. As vantagens imediatas do treino de *phishing*, são claras: sem formação, em média **27% dos utilizadores é suscetível a um ataque de *phishing***. Com um programa de *awareness*, ao fim de 3 meses, este número desce para 13% e ao fim de 12 meses, para 2,17%. Precisa de mais argumentos?

8 – **Monitorização 24x7.** É inevitável. Com o crescente número de ciberataques, a ocorrerem a qualquer hora e com um nível de sofisticação cada vez maior, é fundamental uma monitorização ativa dos ativos da sua organização, num modelo 24*7. Só assim se pode reduzir o tempo de deteção e resposta em caso de ataque.

9 – **Plano de Resposta a Incidentes.** Já o dissemos aqui: Com a mudança de paradigma, sabemos que os incidentes vão inevitavelmente acontecer. É, por isso, essencial, medirmos o risco, termos um plano e testarmos recorrentemente tecnologia de deteção, processos e equipas, para uma resposta, mais eficaz e rápida possível.

10 – **Backups and Restores.** Quando tudo o resto falha, ou quando somos alvo de um ataque de *ransomware*, o nosso processo de *backups* pode ser posto à prova. Fundamental, para reduzir a disrupção das nossas operações e limitar problemas de continuidade do nosso negócio. Importa recordar que, o processo de *backups* tem que ser protegido contra destruição por parte dos ataques e testado de forma recorrente.

Por fim, não podemos esquecer que os atacantes não trabalham isolados. Em resposta a isto, um passo fundamental, é **pedir ajuda**, ou apoio. Tanto às entidades oficiais – casos da PJ e do CNCS – como aos Profissionais de cibersegurança, seja através da contratação de empresas ou de colaboradores especializados. Num mundo cada vez mais global, a mensagem mais importante a reter é que **ninguém está 100% seguro**. Mas podemos estar mais bem preparados. ■

S21SEC LANÇA O THREAT LANDSCAPE REPORT

– RELATÓRIO DE CIBER AMEAÇAS DO 2º SEMESTRE DE 2021

Com o objetivo de sensibilizar as empresas e utilizadores para a necessidade de reforçar a segurança do tecido empresarial e investir em sistemas sofisticados que protejam a sua atividade da ameaça iminente de cibercriminosos, a S21sec lançou o seu relatório referente às ciberameaças do 2º semestre de 2021.

O RELATÓRIO é elaborado pela equipa de Cyber Threat Intelligence da S21sec, que é composta por analistas e engenheiros especializados com conhecimentos em inteligência dos indicadores e fontes que provêm das ameaças detetadas por outros clientes no seu MISP.

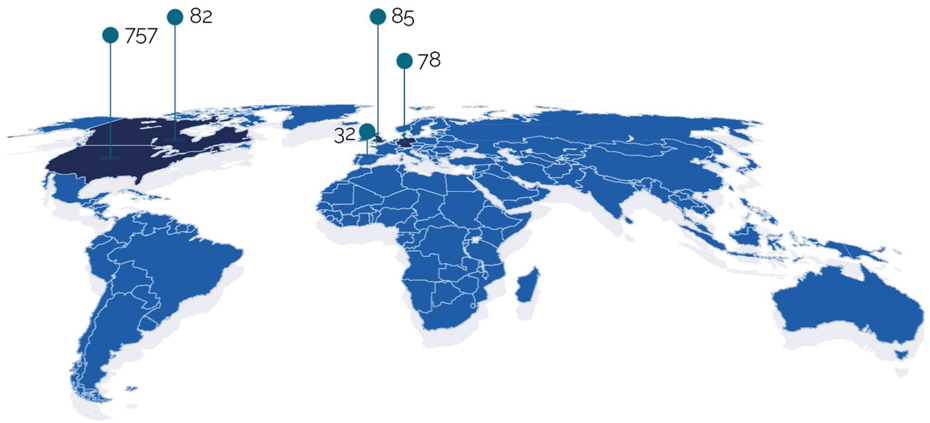
Entre as principais descobertas, a equipa de Threat Intelligence da S21sec detetou a identificação de cerca de 10.500 novas vulnerabilidades nos últimos seis meses, que aumentaram a suscetibilidade da comunidade empresarial sobre ameaças que explorem estas debilidades agora identificadas. Destas vulnerabilidades, foram registadas mais de 5.000 com um nível crítico ou elevado, que os cibercriminosos tentam explorar ativamente para a execução de diferentes tipos de ataques.

"Uma das principais falhas de segurança observadas tem sido a exploração das vulnerabilidades existentes na infraestrutura alvo. Por esta razão, é importante que as empresas tenham em consideração este tipo de ameaça e que se concentrem na atualização e manutenção das suas infraestruturas", afirma Hugo Nunes, responsável da equipa de Intelligence da S21sec.

1.694 VÍTIMAS DE RANSOMWARE EM TODOS OS 101 PAÍSES ABRANGIDOS PELO ESTUDO

A S21sec rastreou um total de 1.694 vítimas de ransomware em todos os países do estudo nos últimos seis meses. Olhando para o número de casos para cada território analisado, os EUA lideram a classificação dos países mais afetados por ransomware nos últimos seis meses do ano, com um total de 757 ataques, sendo

o principal alvo dos cibercriminosos. O Reino Unido, Canadá, Alemanha e França aparecem logo de seguida, enquanto a vizinha Espanha, com 32 ataques de ransomware registados, está no oitavo lugar. Portugal aparece em 31º lugar de 101 países abrangidos pelo estudo.



ATAQUES DE RANSOMWARE POR SETORES

De acordo com o estudo, os setores que mais sofreram ataques de ransomware durante a segunda metade de 2021 são a eletrónica de consumo e o imobiliário/construção. No entanto, também é de destacar o setor de serviços IT e comunicação, com uma elevada incidência de casos. Em Portugal, os exemplos mais mediáticos foram os ataques perpetuados ao Grupo Impresa e Vodafone, e mais recentemente, o Grupo Germano de Sousa foi alvo de um ataque bem-sucedido de ransomware, tendo sido inutilizada uma parte da sua infraestrutura.

Também o setor das telecomunicações teve os seus desafios. "O setor das telecomunicações tem sido um dos mais atingidos durante a pandemia, desde os embustes partilhados nas redes sociais sobre o 5G, até aos *phishings* em que os clientes das operadoras são aliciados com falsas ofertas de *gigabytes* gratuitos por causa do coronavírus ou concursos para ganhar telemóveis. Mais recentemente também foi notório o impacto que um ciberataque teve na operadora Vodafone e na forma como afetou todos os seus clientes pessoais e empresariais", explica Hugo Nunes.

CIBERATAQUES A INFRAESTRUTURAS CRÍTICAS

As infraestruturas críticas de diferentes países, principalmente relacionadas com meios de transporte, geração eólica de energia, fornecedores de eletricidade e água, companhias petrolíferas, forças de segurança e serviços de emergência, entre outros, foram alvo de numerosos ataques de ransomware ao longo do ano passado. Devido à magnitude das consequências e aos grandes danos que podem ser causados, os ciberataques a sistemas de infraestruturas críticas tornaram-se um dos maiores perigos para a sociedade atual. Segundo os peritos da S21sec, os efeitos mais devastadores incluem a interrupção ou colapso dos serviços públicos e situações de escassez no abastecimento. ■

Faça o download do *Threat Landscape Report* **aqui**

POR BRUNO CASTRO,
fundador e CEO da Visionware

VISIONWARE,

A PREPARAR AS EMPRESAS PARA ENFRENTAR OS DESAFIOS DA CIBERSEGURANÇA NA ERA DIGITAL

Fundada em 2005 pela visão pioneira e ousadia empreendedora de três amigos e colegas de trabalho, a VisionWare, empresa portuguesa com sede no Porto, filial em Lisboa e para o Mundo, é hoje uma das grandes referências (nacionais e internacionais) no que diz respeito à sua atividade exercida no âmbito da Segurança da Informação, uma área cada vez mais relevante nesta era digital: cibersegurança, TI, investigação forense, compliance, privacidade, formação e intelligence.

RECONHECIDA como detentora de capacidade técnica relevante e elevado *know-how* por instituições portuguesas e estrangeiras ligadas à justiça e com interesse no tema da segurança da informação, a VisionWare tem estado envolvida em diversos projetos internacionais e apoiados pela União Europeia, colocando-se a um nível máximo de exigência e cumprimento de requisitos em termos de inovação e especialização comparativamente a outros países europeus.
Desde o seu início, a VisionWare, empresa portuguesa credenciada pela NATO, trabalhou arduamente para ser reconhecida pela comunidade e pelo setor de Segurança da Informação, obtendo assim a confiança e fidelização contínua dos seus clientes como empresa altamente especializada e certificada, capaz de desafiar um mundo cada vez mais inseguro e complexo, protegendo e monitorizando diariamente o negócio dos seus clientes.

Em 2006 expandiu os seus escritórios para Lisboa e partir daí nunca mais parou. A crescente importância e tendência da Segurança da Informação em todo o mundo mostrou que a VisionWare estava no caminho certo. Em 2007, venceu o seu primeiro projeto em Cabo Verde, lançando a sua presença nos Países Africanos de Língua Oficial Portuguesa, a qual se mantém sólida até hoje.

Desde a sua génese, os fundadores da empresa sabiam que para promover uma verdadeira Segurança da Informação, esta deveria ser abordada de uma forma holística. Neste sentido, a partir de 2016, e depois de uma década de experiência acumulada, a garantir que as suas áreas centrais estavam devidamente consolidadas, a VisionWare avançou para o desenvolvimento e implementação de áreas independentes e complementares de *Privacy*, *Intelligence* e a criação de uma *Academy* para aliar uma componente crítica e emergente de formação. Conhecimento e aprendizagem contínua num mundo em constante evolução são fatores chave para corresponder às necessidades dos seus clientes e, por fim, alcançar sucesso. Hoje, com perto de duas décadas de experiência em diversificados tipos de mercados e em distintas geografias, a empresa sente a mesma ambição, acumulando mais sabedoria. A sua missão é continuar a disponibilizar e orientar as melhores práticas e soluções aos seus clientes, conquistando assim o reconhecimento e sucesso em qualquer parte do Mundo.

Com o aumento da cibercriminalidade e o consequente incremento na procura de apoio na mitigação de ciberataques, por parte de novos clientes, a VisionWare tem assistido a um crescimento bastante considerável, facto que obrigou a uma aposta da empresa na área de recrutamento face à necessidade de responder rapidamente às exigências do mercado e, também assente na dinâmica de inovação, e na criação de novas unidades de negócio orientadas para vertentes alternativas do mundo da segurança.

A atividade diária da VisionWare demonstra que o fator humano continua a ser um dos grandes responsáveis pela consumação das ameaças e que estas tanto podem vir de fora, como de dentro da própria organização. Neste sentido, além de ser fundamental preparar-se uma estrutura capaz de responder às ameaças que vêm do exterior, investindo na tríade de segurança (pessoas, processos e tecnologia), é fundamental olhar para dentro da organização, sensibilizar e formar as pessoas para que estas sejam conscientes e não se transformem em veículos de ameaça.

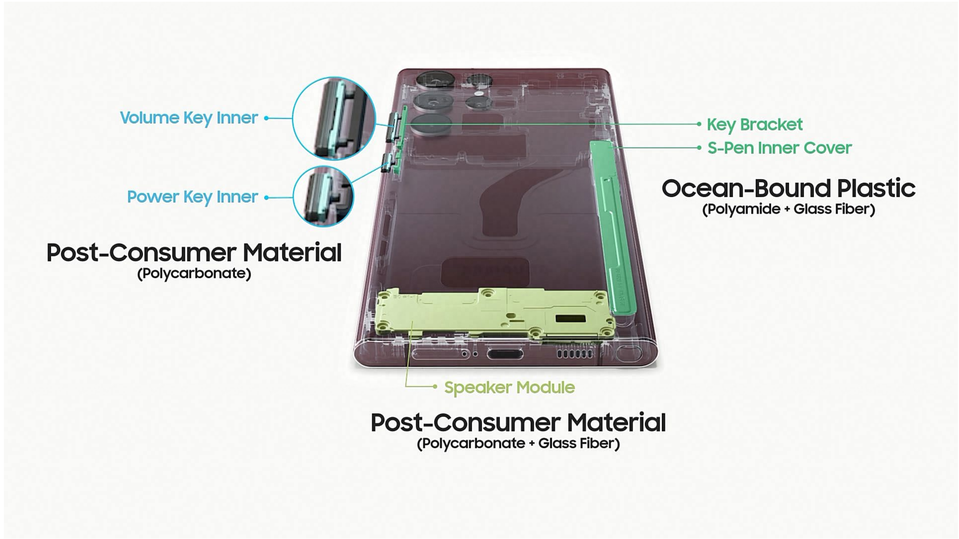
Atualmente, a VisionWare está presente em diferentes geografias tendo alcançado dimensão mundial através dos seus inúmeros projetos de relevo. Tem conquistado a confiança dos seus clientes nacionais e internacionais, e o reconhecimento da comunidade e das principais entidades reguladoras do setor. Sob o mote '*Challenging an Unsafe World*', a missão da VisionWare consiste em contribuir para o Sucesso dos seus clientes, em estreita relação de parceria, num mundo que é marcado pelas constantes inovações tecnológicas. O foco passa por zelar pelo bem mais precioso das Organizações - a sua Informação – auxiliando e orientando as melhores práticas que visam mitigar riscos desnecessários e criar um ambiente de negócio mais fiável. ■

GALAXY S22 ULTRA: O NOVO TOPO DE GAMA DA SAMSUNG

A Samsung juntou num só dispositivo a linha Galaxy S e Galaxy Note e criou o Galaxy S22 Ultra, um smartphone com "a melhor câmara, o melhor desempenho e a melhor conectividade de sempre num smartphone".

NO INÍCIO DE FEVEREIRO, a Samsung deu a conhecer o Galaxy S22 Ultra, um equipamento que junta dois legados de smartphones: a linha Note e o desempenho e qualidade das câmaras fotográficas da linha S. A Samsung afirma que, com esta fusão de linhas, procura estabelecer um novo padrão no que toca à categoria de smartphones premium.

O Galaxy S22 Ultra – que foi apresentado no mesmo dia que as versões Galaxy S22 e S22+, o Galaxy Tab S8 e GalaxyWatch4 – conta com uma S Pen integrada – que costuma acompanhar a linha Note – capacidades de vídeo e fotografia noturna, assim como uma bateria de longa duração.



QUALIDADE E DESEMPENHO

Procurando ser um dispositivo de topo de gama, o Galaxy S22 Ultra da Samsung conta, naturalmente, com as melhores especificações disponíveis. A S Pen, por exemplo, tem 70% menos latência, o que permite escrever e desenhar mais naturalmente no ecrã.

Com objetivas fotográficas integradas numa estrutura metálica que cria um efeito espelhado, o Samsung Galaxy S22 Ultra representa a aparência e o toque mais premium da Samsung. O vidro e o acabamento mate acrescentam um toque elegante ao *layout* linear e fluído do S22 Ultra – incluindo os contornos icónicos do Galaxy Note - tudo isto envolvido num design aerodinâmico. Tão durável como impressionante, o Samsung Galaxy S22 Ultra estará disponível em quatro cores inspiradas na natureza, incluindo o Phantom Black, o Phantom White, Verde e o novo S22 Ultra Burgundy.

De acordo com a própria Samsung, o Galaxy S22 Ultra foi "desenvolvido para tornar os dias de trabalho mais produtivos". Faz parte da primeira linha Galaxy S a ser equipada com o mais recente processador de 4nm, que alimenta o mais avançado processamento de Inteligência Artificial (IA) da Samsung.

O dispositivo também inclui Wi-Fi 6E, até duas vezes mais rápido do que Wi-Fi 6. Isto significa que é possível desfrutar de um desempenho superior em todas as aplicações mais utilizadas, quer esteja a jogar, em streaming, ou a trabalhar. Toda esta potência funciona com a bateria do Samsung Galaxy S22 Ultra, que oferece até mais do que um dia inteiro de utilização após uma carga completa. O Samsung Galaxy S22 Ultra suporta também carregamento super-rápido de 45W, para que possa gravar mais de 50 minutos de vídeo após um carregamento de dez minutos.

CÂMARA FOTOGRÁFICA

Com o Samsung Galaxy S22 Ultra, a noite e a falta de luz deixam de ser uma barreira à qualidade fotográfica. As características avançadas do sistema Nightography, que alia sensores de imagem à grande capacidade de processamento de IA, disponíveis em toda a família de dispositivos S22, permitem captar vídeos e fotos mais nítidos e vívidos quer com a câmara frontal como através das câmaras traseiras – esteja a gravar durante o dia ou durante a noite. O Samsung Galaxy S22 Ultra inclui um sensor de 2.4um - o maior sensor de pixéis de sempre da Samsung que permite às suas objetivas captar mais luz e mais dados, otimizando a iluminação e os detalhes de qualquer gravação. Além disso, a lente Super Clear Glass do S22 Ultra ajuda a captar vídeos noturnos mais fluídos e nítidos, sem qualquer problema. Por sua vez a funcionalidade de Auto Framing assegura que a câmara capta sempre exatamente aquilo e quem deseja, quer seja uma ou dez pessoas.

Com capacidades de zoom que permitem uma aproximação de cem vezes da ação, o Samsung Galaxy S22 Ultra não inclui apenas a câmara mais potente da Samsung, como também a mais inteligente. Repleto de novas características baseadas em IA como o modo Portrait, o Samsung Galaxy S22 Ultra foi desenvolvido para tornar todas as fotografias em conteúdos profissionais. Com as capacidades robustas do sistema inteligente de câmaras do Samsung Galaxy S22 Ultra, o equipamento fará todo o trabalho pesado e irá ajudar a captar fotografias e vídeos superiores em qualquer condição de iluminação.

DISPONIBILIDADE

Os novos equipamentos da Samsung estão disponíveis em pré-compra desde o início de fevereiro, com o Galaxy S22 Ultra a estar disponível no mercado nacional desde o dia 25 de fevereiro.

O Galaxy S22 Ultra está disponível em quatro cores – já referidas – e em modelos com armazenamento de 128GB, 256GB, 512GB e 1TB, com 8GB ou 12GB de RAM. O preço de venda ao público recomendado do Galaxy S22 Ultra começa nos 1.279,99 euros. ■

THREAT LANDSCAPE REPORT

O departamento de Cyber Threat Intelligence da S21sec oferece um relatório semestral que apresenta e explica as ameaças que prevaleceram no segundo semestre de 2021 e que podem colocar em risco a segurança de empresas e indivíduos,

DOWNLOAD

S21 SEC

Segundo semestre 2021

BANCA E SEGUROS: O CLIENTE NO CENTRO DA INOVAÇÃO

A mudança radical da expectativa dos clientes, agravada pela entrada de novos players digitais no mercado, levou a que os setores da banca e seguros tenham de alterar os seus processos e modelos de negócio de forma a manter a competitividade.

MARGARIDA BENTO

A TRANSFORMAÇÃO DIGITAL, particularmente a experienciada de forma acelerada durante a pandemia, está sem dúvida a afetar todos os setores, criando, assim, novas oportunidades de crescimento, mas causando ao mesmo tempo uma enorme disrupção, obrigando as organizações a acompanhar o ritmo evolutivo sob pena de ficar para trás.

No entanto, poucos setores sentiram esta disrupção de forma tão intensa como os da banca e dos seguros. Tendo, à partida, modelos de operação distintos, as instituições financeiras convergiram nas suas necessidades evolutivas, deparando-se com uma rápida mudança das expectativas dos clientes, que divergem cada vez mais dos seus modelos tradicionais.

Para manterem a competitividade e resiliência, estas organizações terão, então, de acompanhar o ritmo de mudança – não só ao nível da simples digitalização que se faz sentir em todos os setores como também no sentido de marcar passo com os novos *players* que estão a subir a fasquia no mercado. Isto não só passa pela criação de novos produtos e serviços, novos modelos de negócio e novas experiências de cliente, como também da transformação de todos os processos subjacentes, transformando profundamente as suas operações, cultura interna e sistemas, independentemente das tecnologias que utilizem.

"Não creio que a transformação digital seja um processo cristalizado no tempo, é um processo que se quer contínuo, por isso mesmo terá de estar sempre nas agendas das entidades que querem marcar a diferença por usar a tecnologia no modernizar e acelerar a entrega de mais valor aos seus principais *stakeholders*, no setor segurador em especial, aos clientes e à rede de mediação", refere Sérgio Martinho, Chief Information Officer da Lusitania Seguros.

O CLIENTE COMO MOTOR DE INOVAÇÃO

No que toca a serviços, isto traduz-se sempre num maior foco no cliente – por um lado, no sentido da rapidez de resposta ao contacto e, por outro, na personalização e *self service*.

Cada vez mais informado das suas escolhas e disposto a procurar ativamente a opção que traga mais benefícios, o cliente espera, agora, que os serviços se adequem às suas necessidades e que o prestador esteja sempre disposto a atender às mesmas.

"Claramente, os clientes têm desenvolvido uma capacidade de procura e exigência de serviços, em que a experiência e facilidade de acesso a respostas efetivas são determinantes", refere João Moradias, Head of banking & Insurance da DXC. Esta maior exigência por parte dos clientes, que rapidamente adotam novos modos de utilização como experiência base, obriga a um constante acompanhamento das expectativas dos seus clientes.

- João Moradias, Head of banking & Insurance da DXC -

"As instituições bancárias têm de assumir uma competência muito particular em compreender a transformação das expectativas dos seus clientes, envolvendo-se no seu modelo evolutivo e criando uma combinação ideal de interações digitais e humanas para uma boa prestação do serviço e satisfação dos seus clientes", acrescenta.

Como tal, os bancos e seguradoras têm que se adaptar, endereçando o cliente numa lógica multicanal e de proximidade, simplificando os processos de interação com o cliente, sem perder o foco com cada um.

"Neste contexto a permanente adaptação das plataformas multicanal de contacto com os clientes são uma nova realidade, e consequentemente, a organização tem que se dotar de processos mais automáticos e flexíveis, que permitam uma resposta mais objetiva e em tempo útil, não permitindo que o cliente se sinta desapoiado," alerta Luís Teodoro, Administrador da Softfinança.

Para além do próprio contacto, as expectativas face à própria oferta mudaram radicalmente nos últimos anos.

"O cliente hoje faz uma gestão do seu tempo de forma mais flexível e informal, está mais esclarecido e atento aos pormenores, com uma maior expectativa e valoriza a disponibilidade e a melhor experiência de consumo, impulsionando assim as organizações a se adaptarem a este novo perfil de clientes, e desta forma manterem as suas relações de fidelização numa lógica multicanal integrada

A BANCA ESTÁ A TRANSFORMAR-SE PARA ESTAR MAIS PRÓXIMA E SER MAIS EFICIENTE E RÁPIDA, APESAR DE UTILIZAR CADA VEZ MAIS SOLUÇÕES REMOTAS EM DETRIMENTO DA PRESENÇA FÍSICA

que desta forma abarca os diferentes tipos de contacto com o cliente, nas diferentes fases em que ele se possa encontrar", relata o responsável.

Na banca, o exemplo mais óbvio disto é a quase total ubiquidade do pagamento eletrónico, o qual – precedido há já várias décadas pela crescente predominância do uso de cartões de crédito e débito – verificou uma verdadeira explosão nos últimos anos, com o advento do *mobile banking* e plataformas de pagamento como a MBWay. Quantas pessoas em tempos recentes nunca foram apanhadas despercebidas quando, deparadas com uma situação na qual não é aceite pagamento eletrónico, se aperceberam que haviam perdido o hábito de trazer consigo dinheiro vivo?

"Hoje, a grande maioria das operações de retalho já são feitas nos canais digitais ou ATM; registamos mensalmente 16 milhões de acessos às nossas plataformas de banca digital", relata uma fonte no BPI. "Estes números refletem já hoje uma alteração definitiva do modelo de distribuição bancário e das condições de prestação dos serviços financeiros, através da articulação de uma profunda mudança tecnológica com uma alteração radical do comportamento dos clientes. É mais visível no retalho, mas atingirá, sem exceção, todos os segmentos".

Na era digital, o utilizador dará sempre primazia à opção mais conveniente, mais ágil e que mais se adeque ao seu estilo de vida. Isto é tornado particularmente óbvio pela rápida popularização de serviços digitais como a Revolut, que beneficiaram de um crescimento explosivo por virtude de se posicionarem como alternativa mais ágil e flexível e menos burocrática do que os modelos tradicionais.

Como tal, para manter a atratividade num ambiente cada vez mais competitivo, os bancos e seguradoras terão cada vez mais de endereçar o cliente numa lógica multicanal, sem que se perca a integração e coerência na relação com o cliente.

Aos olhos do BPI, "a banca está a transformar-se para estar ainda mais próxima, mais eficiente e mais rápida, apesar de utilizar cada vez mais soluções remotas em detrimento da presença física, sem perder o essencial da sua função de intermediação financeira, baseada na confiança".

Os bancos e fintechs exclusivamente digitais apresentaram um desempenho significativamente maior do que os bancos tradicionais

- Sérgio Martinho, Chief Information Officer da Lusitania Seguros -

Contudo, defende Sérgio Martinho, o setor dos seguros diverge em parte da tendência geral, por virtude da natureza do contacto com o cliente. Enquanto os serviços financeiros têm um contacto quase diária com os seus utilizadores, a seguradora é, na maioria dos casos, uma figura com a qual, idealmente, não se toma contacto a não ser que algo esteja errado.

"Não considero que seja o cliente o instigador direto da transformação; creio que é mais relevante o peso que a rede de mediação terá, pois, esse sim, tem um contacto muito mais próximo e são mais instigadores da transformação".

A exceção é, naturalmente, os clientes corporativos, visto que este segmento implica maior contacto com o cliente individual e, como tal, maior exigência em termos de prestação de serviço.

NOVOS MODELOS NO SETOR BANCÁRIO

O setor da banca depara-se com um problema único. Para além dos níveis base de inovação requeridos pela digitalização, os bancos tradicionais precisam de marcar passo com os novos *players* do mercado, criados de origem para esta nova realidade.

De acordo com um recente estudo da Accenture, os bancos e fintechs exclusivamente digitais apresentaram um desempenho significativamente maior do que os bancos tradicionais entre 2018 e 2020.

Isto, detalha o estudo, deve-se em grande parte à diferença entre modelos de negócio. Os modelos de negócio bancários tradicionais, verticalmente integrados, ficam em clara desvantagem face aos modelos empregados por *players* digitais, os quais, através da desagregação dos produtos tradicionais e parcerias com terceiros, permitem criar ofertas personalizadas de valor acrescentado.

Para além destes *players* mais bem sucedidos, aqueles que adotaram modelos não lineares verificaram um maior crescimento nas receitas durante este período do que aqueles que replicaram

os modelos tradicionais, linearmente integrados verticalmente.

De acordo com este estudo, os bancos tradicionais que adotem estes novos modelos poderão aumentar as receitas em 4% por ano.

"Neste contexto, o setor tem criado desenvolvimento de estratégias que permitam combater esta evolução, promovendo modelos colaborativos com as fintechs na procura de parcerias de benefícios mútuo, desenvolvendo capacidade de interligação fácil com as múltiplas entidades que se movem no setor financeiro, através de contextos de *openbanking*, e tendo por base o seu ativo mais importante que é a enorme base de clientes", indica João Moradias.

Assim, explica, as empresas do setor conseguem acompanhar o ritmo da inovação e criar soluções adaptadas aos requisitos dos seus clientes, conseguindo uma experiência de utilização dos seus serviços bancários vastamente superior.

NOVOS MODELOS NO SETOR DOS SEGUROS

Também as seguradoras enfrentam pressão por parte de novos *players* digitais, com maior foco no marketing e distribuição, permitindo-lhes ir ao encontro das necessidades dos clientes através de experiências digitais melhoradas. Como na banca, e como já referido, o cliente espera uma experiência multicanal, personalizada e sem atritos.

Segundo um recente estudo da McKinsey, uma experiência de cliente digital deixará de ser um *nice to have*, passando a ser uma condição-base para o crescimento, obrigando as seguradoras a formar parcerias ou, em alternativa, a

O DESAFIO DOS BANCOS E DAS SEGURADORAS SERÁ ACOMPANHAR O RITMO EVOLUTIVO DO SETOR

- Luís Teodoro, Administrador da Softfinança -

fazer grandes investimentos tecnológicos. A mudança para o digital será possivelmente a última oportunidade para as seguradoras recuperarem terreno na luta pelo cliente.

Segundo a consultora, as seguradoras terão de se focar na personalização do serviço e experiência do cliente, envolver-se com os novos *players* para formar parcerias tecnológicos, modernizar as plataformas e tomar partido dos dados, analítica e automação.

"As companhias, seguradoras ou não, que usualmente ganham relevância no mercado são aquelas que antecipam necessidades, as que pensam mais à frente e estão mesmo centradas nos seus clientes, não conheço nenhuma que tenha feito um trabalho de relevância sem que com isso seja utilizada em grande extensão as tecnologias de informação", comenta Sérgio Martinho. "O IT deve, inclusivamente, ser mais do que um meio para se atingir um fim, deve ser um motor *per se* do espírito da inovação por estarem atentas ao potencial que é possível explorar por fazer com que os clientes incrementem os seus níveis de confiança e com isso incremente o seu footprint."

Aqui, acrescenta, o *pay per use* será uma realidade. Popularizado pelas insurtechs, estes modelos mais flexíveis apresentam um maior apelo junto do cliente e esta é uma tendência que as seguradoras terão de acompanhar se tencionarem recuperar terreno face aos novos *players*, oferecendo simultaneamente valor acrescido através de consultoria e aconselhamento.

OS DESAFIOS DA INOVAÇÃO

Tanto no setor bancário como dos seguros, o principal desafio será o acompanhamento do ritmo evolutivo do setor, em particular no que toca à gestão da dívida técnica, o que obrigará a uma revisão e adaptação de processos e organização interna.

Este é, na verdade, um duplo desafio: não só a gestão da dívida técnica é um obstáculo inevitá-

vel para todas as organizações que procurem inovar, como a própria cultura de inovação irá determinar a sua capacidade de acompanhar o ritmo de mudança em tempo útil.

"Como se depreende, a tempestade perfeita acontece quando há uma enorme dívida técnica e uma não vontade de uma mudança, tudo fica substancialmente mais complicado," reforça Sérgio Martinho. "É por isso mesmo que deve haver uma cultura corporativa que instigue a saída de todos, da sua zona de conforto, pois só assim é promovida a necessária vontade de querer fazer mais, sempre melhor".

Assim, a inovação terá necessariamente de ser holística, tanto a nível tecnológico, operacional e humano, em organizações nas quais, pela sua dimensão, criticidade e antiguidade, qualquer mudança se apresenta como um processo extremamente complexo.

Todos estes desafios devem ser ultrapassados de forma a que as instituições financeiras possam acompanhar a evolução de um mercado cada vez mais competitivo, não só por virtude das expectativas dos clientes como também da entrada de fintechs e insurtechs no mercado, por natureza mais tecnologicamente competentes e ágeis na sua utilização.

"O IT deve ser mais do que um meio para se atingir um fim. Deve ser um motor do espírito da inovação em si só, por estarem atentas ao potencial que é possível explorar por fazer com que os clientes incrementem os seus níveis de confiança, e com isso incremente o seu *footprint*", refere o responsável.

DE OLHOS NO FUTURO

Independentemente do setor, a pedra basilar da inovação será sempre a capacidade de acrescentar valor aos clientes através de serviços que respondam às suas necessidades, com maior rapidez de resposta, compreensão e ação. Como tal, os dados estarão sempre no centro da mudança – em particular, reforça João Moradias, através da Inteligência Artificial (IA), que, prevê, será preponderante num futuro próximo.

Na banca, as plataformas multicanal e omnicanal de contacto com os clientes serão uma nova realidade, requerendo que as organizações desenvolvam processos mais automáticos e flexíveis para resposta e apoio ao cliente.

"O futuro que se prepara é um modelo a que chamamos omnicanal, em que o cliente tem à disposição uma plataforma de serviço comum a todos os canais disponíveis, remotos e presenciais, com um suporte de tecnologias que vão desde a inteligência artificial, ao metaverso/Web 3.0 e às finanças descentralizadas", acrescenta também o representante do BPI

Já nos seguros, Sérgio Martinho prevê também uma integração em massa de tecnologias como Internet das Coisas, machine learning e inteligência artificial, com vista a conseguirem maior flexibilidade e proximidade ao cliente.

A IA, em particular, terá um efeito disruptivo na cadeia de valor dos seguros, criando um modelo '*human in the loop*' que potenciará a produtividade e maior qualidade no contacto com os clientes. Aqui, o setor beneficia de um vasto histórico de dados pré-existentes, dos quais poderão tomar partido para criar modelos operacionais mais inteligentes, e mesmo desenvolver produtos e serviços com base em IA.

"Nessa realidade, não duvido que a seguradora estará muito mais no *mindset* do cliente pois deixa de ser uma *commodity* para ser um verdadeiro *trusted business partner*", diz.

Como consequência desta forte evolução tecnológica, a Lusitania prevê uma maior concentração do mercado, com um número menor de seguradoras a operar globalmente e cujas operações se vão basear na personalização dos serviços.

Esta tendência será também acompanhada por uma evolução dos mediadores: "vejo um canal de mediação diferente, muito mais centrado no cliente, mais uma entidade que, em conjunto com a seguradora, consegue aportar mais valor na relação", conclui. ■

SoftFinança

POR LUIS TEODORO,
Administrador da SoftFinança

A DIGITALIZAÇÃO COMO RESPOSTA À EVOLUÇÃO DA EXPERIÊNCIA DO CONSUMIDOR NOS SETORES DA BANCA E DOS SEGUROS

O ano de 2022 não poderá deixar de ser diferente no que concerne à adoção das melhores práticas e mais recentes tecnologias por parte das empresas, por forma a dar resposta às exigências dos clientes na experiência que lhes é proporcionada, nas diversas tipologias de serviços que integram o seu quotidiano.

A IDEIA DE QUE A DIGITALIZAÇÃO é apenas crucial para as gerações mais jovens deixou de fazer sentido, sendo exemplo disso a previsão da Forbes (2021), que indica 2022 como o ano em que o conhecimento digital deixará de seguir estereótipos, e que a procura por serviços, e resolução de problemas através da internet, será uma realidade generalizada, em que mesmo as camadas mais envelhecidas interessar-se-ão cada vez mais pelo digital e a sua oferta.

Posto isto, as empresas preocupadas com a fidelização e satisfação dos seus clientes terão pela frente uma jornada na procura por uma oferta que melhor satisfaça as exigências e necessidades dos mesmos, bem como que conjugue, na medida certa, a experiência de utilização, a humanização do serviço e as expeta-

tivas do *target*, tirando proveito dos mais recentes desenvolvimentos tecnológicos, como a inteligência artificial, análise preditiva e a computação quântica, uma vez que apesar dos clientes, agora na posse de muito mais informação, procuram um serviço rápido, prático e eficaz, continuam a ambicionar uma abordagem personalizada às suas questões, ou problemas, pelo que os *chatbots*, um email automático, ou um SMS pré-definido, não serão suficientes para o deixar satisfeito, e as empresas terão de equilibrar a componente tecnológica com a componente humana nos seus serviços e oferta.

Nas áreas dos seguros e da banca, que tipicamente são mais frugais e institucionais, a realidade será semelhante, com o acréscimo de que o investimento na relação com o cliente será mais elevado, devido ao tipo de serviço prestado e a relação que, por norma, existia entre este tipo de instituições e os seus clientes.

Como tal, as plataformas digitais, sempre disponíveis, serão a solução a adotar perante os novos hábitos e objetivos de consumo. Se antigamente as pessoas iam ao banco todos os meses, ou tratavam dos seus seguros presencialmente, a verdade é que na azáfama do dia-a-dia, e no acesso mais facilitado à informação e oferta generalizada destes serviços, o cliente atual, independentemente da sua idade já não tem disponibilidade e motivação para se deslocar presencialmente com tanta frequência para tratar deste tipo de questões.

Ter uma plataforma, ou aplicação, que torne possível dar resposta às necessidades e questões, de forma segura, é a exigência atual para estes setores, notando-se um aumento da preocupação dos clientes e das organizações em relação à utilização dos seus dados online, e à segurança e integridade dos mesmos, ainda mais num contexto como o que se vive hoje, com ataques a organizações dos mais diversos setores, com cada vez maior frequência.

É por isso importante que na implementação destas soluções digitais, as organizações procurem parceiros tecnológicos qualificados, com experiência, que lhes dêem a garantia de que para além da *performance*, experiência de utilização e diferenciação, essas soluções sejam resilientes e seguras, evitando incidentes que possam fragilizar a relação e lealdade com os seus clientes, bem como a sua satisfação em relação à organização.

A verdade é que se o investimento no digital for feito de forma correta, e por profissionais qualificados para tal, a própria digitalização irá facilitar a gestão da banca e das seguradoras, já que irá permitir agilizar operações, obter ganhos de eficácia e melhorar a relação com o cliente.

Apesar da digitalização ter sido fortalecida devido ao contexto em que vivemos, já era reconhecida como uma mais-valia para qualquer empresa, perante o paradigma envolvente. ■

Este é o melhor caminho para o coração do consumidor.

Estar sempre perto, sempre disponível, sempre à mão, é construir uma relação duradoura com o consumidor. Através de uma **app própria**, a sua marca pode estabelecer um contacto **personalizado**, apresentar toda a informação comercial, facilitar **pagamentos** e apresentar campanhas promocionais ou comunicação pontual. Se acha difícil ter uma app própria **fale connosco** e conheça as nossas **Mobile Solutions**. E ainda lhe contamos como desenvolvemos a app móvel com maior número de utilizadores em Portugal.

Porque afinal, andar com o cliente nas palminhas ainda é uma boa estratégia comercial.

SoftFinança®

smarter companies, happier lives

softfinanca.com

moving to the cloud

UM NOVO OLHAR SOBRE A CLOUD EM 2022

No início de dezembro do ano transato, a Meta (anteriormente Facebook) e a AWS (a divisão de cloud da Amazon), anunciaram um acordo de colaboração estratégica, que cobre diversas aplicações e casos de uso de cloud, mas especialmente os que se referem a IA. No anúncio das duas empresas é referido que a Meta expandirá através da AWS as suas plataformas internas, mas também virá a suportar empresas que venha a adquirir na cloud da Amazon.

HENRIQUE CARREIRO

OU SEJA: existe, de facto, uma utilização da infraestrutura da AWS por parte da Meta, não se referindo o acordo apenas a otimização de código desenvolvido por esta, por forma a tirar melhor partido das capacidades oferecidas pela AWS. Mas mesmo nesta última vertente, o acordo contempla algo de particular interesse.

É dito explicitamente que será feito trabalho adicional para que a plataforma PyTorch, usada por exemplo pela Tesla e pela Uber, seja melhor integrada, por exemplo no Amazon SageMaker, o serviço de machine learning da AWS – presumivelmente para servir não apenas utilizadores externos mas também os próprios investigadores e equipa de desenvolvimento da Meta, que tem um dos melhores laboratórios de IA do mundo.

Este anúncio é um prenúncio do que serão algumas das tendências mais relevantes no espaço da cloud no corrente ano e de que três das quais se enunciam a seguir.

1) A CLOUD CONTINUA A CRESCER E A EVOLUIR COM BASE EM CENÁRIOS DE UTILIZAÇÃO INOVADORES

De acordo com previsões da Gartner, espera-se que os gastos globais em serviços na cloud atinjam mais de 482 mil milhões de dólares em 2022, que se comparam com 313 mil milhões de dólares em 2020. A infraestrutura da cloud é hoje a base sobre a qual assentam todos os modernos serviços digitais, englobando desde as redes sociais aos serviços de *streaming* e aos carros ligados e infraestrutura de *Internet of Things*. Formas de conectividade que prometem maior largura de banda e menor latência, como as redes 5G (e futuro 6G, de que se começa a falar), assim como Wi-Fi 6 não significam apenas que mais dados chegarão à cloud -- significam também o aparecimento de dados de novas origens, provavelmente com maiores débitos, com maior variação de entrega, com mais exigências de tratamento em tempo real. Esperem-se, por exemplo o aparecimento de mais plataformas de jogos na cloud, como já o são a Vortex, a Boosteroid ou a Amazon Luna. Esperem-se grandes aumentos de investimento em tais plataformas ao longo de 2022.

2) A EVOLUÇÃO EM INTELIGÊNCIA ARTIFICIAL É INDISSOCIÁVEL DA EVOLUÇÃO DA CLOUD

A cloud desempenha um papel fundamental nos desenvolvimentos de IA, o que foi descrito pelo CEO da Google, Sundar Pichai, como "mais transformador do que a eletricidade ou o fogo" em termos do efeito que terá na sociedade. As plataformas de machine learning e deep learning requerem uma enorme capacidade de processamento e de largura de banda para treino e processamento

estão aí e são incontornáveis. Adicionalmente, longe vão os tempos dos assistentes pessoais com vozes robóticas. É cada vez mais difícil distinguir entre um texto dito por uma voz artificial e uma natural. Tudo isto é fruto do desenvolvimento concertado da IA na cloud. A cloud continuará a aumentar o seu peso na prestação destes serviços aos utilizadores, e esse será decerto um dos mais notáveis desenvolvimentos no ano que decorre.

3) A CLOUD EVOLUI PARA PRESTAÇÃO DE SERVIÇOS EM MODO "SERVERLESS": É ALTURA PARA COMEÇARMOS A ENTENDER OS IMPACTOS DESTA FORMA DE TRABALHAR

A prestação de serviços em modo "*serverless*" na cloud é um conceito relativamente recente que está a ganhar força no mercado por parte de fornecedores como a Amazon (com AWS Lambda e outros serviços) e Microsoft (com Azure Functions, por exemplo), entre outros. Por vezes referido como "Functions-as-a-Service", este modo de funcionamento significa que as organizações não estão obrigadas a terem de fazer aprovisionamento prévio de serviços na cloud, lançar e manter máquinas virtuais ou preocupar-se com questões de escalabilidade. Promete um verdadeiro serviço "*pay-as-you-go*" em que a infraestrutura se dimensiona invisivelmente como uma aplicação o exige. Na verdade, o nome é enganador: existem, evidentemente, servidores, por detrás de tudo. Mas as configurações destes são invisíveis para o utilizador final, o que pode ser uma bênção – ou nem tanto, porque implica toda uma nova forma de pensar e trabalhar, para a qual as empresas não estão necessariamente preparadas. Até por questões de custos de utilização, com modelos diferentes dos tradicionais. Mas é a altura certa para começarmos a entender mais esta tendência e respetivos impactos, uma vez que se está a estender rapidamente a inúmeros serviços disponíveis em cloud, em todos os fornecedores.

Na verdade, como indicámos no início, o anúncio conjunto da Meta e da AWS cristaliza, na perfeição,

estas tendências, até mesmo a da evolução para "*serverless*", uma vez que cada vez mais a AWS, como os restantes fornecedores de serviços de cloud tendem a privilegiar o lançamento de serviços que dispensam aprovisionamentos complexos pelo lado do cliente. Em primeiro lugar porque são, efetivamente, mais simples de usar. Em segundo, e não menos importante na ótica dos fornecedores, porque estes serviços são garantes de

que os clientes não mudam com facilidade de fornecedor. Se há uma tendência que será também visível, mais ainda em 2022, é que, na cloud, os casamentos são de longa duração: a quebra de uma tão entrançada ligação entre fornecedor e cliente é de tal forma complexa que o caminho para a cloud – e dentro desta para um fornecedor específico é, praticamente irreversível. Assim, os fornecedores continuem, sem falhas, a manter as respetivas posições competitivas. ■

O CAMINHO PARA A CLOUD

A cloud é uma realidade para um número considerável de organizações, mas "não é simplesmente um destino" e a decisão de migrar para a cloud "não deve ser tomada de ânimo leve".

RUI DAMIÃO

A TRANSFORMAÇÃO DIGITAL ditou que as organizações adotassem a cloud como o modelo de eleição. No entanto, essa pode não ser a realidade para a totalidade das empresas e existem várias entidades que não colocam tudo na cloud, seja por que razão for.

Mas, hoje, a ida para a cloud não tem de ser uma aventura onde se explora o desconhecido. A jornada para a cloud pode ser definida à partida, escolhendo as melhores opções e sem as empresas terem de voltar atrás na sua infraestrutura ou ficar presos a um determinado fabricante.

ESTRUTURA

A jornada para a cloud já não tem de ser algo feito no momento e as organizações podem ter estruturados todos os passos para que essa jornada seja o melhor possível, tendo acesso às tecnologias, processos e soluções que mais se adequam às suas necessidades.

Ilustração: iStock/id-work

Vasco Afonso, Head of Cloud & Security da Claranet, refere que "a decisão de migrar para a cloud não deve ser tomada de ânimo leve", e deve resultar "de um exercício de análise profundo de cada organização".

Esta análise, diz, deve ser feita em termos de modelo de negócio, nas formas de beneficiar a adoção da cloud e potenciar o negócio, assim como o que é necessário fazer ao nível da operação, da capacitação de competências, alteração de processos e governança para conseguir tirar o máximo potencial da cloud.

Arlindo Dias, Cloud Architect da IBM, afirma que "a cloud não é simplesmente um destino", mas sim "é um modelo cuja adoção implica de facto uma jornada, seja esse modelo assente puramente numa única cloud pública, multicloud ou uma solução híbrida".

O representante da Claranet indica que "muitos projetos de migração para a cloud acabam por não correr como é esperado". Por várias razões,

- Vasco Afonso, Claranet -

acrescenta, "muitas organizações não obtêm as reduções de custos operacionais, as melhorias de desempenho e outros benefícios que se acredita serem o resultado de uma migração para a cloud".

Para o Cloud Architect da IBM, as organizações têm à sua disposição "um crescente número de opções e tecnologias que visam facilitar a jornada para a cloud. Não existe uma estratégia única e aplicável a todas as organizações, uma aferição consultiva que permita identificar a melhor estratégia é fundamental. A realidade e especificidade de cada organização obriga a identificar a melhor abordagem para cada *workload*, seja ela o '*lift & shift*' ou o '*refactor*'".

FIM DA EXPERIMENTAÇÃO

Se, numa primeira fase, a jornada para a cloud ficou definida pela experimentação, hoje já não é bem assim. No entanto, importa pensar se as organizações ainda podem investir sem receios, tendo um maior grau de certeza de que o dinheiro investido vai, de facto, trazer retorno.

Arlindo Dias refere que, hoje, o mercado dispõe de cada vez mais tecnologia, muitas vezes proveniente da comunidade. "A experimentação passou para o patamar da otimização, o que tem permitido que o retorno do investimento tenha vindo a acelerar, com especial realce desde 2019", acrescenta, explicando, ainda, que "com uma estratégia adequada e uma escolha criteriosa do modelo a adotar os riscos são fortemente mitigados",

- Arlindo Dias, IBM -

ainda que não deixem de existir por completo.

Para Vasco Afonso, "a cloud veio democratizar o acesso à tecnologia e hoje é incrivelmente simples e rápido ter acesso à mais recente tecnologia de cloud, por uma fração do custo quando comparado com os cenários tradicionais de aquisição. Isto permite, desde já, que as organizações adotem uma cultura de inovação baseada na experimentação".

Ao mesmo tempo, acrescenta o Head of Cloud & Security, o conhecimento que hoje existe da cloud "é incomparavelmente maior do que há dez anos" o que permite "tomar decisões muito mais bem fundamentadas, que reduzem o risco e a incerteza".

No entanto, é preciso ter em conta que a cloud "é dinâmica e está em constante evolução" e, como tal, "é essencial que as empresas continuem a atualizar-se no que respeita a novos serviços ou alterações nos serviços existentes".

O PREÇO EM CIMA DA MESA

O fator preço faz parte da realidade de qualquer empresa. O investimento não é ilimitado e, por isso, é preciso pesar bem o custo de uma solução e o seu real benefício para a organização. Na verdade, diz Vasco Afonso, "a gestão de custos na cloud é um dos pilares fundamentais de qualquer plano de governação".

Arlindo Dias explica que "existe um paradoxo que ainda está em fase embrionária de transformação" que "reside nas direções financeiras e de orçamentação em que as despesas de TI sempre foram investimento com valores fixos por prazos mínimos de três anos". Esta já "não é a realidade", uma vez que "a flexibilidade do negócio" exige uma "flexibilidade nos consumos das TI o que implica flexibilidade orçamental".

Assim, esclarece o Cloud Architect da IBM, "o controlo de custos num modelo de cloud implica duas vertentes: a funcional, em que a organização terá que se adaptar criando novas funções" onde a "missão é o controlo dos recursos alocados e os consumos efetivos". A outra vertente é "a tecnológica, em que é inevitável a adoção de ferramentas que permitam o controlo efetivo dos custos e acima de tudo a otimização na utilização dos recursos".

Vasco Afonso afirma que, habitualmente, os ambientes tradicionais estão sobredimensionados face às reais necessidades, "o que leva à perpetuação de *workloads* que ninguém conhece, pois foram implementados para efeitos de testes, ou então suportam aplicações que, entretanto, foram descontinuadas".

Na cloud, acrescenta, "é essencial que se garanta desde cedo a implementação de procedimentos de controlo que permitam assegurar uma boa gestão de todos os recursos utilizados – e isto porque na cloud todos os serviços têm um custo, pelo que é essencial assegurar que só utilizamos mesmo os serviços de que necessitamos".

"A correta gestão de capacidade é apenas um dos princípios básicos de uma boa gestão de custos. Outro pilar fundamental é a adoção de um serviço de FinOps e Cost Advisory realizado por empresas especializadas em cloud, que, de forma, contínua analisam os serviços cloud utilizados e apresentam recomendações de otimização", conclui Vasco Afonso.

RAZÕES PARA MIGRAR PARA A CLOUD

Ao longo dos anos, foram muitas as razões partilhadas por empresas e especialistas do porquê de as organizações deverem migrar para a cloud. Hoje, tantos anos depois do início das primeiras jornadas, é possível estabelecer concretamente as principais razões para as organizações migrarem para a cloud, mesmo sabendo que cada caso é um caso.

- **Redução de custos de IT** – os líderes de IT procuram os recursos de computação certos para os seus requisitos de negócios e, idealmente, com o menor custo possível;
- **Maior agilidade de negócio** – ter acesso a recursos de IT flexíveis e disponíveis *on-demand* é crucial para estar a par dos concorrentes e das alterações da indústria;
- **Melhor segurança** – as organizações podem modernizar as suas infraestruturas de IT de acordo com as melhores práticas;
- **Fim das preocupações com o fim de vida dos produtos** – ao migrar para a cloud, a preocupação com o fim de vida de hardware e software crítico diminui, uma vez que se deixa de estar preso a acordos de licenciamento rígidos;
- **Consolidação dos data centers** – com a computação cloud, as empresas deixam de ter de gerir os seus próprios data centers *on-premises*;
- **Permitir a transformação digital** – com o crescimento de processos de transformação digital, os líderes de IT podem ter ao seu dispor os mais recentes avanços para digitalizar as funcionalidades mais essenciais;
- **Crescimento acelerado** – com a cloud, as organizações podem integrar novas tecnologias mais rapidamente;
- **Alavancar novas tecnologias** – ao migrar para a cloud, as organizações podem adotar as vantagens de novas tecnologias, como machine learning e inteligência artificial. ■

CYCLOID
Technology and Consulting

"CLOUD LOCK-IN NUNCA FOI UM PROBLEMA"

Data & Analytics, Modern App, Database Freedom e Machine Learning são as áreas onde a Cycloid recebe um forte apoio técnico do seu parceiro AWS.

- Nuno Neto -
Chief Technology Officer at CYCLOID Technology and Consulting, Lda.

Quais são ainda as principais objeções por parte das organizações portuguesas para a adoção de soluções cloud?

Acreditamos que as principais objeções estão relacionadas com os custos e a segurança. As empresas portuguesas já têm uma noção das vantagens de migrar os sistemas para a cloud, mas estes dois pilares causam alguma insegurança porque o *ownership* passa a ser partilhado com outras empresas.

Existe também outro receio que se prende com o facto de que, no final dos projetos, a parte de manutenção para o cliente se torna complexa pela falta de *know-how* interno. O *know-how* da cloud é diferente do sistema *on premise* e ainda está a ser construído, sendo que ainda existe uma falta de recursos nesta área que, de alguma forma, torna o processo mais custoso.

Como deve ser planeada a migração dos *workloads*?

Uma migração para a cloud tem que, estrategicamente, fazer sentido para a empresa. Eu vejo esta necessidade de duas formas: uma é o crescimento do negócio e, acima de tudo, dos dados e dos clientes, ou seja, um aumento do *load*, não só dos dados, como também do acesso aos dados.

E por outro lado, a possibilidade de haver novas soluções e novas visões para o negócio, através de novos serviços que a cloud oferece.

A empresa tem que estar alinhada em, pelo menos, uma destas visões. O que acontece depois é a necessidade de fazer uma migração mais planeada e otimizada para a cloud, tirando o melhor partido das funções, o que normalmente implica um grande trabalho de reengenharia.

Necessitamos de ver os sistemas informáticos de uma forma diferente porque desenvolver para a cloud é na-

tivamente diferente do que vender *on premise* e os projetos acabam por ser mais demorados e têm um investimento CAPEX maior.

Como é que a Cycloid ultrapassa, com os seus clientes, os desafios de cloud *lock-in* e da imprevisibilidade dos custos?

Temos uma visão diferente do *mainstream*. Estamos há 15 anos no mercado e sempre existiu vender *lock-in*, por exemplo a escolha de base de dados ORACLE vs MICROSOFT e, sempre se optou pela melhor solução, consoante o cenário, tendo em conta as necessidades da empresa. Cloud *lock-in* nunca foi um problema. Na realidade, desenvolve-se um sistema para uma cloud e, se caso necessário, mais tarde, pode migrar-se para outra bem mais facilmente porque, por exemplo, não há hardware envolvido. Além disso, conceptualmente, as principais clouds são semelhantes em termos de *building blocks*, sendo que umas são mais avançadas do que outras, mas a transição prende-se apenas ao software, portanto não envolve grandes custos e pode ocorrer em paralelo.

Alguns recentes ciberataques mediáticos fragilizaram a perceção de segurança na cloud por parte dos clientes?

É um facto que a cloud tem sido posta em causa. As empresas têm receio de passar para a cloud pelo desconhecido. De facto, há muitas particularidades que têm de ser bem configuradas e dimensionadas e ainda não existe uma maturidade nestas novas áreas.

Não há nada 100% seguro, mas consideramos que a cloud é bem mais segura do que *on premise*, uma vez que os provedores de cloud garantem um conjunto de regras de segurança bastante apertadas.

Para tal acontecer *on premise* era preciso um grande *expertise*, desde firewalls a bases de dados, sistemas operativos e um *know-how* interno, o que não acontece dado que nem todas as empresas têm departamentos de segurança que contemplem todas estas *skills*.

Por outro lado, existe a parte da aplicação em si, desenvolvida pela empresa e que deve proteger elementos como *logins* e falhas de segurança da própria aplicação.

A Cycloid é Consulting Partner da AWS, como é que esta parceria pode aportar valor adicional aos clientes?

A parceria com a AWS é muito importante. A AWS tem presença física na Península Ibérica há relativamente pouco tempo e estão a apostar bastante no crescimento local com serviço de plataformas e integração de mini data centers.

A AWS presta apoio à Cycloid em quatro áreas: Data & Analytics, Modern App, Database Freedom e gerações de bases de dados para a cloud e na área de Machine Learning. Portanto, nestes pilares temos, internamente, um apoio técnico muito forte.

Para os nossos clientes, há um grande apoio financeiro para projetos, nomeadamente em custos da AWS, e também um apoio a nível de marketing com vídeos ilustrativos do que é a solução ou até com a realização e divulgação de *use cases*. ■

INFORMANTEM informática | manutenção

POR MÁRIO ACÚRCIO,
CTO da Informantem

MOVING TO THE CLOUD

Atualmente observamos que as organizações as quais ainda não iniciaram a adoção de uma estratégia cloud, irão em breve adotar a mesma, garantindo uma jornada para adoção de plataformas, aplicações e serviços na cloud.

MOTIVO ESSE que se prende por diversos fatores como modernização, escalabilidade e agilidade da infraestrutura, controle de custos e gestão simplificada.

No entanto a transição para a cloud é algo que deve ser ponderado e decidido de forma metódica por qualquer organização, sendo que se torna fundamental obter resposta para as seguintes questões:

- Porquê usar a cloud?
- Qual o seu papel na organização?
- De que forma poderá beneficiar o negócio?
- Como irei comprometer (ou não) o meu futuro ao adotar serviços na cloud?

O mercado nos últimos anos tem vindo a tornar-se cada vez mais competitivo e exigente sendo que existe uma procura por inovação, eficiência e agilidade. Estes 3 fatores estão presentes nas plataformas cloud, sendo que as organizações procuram modernizar as suas plataformas de dados e assegurar níveis de desempenho superiores que permitam acompanhar o ritmo do mercado.

Com as últimas notícias publicadas recentemente relativamente a ciberataques, é normal verificarmos cada vez mais organizações que optam por colocar os seus dados na cloud, sendo que muitas organizações não dispõem de equipas com recursos especializados na área da cibersegurança, levando a que a cloud seja uma opção rápida e segura para quem pretende reforçar a segurança e a proteção dos seus dados.

Para além da questão da segurança, a cloud está a tornar-se um local de eleição para o armazenamento de dados, e

- Mário Acúrcio -
CTO da Informantem

acompanhando este movimento as organizações optam por migrar as suas aplicações para plataformas cloud de forma a poderem aproveitar aplicações inovadoras e analítica avançada. Tal como sabemos, os dados são de extrema importância e garantir uma rápida e correta análise de todos os dados é uma das principais bases de sustentação das decisões e estratégias das organizações, tanto a nível de observação, como prospeção e previsão. Também o custo de garantir a aquisição e manutenção de um Data Center *On-Premises* bem como uma equipa técnica com as características idênticas às que que encontramos num provedor cloud é muito superior. No entanto, para além do menor custo um dos maiores fatores que levam às organizações pela adoção cloud são os benefícios associados: sistemas mais ágeis e modernos, soluções e serviços que promovem a transformação digital, entre outros exemplos.

Apesar das inúmeras vantagens acima mencionadas, estará a cloud diretamente relacionada com o sucesso? Não.

Para garantir o sucesso da adoção cloud por parte das organizações, deve-se seguir uma metodologia assente em 4 pilares: Análise da infraestrutura atual que permite definir quais serão os desafios e obstáculos durante a sua transição. Planeamento de todo o processo de transição e demais tarefas para garantir a operacionalidade de todos os sistemas. Preparação das tarefas e pré-requisitos para o processo de migração. E para terminar a implementação dos *workloads* e parametrização definida inicialmente para garantir o ótimo funcionamento da infraestrutura na cloud. Apenas seguindo uma metodologia poderemos garantir o sucesso da transição para a cloud.

Várias organizações que optaram por ambientes cloud devido às necessidades emergentes do mercado, efetuaram uma transição não respeitando qualquer metodologia e desta forma não adotando as melhores práticas, o que levou a que tenham tido vários dissabores relacionados com questões operacionais, mas também com custos inesperados.

Atualmente existem diversas soluções no mercado que permitem analisar a utilização de ambientes cloud, fornecendo informação pertinente para que possamos desta forma redimensionar os *workloads* em caso de contratação excessiva de recursos ou por questões de *performance* e inclusive relativamente à utilização dos mesmos *workloads* em diferentes provedores cloud para garantir não só uma melhoria de *performance* e cumprimento de regras de segurança como também para redução de custos.

Para concluir, 3 pontos que devemos considerar:

- Seleção da abordagem correta para a organização, assegurando as expectativas definidas;
- Envolvência de diversas equipas/elementos com competências relevantes para abordar questões centrais do funcionamento da organização;
- Escolha e utilização de ferramentas apropriadas: fáceis de utilizar, seguras e escaláveis e com integração com os diversos ambientes.

É de extrema importância a escolha de um parceiro como a Informantem, capaz de identificar, arquitetar, implementar a melhor solução e efetuar o devido acompanhamento durante toda a jornada de transformação ■

POR HUGO SILVA,
Business Unit Manager,
Data Center & Multi Cloud

MOVING TO THE CLOUD

As empresas enfrentam hoje ambientes voláteis e em mudança, fruto de disrupções cada vez mais frequentes, profundas e que deixam menos espaço de manobra.

AS EMPRESAS PASSIVAS que apenas reagem à mudança estão condenadas a perder competitividade a longo prazo, enquanto que as empresas pró-ativas e orientadas para a inovação irão sem dúvida liderar a economia digital.

Em todo o caso, todas enfrentam um mercado que converge para a complexidade, sendo hoje mais necessário que nunca colaborar para desenvolver serviços e soluções específicos que respondam aos desafios da economia digital de uma forma transversal. Os objetivos, contudo, permanecem inalterados ao longo dos anos: aumentar as vendas e a satisfação do cliente e oferecer experiências de utilização seguras, eficientes e escaláveis.

Atualmente, para o conseguir, **é essencial fazer da cloud um elemento central da estratégia organizacional, para ganhar em agilidade, flexibilidade e eficiência.** Mas acreditamos que o salto para a cloud já não é, por si só, suficiente. Na Warpcom e na Evolutio, dividimos a viagem digital dos nossos clientes em duas fases.

Em primeiro lugar, é essencial criar um núcleo digital *ad hoc* (integrando modelo de negócio, processos e plataformas), que permita à organização responder a novos desafios sem abandonar as necessidades mais imediatas. Isto é o que é conhecido como "***enabling the cloud***": construir os alicerces que permitirão extrair todo o

- Hugo Silva -
Business Unit Manager,
Data Center & Multi Cloud

potencial. Parte destes alicerces é a capacidade de proporcionar experiências digitais de qualidade aos clientes e colaboradores, sem esquecer a cibersegurança e assegurando a conformidade regulamentar e a confiança digital.

Como integradores líderes de serviços na cloud no mercado ibérico, estamos conscientes de que este ponto do processo é crítico. Em muitos casos, verificamos que as organizações iniciaram um processo de adoção da cloud sem passar por esta análise prévia, o que, a longo prazo, gera problemas em múltiplas áreas (custos, desempenho, regulamentos, falhas de segurança...) que se tornam mais visíveis à medida que a carga de trabalho aumenta. Felizmente, nunca é demasiado tarde para enfrentar este processo e estabelecer uma arquitetura e quadros operacionais e de governação que nos permitam escalar com garantias e passar à fase seguinte, conhecida como "***empowering the cloud***".

Para competir com sucesso na economia digital, as empresas devem ir mais longe e aproveitar todo o potencial da cloud em termos de agilidade, canais digitais, automação de processos, soluções cognitivas e analíticas avançadas, entre outros. Tudo isto, sem esquecer que a abordagem tecnológica deve ser eminentemente prática e orientada para o negócio. Parte da realização destas premissas, como já salientámos, deve-se à implementação de arquiteturas modernas, adaptadas aos novos modelos de integração e de implementação contínua de aplicações na cloud. A operação deve ser entendida como um processo imbricado no desenvolvimento das aplicações, mas também com uma visão transversal e homogénea que garanta o controlo correto de custos, segurança e conformidade com os regulamentos em vigor.

O salto para um modelo digital traz benefícios, mas também desafios. Abordá-los proativamente é a chave para alcançar os primeiros. Podemos gerir mais facilmente a complexidade se anteciparmos e definirmos claramente os nossos objetivos e compreendermos o ponto de partida e o processo existente, as barreiras tecnológicas e culturais. Isto é o mais importante, pois envolve a tomada de decisões estratégicas que afetam a empresa de forma holística. **Em qualquer caso, a digitalização não é opcional nem uma reivindicação comercial. É uma verdadeira necessidade de negócio que veio para ficar.** ■

warpcom

Os ciberataques não batem à porta

Apoiamos a sua organização no desenho e implementação de soluções de **Cybersecurity**.

Saiba mais sobre nós:

warpcom.com

SOFIA VAZ PIRES, CEO DA ERICSSON PORTUGAL

“5G É A GRANDE PRIORIDADE NA ERICSSON”

A empresa, liderada por Sofia Vaz Pires, acredita que terá um papel inovador e preponderante na estratégia nacional de transformação digital, mas esta é, como refere a diretora-geral para Portugal, uma revolução que se faz a várias mãos.

FÁTIMA FERRÃO E HENRIQUE CARREIRO

HÁ 18 ANOS, Sofia Vaz Pires iniciava uma já longa carreira no setor das tecnologias da informação, precisamente na Ericsson, onde regressou em julho de 2021 para assumir a liderança da subsidiária nacional. Foram quase duas décadas ligada essencialmente ao mercado das telecomunicações, para agarrar agora o comando da estratégia onde a grande prioridade é o 5G. A CEO acredita que este é um momento de evolução tecnológica mundial, em que Portugal não fica atrás. O país é, na sua opinião, competitivo, inovador e atrativo para o investimento externo, especialmente no setor das tecnologias da informação, e não será o arranque mais tardio do 5G que irá limitar as suas hipóteses de ter um papel preponderante a nível internacional. Para tal, a Ericsson está pronta a fazer a sua parte, tirando partido da liderança mundial nesta tecnologia, onde detém 16% das patentes essenciais do 5G, e 170 dos 180 acordos comerciais de redes 5G, com operadores de telecomunicações em cinco continentes.

A revolução está em curso, mas, alerta a responsável, esta faz-se a várias mãos. Quando o objetivo é construir um ecossistema inovador e capaz de dar resposta às necessidades públicas e privadas, em todos os setores, o esforço tem que ser comum e, no fundo, "remarmos todos na mesma direção".

A conversa com a IT Insight, na primeira pessoa, deixa ainda exemplos do que já se faz lá fora com o 5G e muito do que a experiência acumulada da Ericsson pode trazer para que Portugal se mantenha competitivo.

Em que áreas se movimenta a Ericsson atualmente?

A Ericsson evoluiu, nas últimas décadas, do portfólio que todos conheciam dos telefones e de outras tecnologias. Estamos agora na vanguarda tecnológica de soluções para as redes móveis e, sobretudo, na liderança comercial do 5G que neste momento é a grande prioridade da empresa.

Para fornecer alguns números que reforçam essa

liderança, normalmente referimos diversas variáveis, e uma que vem também do grande investimento em R&D que a Ericsson faz a nível mundial, dizemos com orgulho que até à data temos cerca de 16% do que é definido como patentes essenciais do 5G. Isso é basicamente a posição de liderança em termos das patentes registadas. Por outro lado, é com orgulho que também partilho que, neste momento, de 180 acordos comerciais de redes 5G a Ericsson detém 170, isto com operadores de telecomunicações em cinco continentes.

Na Europa já temos mais de 50 referências, portanto, acho que isto é demonstrativo da nossa liderança a nível mundial e também por já estarmos presentes em Portugal, de forma ininterrupta há quase 70 anos – o nosso aniversário será no próximo ano, em 2023 –, também reflete o papel inovador e de preponderância que temos tido no mercado português na estratégia nacional de transformação digital.

Portanto, essa é também a estratégia para Portugal?

A nossa grande estratégia em Portugal é mantermos a posição de liderança e, mais do que isso, estarmos focados na implementação de projetos que sejam diferenciadores, tanto para o mercado nacional e para todo o ecossistema, desde empresas privadas e públicas, como os próprios utilizadores finais que no seu conjunto irão ajudar a colocar o país na vanguarda digital.

Convém também dizer que Portugal é, cada vez mais, um país competitivo e atrativo para o investimento externo, especialmente nas áreas de tecnologias de informação e, portanto, é com orgulho que a Ericsson, com o seu *know-how* e talento das nossas pessoas em Portugal, que são altamente reconhecidas pela *expertise* que têm na sua área de foco, que estamos também a contribuir para todo esse desenvolvimento.

> A ERICSSON POSICIONA-SE PARA AJUDAR OS NOSSOS PARCEIROS E CLIENTES A DESTACAREM-SE COM QUALIDADE NA FORMA COMO FORNECEM EXPERIÊNCIAS

Mas o foco é o 5G, dentro e fora de Portugal?

Atualmente, o grande momento é do 5G. Obviamente que temos um vasto portfólio tecnológico com diversas soluções, não apenas todo o hardware, software e serviços associados à implementação de redes 5G, mas também outras soluções muito assentes em machine learning. Por exemplo, aqui o foco é mais na otimização das redes para que possam operar de forma segura, mas também sustentável de um ponto de vista energético, com benefícios do ponto de vista da pegada de carbono.

Enquanto tudo isto acontece do ponto de vista de soluções comerciais que atualmente já temos disponíveis, a Ericsson, sendo uma empresa de investigação e desenvolvimento tecnológico, está também já a olhar para soluções do futuro como a Internet of Things e, também, toda a tecnologia à volta daquilo que chamamos as máquinas inteligentes conectáveis. Isto sempre assentes em protocolos standard porque também nesse tipo de fóruns a Ericsson tem uma posição de destaque.

Na sua opinião, quais são hoje os desafios que tiram o sono a quem está no mercado das telecomunicações?

A Ericsson está presente nas telecomunicações, a nível mundial, há mais de 145 anos e tanto a nível global como local, é uma empresa que se pode dizer que é um parceiro de longa data e de elevada confiança dos nossos parceiros comerciais e do mercado. Temos perfeita noção do poder que tem o nosso *know-how* acumulado junto dos nossos parceiros e junto da indústria, bem como do nosso papel enquanto parceiro inovador.

Em Portugal, sempre trabalhámos com todos os operadores e queremos continuar a fazê-lo. É importante referir que, à medida que estamos agora muito focados no 5G, a Ericsson posiciona-se aqui para ajudar os nossos parceiros e clientes a destacarem-se com qualidade na forma como fornecem essas experiências aos seus clientes. Portanto, ajudar os operadores – que são os nossos clientes diretos –, a entender como é que podem responder de forma adequada às necessidades dos seus clientes finais. Porque mais

do que um bom serviço de comunicações de qualidade, é importante destacarem-se agora com diferentes camadas de conectividade na apresentação do mesmo serviço, de forma que o cliente final possa ter uma experiência com qualidade, mas também um serviço que realmente agregue valor.

Podemos dizer que o arranque do 5G é o mais emblemático de 2022. Estamos a começar, mas há outros países mais avançados. Que *use cases* destaca noutros países e quais os que, na sua opinião, se poderão destacar ou ser os primeiros a arrancar em Portugal?

Acho que há que destacar que também advém da nossa liderança em termos de soluções de 5G a nível mundial, as experiências que podemos trazer de outras geografias para Portugal. O que temos visto é que, de facto, o impacto do 5G afeta de forma positiva várias indústrias de forma transversal como sejam, por exemplo, a indústria manufatora, a indústria automóvel, mas também outras indústrias como portos, logística e saúde.

As caraterísticas associadas à tecnologia 5G, como as redes de alta qualidade com baixa latência permitem, de facto, entregar experiências de alta qualidade nestas indústrias. Para dar alguns exemplos concretos de projetos associados a estes setores que fizemos em alguns países que, certamente, o nosso mercado nacional pode beneficiar destaco, por exemplo, em Itália, o Porto de Livorno. Ali utilizámos a tecnologia 5G e as soluções da Ericsson para fazermos a operação dos navios de forma mais eficiente e, também, a carga e descarga que acontece entre os barcos e os camiões que estão no porto, de forma que os operadores possam

> “ OUTRA SOLUÇÃO INTERESSANTE FOI A IDENTIFICAÇÃO DE TODAS AS FERRAMETNAS QUE OS OPERÁRIOS ESTAVAM A USAR PARA QUE SOUBESSEM SEMPRE ONDE ESTAVAM AS SUAS FERRAMENTAS ”

identificar – através de soluções de realidade aumentada e machine learning –, onde colocar uma determinada carga e qual a rota mais inteligente a seguir. Isto, pelo menos neste projeto de Livorno, foi algo que se traduziu em benefícios muito concretos. Tanto a nível da redução da pegada de carbono em cerca de 10%, como em termos do benefício do aumento de eficiência de cerca de 28% na forma como estas rotas são feitas dentro do porto.

Outro exemplo muito interessante é, por exemplo, junto da fábrica da Mercedes, na Alemanha – e há que referir que todos estes casos de uso são feitos com a empresa em si, mas também com o operador. Aqui o caso de uso foi, não só, descarregarem o software para os automóveis através da tecnologia 5G, mas também a entrega dos materiais nos diferentes postos de trabalho na fábrica. Outra solução interessante, também dentro deste caso de uso, foi a identificação de todas as ferramentas que os operários estavam a usar para que soubessem sempre onde estavam as suas ferramentas.

Referiu a saúde, um setor que ganhou destaque com a pandemia. Pode dar-nos alguns exemplos do que já fizeram a nível internacional?

Sim. Por exemplo no Reino Unido, juntamente com a Universidade Coventry. Através do uso de tecnologia de realidade virtual, os estudantes de medicina conseguiram ver partes do corpo humano de uma forma que não poderiam compreender se vissem apenas em formato 2D (fosse num computador ou num livro), e isto também já foi usado na preparação de cirurgias de forma a serem o menos invasivas possíveis.

Neste sentido, estes estudantes, para serem futuros cirurgiões, podem preparar através de um modelo 3D digital exatamente onde está o problema e como o podem atacar de forma preditiva, antes de realmente entrarem na operação.

E se pensarmos mais ao nível da cultura ou do entretenimento. Há exemplos?

Também se prevê que haja uma verdadeira revolução a nível do entretenimento dos utilizadores

finais. Por exemplo, através do uso de soluções de realidade aumentada ou realidade virtual, sendo exemplo disto o uso de hologramas em concertos. Ou dando um exemplo mais concreto: na Coreia do Sul o que estão a fazer em monumentos históricos é colocarem uns óculos aos visitantes para que estes consigam ter uma perceção de como as pessoas naquela época se vestiam, lutavam, ou seja, ter experiências muito imersivas. Sendo Portugal um país com uma História tão rica, acho que seria uma ideia facilmente aplicável.

E sobre o que já foi testado em Portugal, o que nos pode revelar?

Temos vários exemplos concretos de inovação que temos feito em Portugal, à volta do 5G. Em outubro divulgámos, em conjunto com a NOS, a primeira escola 5G em Matosinhos. Também em 2021, certamente se recordam da orquestra conduzida pela maestrina Joana Carneiro, que foi totalmente assente numa experiência 5G fornecida pela Ericsson. Outro exemplo foi o transporte via holograma de um pivô da TVI para um espetáculo em Paredes de Coura, em parceria com a Vodafone. E, em 2019, outro caso prático foi um simulacro numa situação de emergência feita em conjunto com a Altice, em Aveiro. Portanto, penso que há uma infinidade de experiências que certamente vão transformar as experiências que temos, tanto a nível de utilizador final, como das próprias empresas.

Acha que será possível a Europa aproveitar esta oportunidade para avançar com a reindustrialização?

Sim, sem dúvida. Na verdade, as tecnologias vêm trazer as pessoas mais perto entre si mesmas e também mais perto das coisas. Obviamente que para Portugal, já no curto-médio prazo, podemos ver benefícios de cariz económico, em que podemos acelerar a produtividade de determinados setores. Por exemplo, já não importa onde é que o talento ou a pessoa que é espe-

cialista numa determinada área está. Esse especialista pode estar a operar uma fábrica que fica no interior do país, o que também nos permite aproximar o litoral do interior, o que é sempre uma questão importante.
Isto tem impactos de cariz económico, do ponto de vista geográfico e, naturalmente, também se traduz em qualidade de vida porque, sobretudo para Portugal, pode ter vantagens diretas e impactos imediatos, na estratégia de como realmente desenvolver o interior e aproximar as indústrias de onde o talento está.

Acha que o interior será contemplado nas fases de *roll-out* do 5G? Vamos ter um rol-out faseado de forma uniforme em todo o país?

Convém dizer que o *roll-out* será feito e tivemos vários operadores que obtiveram licença de rede para operar redes 5G após o fecho do leilão. E um dos requisitos do leilão será a cobertura de todo o território nacional a 95% até ao ano de 2025.
Portanto, esse *roll-out* será feito pelos nossos operadores, em linha com o regulamento estipulado pelo leilão. Também gostaria de acrescentar que numa primeira fase, e a nível de benefícios do 5G, ao longo dos próximos anos – e tal como já referi relativamente aos casos de uso das diferentes empresas –, o 5G será especialmente relevante para a indústria e para os setores produtivos.
Obviamente que toda a parte das experiências para o consumidor final é algo em que estamos a trabalhar, como já referi, através de soluções de realidade aumentada, realidade virtual e através de conteúdos de alta qualidade. E um exemplo é no segmento dos gamers, ou seja, sabemos que aqui é fundamental que tenham qualidade na experiência e, para tal, a latência tem de ser muito reduzida. É um daqueles exemplos que encaixa perfeitamente numa das aplicabilidades da tecnologia 5G, em que podemos dar o mesmo nível de acesso *anytime, anywhere*. Portanto, não importa se a pessoa está num dispositivo móvel ou num dispositivo fixo, mas a ideia é transmitir e dar aos clientes finais a mesma experiência, independentemente do meio de acesso.
Acho que há aqui toda uma progressão na forma de adoção do 5G, tanto a nível territorial e geográfico, como também do ponto de vista de aplicabilidade, quer seja no setor da indústria ou no cliente final.

Outra coisa interessante é o aparecimento das redes privadas de 5G. Vê isso como uma solução viável em Portugal, haver empresas e instituições que optem por essa via? E se assim for, quais poderão ser os *use cases* que levem a um investimento desse tipo?

No seguimento da nossa liderança tecnológica, especificamente nas redes móveis, obviamente que o nosso posicionamento é sempre continuar a inovar e antecipar eventuais requisitos dos nossos clientes. E especificamente na parte das redes privadas é importante dizer que as nossas soluções são de alta qualidade, de baixa latência e oferecem uma conetividade segura, o que vai ao encontro das necessidades de transformação digital de uma organização.

Uma rede privada é algo fácil de instalar e é na verdade a recomendação para aplicações de uso industrial, tal como os exemplos que já falámos. Neste sentido, cada empresa pode ter o seu portal de gestão em que vai adaptando a experiência consoante as suas necessidades e também garantindo o acesso que necessita de dar aos seus utilizadores. Este acesso, obviamente permite escalabilidade, uma vez que permite que a solução possa ser gerida na cloud, garantindo que a solução está sempre atualizada e também permite – à medida que a empresa cresça –, escalar de forma a garantir compatibilidade com as necessidades em cada momento. As nossas soluções permitem esta evolução na jornada digital que as empresas estão a fazer e pode ser adaptada a qualquer dimensão – desde pequenas a grandes empresas –, e o fundamental é que se consiga responder a cada situação. Desde a gestão de portos à implementação de uma fábrica inteligente, outros exemplos na saúde ou experiências no ambiente académico, para garantir a melhor experiência possível para aquele espectro de utilizadores que estão a captar aquela experiência.

Em relação ao atraso que Portugal tem relativamente aos outros países da Europa, acha que com a preparação prévia que os operadores foram fazendo é possível que em breve consigamos reduzir o gap temporal?

Sem dúvida. Aliás, acho que isso também é o papel da Ericsson, também devido ao seu papel de liderança e conhecimento de redes 5G, de trazer experiências de outros mercados e trazer esses casos que já foram implementados lá fora e adaptá-los – consoante faça sentido –, à nossa realidade nacional. Mas, para isso, necessitamos de fazer este trabalho junto dos nossos operadores. Nesse sentido, sendo a Ericsson uma empresa mundial que está a liderar o desenvolvimento do 5G, tanto do ponto de vista de investigação como de operacionalização nas redes comerciais, conseguimos mitigar

> "O 5G E O EDGE IRÃO FOMENTAR AS VÁRIAS OPORTUNIDADES EM TERMOS DE RECEITAS EM DIFERENTES APLICAÇÕES"

o atraso porque essas experiências vão, obviamente, acelerar o processo de implementação em Portugal e, mais que isso, adequar e dizer quais são as experiências que fazem mais sentido para a nossa realidade.

Como é que a Ericsson hoje se posiciona neste espaço da descentralização do Edge (o que quer que hoje seja o Edge)?

O 5G e o Edge irão fomentar as várias oportunidades em termos de receitas em diferentes aplicações, sejam receitas em manufatura, transportes, gaming, entre outras. O Edge em redes móveis é muitas vezes referido como o mobile edge computing. Basicamente, na nossa linguagem isto quer dizer que é colocar os recursos de execução, do ponto de vista de armazenamento, mas também da própria computação do aplicativo, em redes próximas aos utilizadores finais para proporcionar uma melhor experiência.

Vemos muito isto nos casos de *gaming*, por exemplo, em que a nível de experiência de cliente final é bastante exigente. Portanto, há aqui um cenário em que em vez de todo o aplicativo estar no telemóvel do utilizador, como as nossas soluções incluem baixa latência e elevada largura de banda, o que é feito é distribuir a mesma inteligência e o mesmo *asset* por vários sites dentro da cloud.

Obviamente que isto permite uma grande oportunidade para os fornecedores de serviços, porque em vez de haver um modelo tradicional de conetividade, estamos a falar de uma rede totalmente distribuída que permite, não só melhorar a experiência, como também do ponto de vista de utilizador final já não precisa de ter um smartphone que aguente com uma bateria e capacidade de armazenamento que suporte toda essa experiência. Isto vai desde as experiências de gaming para o utilizador final, como também outras experiências que incluem aplicativos para a área industrial em que, nesse caso, pode ser haver um complemento entre a tal rede privada das indústrias e a rede comercial dos operadores, em que o próprio Edge pode ser colocado em instalações corporativas, seja dentro de prédios, fábricas, comboios, aviões ou carros particulares. E isto é de forma a garantir sempre uma melhor experiência para o utilizador final, e que seja tudo feito de forma eficiente do ponto de vista do fornecedor de serviços.

Que perceção tem a Ericsson, em termos do mercado nacional, sobre a recetividade das empresas em relação ao 5G?

Obviamente que isto será sempre um processo que vamos desenvolvendo em conjunto com os nossos parceiros operadores, mas sem dúvida que é interessante referir que desde a administração pública às entidades privadas, há bastante curiosidade em perceberem exatamente os benefícios do 5G. Isto, não só de uma perspetiva da aproximação das pessoas à tecnologia, mas também a todos os benefícios que daí advêm, desde benefícios de cariz económico a benefícios sociais. Ou seja, para ter uma determinada experiência já não importa onde a pessoa está e, com isto, acho que há muitos benefícios para ainda descobrir, mas há sempre – como em qualquer outra tecnologia –, uma curva natural de adoção que tem a ver com a preparação do mercado para a receção dessa mesma tecnologia e, também, com a evolução natural da tecnologia.

É importante referir que estamos na fase inicial, pelo menos no mercado nacional, mas esperamos que à medida que vamos trazendo esses casos de uso e essas experiências de outros mercados que uma referência gere outra e que se consiga aqui um interessante efeito bola de neve.

Que mensagem gostaria de passar aos leitores da IT Insight, e também aos gestores nacionais, relativamente a esta altura de transição em que nos encontramos?

Diria que, neste momento, estamos num verdadeiro momento de evolução tecnológica em Portugal. Portugal já é um país bastante competitivo, inovador e atrativo de investimento externo, especialmente no setor das tecnologias da informação. E é muito interessante ver que Portugal é muitas vezes usado como referência a nível tecnológico. Portanto, para os vossos leitores, acho que a minha questão é como é que todos em conjunto criamos um ecossistema que beneficie as empresas, a sociedade e o nosso país. Penso que é necessário e seria positivo haver mais sessões de debates entre todos, exatamente para identificarmos essas oportunidades com as quais todos podemos beneficiar.

Isso requer algum *brainstorming* para identificar situações que sejam *win-win* para todos – é um ecossistema bastante completo e complexo –, mas penso que pelo menos não há dúvida de que é uma transformação tecnológica que vai trazer benefícios de larga escala em vários setores. Isso é sem dúvida um bom momento onde todos podemos contribuir e não é em todas as décadas em que podemos assistir e participar nesta revolução tecnológica que estamos agora a iniciar.

Portanto, deixo aqui a todos um voto para participarmos nesta discussão, porque acho que é uma revolução que se faz a várias mãos e, portanto, pelo menos da minha parte e da Ericsson Portugal há toda a disponibilidade e interesse em também dinamizarmos esse tipo de discussões e de debates. ■

CAPEFOXX
smart software solutions

O MELHOR DE DOIS MUNDOS NO CONSUMO DE SOFTWARE

Modelos híbridos de consumo de software permitem às empresas a liberdade para disponibilizar, quando necessário, das versões mais recentes de aplicações Microsoft na cloud e simultaneamente disfrutar da economia e flexibilidade de licenças em segunda mão.

COM O CRESCENTE relevo da agilidade, resiliência e continuidade de negócio, os modelos híbridos são a ordem do dia. Seja nas arquiteturas de cloud, para otimizar a alocação de recursos às diferentes *workloads*, ou nos modelos de trabalho, para maximizar a produtividade e colaboração, as empresas procuram cada vez mais obter o melhor de dois mundos e responder às necessidades dos utilizadores e do negócio com o máximo de eficiência e flexibilidade possível.

Do mesmo modo, muitas empresas usam uma mistura de ferramentas de software desktop e cloud, adquiridas e *as-a-service*, de forma a melhor responder às suas necessidades de negócio, dentro do contexto dos seus recursos, orçamentos e arquiteturas de IT específicas.

Isto verifica-se inclusivamente no uso de produtos Microsoft – no entanto, este uso nem sempre é otimizado. Isto porque, por cada licença, a empresa está a pagar por todas as funcionalidades incluídas independentemente destas serem utilizadas.

Assim, o já de si avultado investimento em produtos Microsoft implica frequentemente – em 70% dos casos, segundo estudos recentes – pagar por funcionalidades que nunca vão ser usadas.

- Corrado Farina, Director Sales South da Capefoxx -

UM MODELO DE CONSUMO MAIS FLEXÍVEL

A resposta a este problema é o desenvolvimento de um modelo de consumo híbrido, ajustado às necessidades das empresas, que integra tanto licenças cloud como em segunda mão.

Assim, as empresas beneficiam do melhor de dois mundos, alocando os recursos de acordo com as necessidades dos utilizadores. A própria Microsoft oferece esta possibilidade através de licenças Enterprise E1, que permitem subscrever a aplicações específicas por utilizador individual. Assim, os colaboradores que, pela natureza das suas funções, precisam de acesso à versão mais recente de serviços como o Microsoft Teams ou o Microsoft SharePoint, podem disfrutar das mesmas. Paralelamente, tanto estes utilizadores como os restantes podem utilizar software Office de desktop adquirido separadamente.

Ao garantir o acesso individual aos serviços cloud necessários dispensa a aquisição em massa de licenças nas quais estas funcionalidades estariam incluídas, oferecendo assim às empresas maior liberdade de escolha. Isto é importante porque as versões mais recentes de ferramentas Office e sistemas Windows nem sempre são a escolha ideal para responder às necessidades das empresas. Em muitos casos, por exemplo, o Office 2016 pode ser tão adequado como o Office 365, a um preço significativamente menor. Nesse caso, as empresas podem conseguir poupanças significativas através da aquisição de licenças usadas, pelas quais outras organizações pagaram na totalidade mas já não usam.

Desta forma, é possível alcançar poupanças de até 70% no licenciamento de software, libertando capital para investir em projetos de valor acrescentado que ajudem a empresa a crescer.

A SOLUÇÃO CERTA COM O PARCEIRO CERTO

Contudo, a implementação de um modelo híbrido de consumo com recurso a licenças em segunda mão deve ser cuidadosamente estudada e planeada com a ajuda de um parceiro qualificado. Por um lado, de forma a criar um use case que responda precisamente às necessidades da organização, tendo em conta os seus recursos, constragimentos, arquitetura de IT, estratégia a longo prazo, etc. Por outro, de forma a mediar o processo de transferência das licenças. Desde 2012, a aquisição e revenda de licenças de software é permissível dentro da União Europeia; contudo, não sendo estas ativos físicos, este é um processo altamente complexo que requer um mediador especializado de forma a garantir a cumprimento legal e dos termos de licenciamento da Microsoft. É aqui que entra a Capefoxx e os seus Parceiros. Não apenas ao fornecer suporte legal e administrativo no processo de transferência das licenças, mas também ao ajudar as empresas a determinar as suas necessidades exatas de forma a criar um modelo de aquisição precisamente ajustado às mesmas.

Como as restantes estratégias digitais híbridas, cada vez mais comuns, este modelo de consumo oferece às empresas altos níveis de flexibilidade, otimizando as suas despesas e *performance* ao mesmo tempo que garante o acesso – sempre que, e apenas quando, necessário – às versões mais recentes de aplicações e serviços Microsoft. ■

Capefoxx is Europe´s trusted source for used Microsoft software licences

CAPEFOXX VERIFIED
LEGALLY COMPLIANT – AUDIT SECURE *

Save serious money with second-hand volume licences.
Or turn your unused software capital into an asset.

- ✓ Capefoxx offers expert advice in all products, licensing, and legal matters.
- ✓ Capefoxx has a proven record of being knowledgeable, experienced, and reliable.
- ✓ Capefoxx strictly observes all legal and manufacturers' requirements.

* Regarding the purchase and sale of licences, Capefoxx verifies that all requirements are met in order for licences to be transferred in line with the law and approved in audits.

Questions? Our experts will be happy to assist you.
sales@capefoxx.com

www.capefoxx.com

CAPEFOXX
smart software solutions

"APOSTAR EM INTEGRAÇÃO É FUNDAMENTAL"

O Credibom sentiu a necessidade de implementar uma plataforma que permitisse crescer de forma sustentada no que toca à integração.

DIANA RIBEIRO SANTOS

O DESAFIO

Anteriormente, o Credibom não tinha uma capacidade forte de rastreabilidade e de *governance* de serviços. As integrações entre sistemas eram realizadas ponto-a-ponto de forma direta ou, em alguns casos, através de outra solução de *middleware*.

No entanto, estas implementações demonstravam uma dependência forte entre os sistemas e fraca rastreabilidade. A falta de normalização e de *governance* tornava a análise dos fluxos e despiste de problemas um processo complexo e a manutenção deste caminho limitava muito o crescimento do negócio porque qualquer alteração era demasiado pesada e até dispendiosa, tanto para o Credibom como para os seus parceiros.

Hoje, as empresas precisam de garantir que as suas plataformas de *middleware* são competitivas, mas seguras. Apostar em integração é fundamental para aumentar a produtividade e suportar, de forma sustentável, o negócio digital das organizações.

A SOLUÇÃO

A Xpand IT teve como objetivo desenvolver uma solução que respondesse aos requisitos do cliente: escalabilidade, agilidade, segurança e visibilidade para toda a empresa. Para além disso, era importante criar uma representação canónica dos dados de forma a poderem modelar de uma forma mais clara e coerente o negócio da organização.

Assim, foi implementada uma solução de *middleware* com os componentes WSO2 necessários para a integração de sistemas e gestão de API. A esta plataforma juntou-se a implementação de uma *framework* de serviços capaz de oferecer às equipas de desenvolvimento os standards, a rapidez e a qualidade na implementação de serviços, promovendo um modelo de fábrica totalmente alinhado com a arquitetura e evolução da solução.

Sendo o WSO2 uma tecnologia *open-source* acaba por beneficiar de atualizações e melhorias constantes resultantes não só do *vendor* como da contribuição da comunidade. Para além disso, ao ser usada mundialmente por inúmeras empresas de todas as dimensões e setores de negócio, obedece a requisitos de qualidade e segurança apertados e garante o alinhamento com os standards da indústria. Da mesma forma, esta tecnologia tem acompanhado e evoluído na direção das tendências arquiteturais, estando atualmente capacitada para responder ao desafio de integração em ambientes *on-premises*, cloud ou híbridos, e em arquiteturas baseadas em microserviços e de containerização, seja ela gerida pelo cliente ou pela própria WSO2 (através da sua oferta iPaaS).

A solução implementada tem três grandes áreas de valor: a tecnologia, a arquitetura e *framework* de desenvolvimento. A arquitetura e a *framework* têm evoluído com a organização, conforme surgem novas necessidades ou particularidades que devem ser endereçadas, sejam funcionais ou técnicas. Alguns exemplos são a adaptação a um crescente volume de transações ou a criação de mecanismos dinâmicos de avaliação de regras.

Com a introdução da nova solução foi desenhada uma arquitetura de integração de raiz, focada na abstração e padronização das integrações, promovendo a reutilização e a modelação da informação para o negócio. Desta forma, o Credibom conseguiu melhorar a visibilidade e a organização dos fluxos de dados, ao mesmo tempo que asseguraram uma maior rapidez e qualidade na criação de novas integrações, suportando assim um crescimento sustentável nas diversas iniciativas de digitalização.

"A Xpand IT é uma empresa bem cotada no mercado e com muita experiência no que diz respeito a soluções de integração. Era também na altura o único parceiro WSO2 em Portugal, uma solução *open source*, mas corporativa, para a qual já estávamos a olhar, e que nos oferece a capacidade de implementação de serviços, a sua reutilização, rastreabilidade, segurança, padronização dos serviços, controlo e muita agilidade", João Mendes, CTO do Credibom.

OS RESULTADOS

Segundo Nuno Santos, IT Manager Enterprise Solutions da Xpand IT com esta solução, é possível, agora, criar novos serviços e alterar existentes no Credibom com grande rapidez e com impacto mais reduzido para os consumidores, o que se revela um enorme benefício. Além disso, a componente de gestão de API oferece um novo meio capaz de facilitar e agilizar todo o processo de criação, disponibilização e consumo de serviços de valor para parceiros e clientes finais.

"O *feedback* foi sempre bastante positivo. Acreditamos que a solução desenvolvida veio, realmente, trazer inúmeros benefícios para a empresa, e os resultados também acabam por comprovar isso mesmo. A forma próxima como trabalhamos com os clientes, numa lógica de parceria, também permite que os projetos acabem por correr da melhor forma, porque conseguimos antecipar necessidades e agir no sentido de resolver os temas mais complexos com as soluções mais adequadas", explica.

O Credibom passou a ter "serviços atómicos" que estão alinhados e fazem sentido para o negócio, o que leva à sua reutilização e até à capacidade de criar serviços compostos e mais complexos com muito mais facilidade e controlo; aumentaram a segurança no acesso aos serviços, assegurando a identidade e a utilização de quem os invoca; passaram a ter dados estatísticos da utilização dos serviços para perceber os sistemas e serviços mais utilizados o que ajuda a planear melhor o futuro dos mesmos; melhoram a padronização e *governance* dos serviços recorrendo a uma estrutura de *middleware* que é escalável e consegue acompanhar o crescimento do negócio; e por último, uma *framework* ágil de implementação de serviços e uma abordagem *self-service* baseada em API que permite aos parceiros e mesmo às suas equipas internas a possibilidade de criar ou aceder à informação de uma forma mais fácil e ágil.

Atualmente, o Credibom já conta com as integrações online suportadas na solução, num universo de cerca de 250 serviços. ■

OBRIGADO POR TER LIDO A IT·Insight

Para continuar a receber regularmente a sua IT Insight, por favor atualize os seus dados profissionais aqui

Conheça a política de privacidade da IT Insight aqui

IT·Insight

PUBLISHER: Jorge Bento

DIRETOR: Henrique Carreiro

CHEFE DE REDAÇÃO : Rui Damião - rui.damiao@medianext.pt

REDAÇÃO: Diana Ribeiro Santos, Margarida Bento, Maria Beatriz Fernandes

JORNALISTA CONVIDADO: Fátima Ferrão

GESTÃO DE PARCEIROS:

Business Development Lead: Rita Castro – rita.castro@medianext.pt

Senior Account Executive: João Calvão – joao.calvao@medianext.pt

MARKETING COMMUNICATIONS ASSISTANT: Daniela Botelho

ARTE E PAGINAÇÃO: Teresa Rodrigues

WEB: João Bernardes

DESENVOLVIMENTO WEB: Global Pixel

A REVISTA DIGITAL INTERATIVA IT INSIGHT É EDITADA POR:

MediaNext Professional Information Lda.

GERENTE: Pedro Botelho

SEDE E REDAÇÃO: Largo da Lagoa, 7c, 2795-116

Linda-a-Velha, Portugal

TEL: (+351) 214 147 300 | **FAX**: (+351) 214 147 301

IT INSIGHT está registada na Entidade Reguladora para a Comunicação Social nº127295

Consulte aqui o Estatuto Editorial