SPECIAL EDITION | NEWS

MAIO | JUNHO 23
DISPONÍVEL POR ASSINATURA

SECURITY MAGAZINE

REVISTA DOS PROFISSIONAIS DE SEGURANÇA

MARQUE PRESENÇA NA SECURITY MAGAZINE

WEBSITE . NEWSLETTER . EVENTOS . REDES SOCIAIS . BRAND CONTENT

Solicite o nosso media kit e/ou tabela de publicidade

GERAL@SECURITYMAGAZINE.PT

"TODOS OS ACONTECIMENTOS SÃO ÓTIMAS OPORTUNIDADES PARA A EVOLUÇÃO"

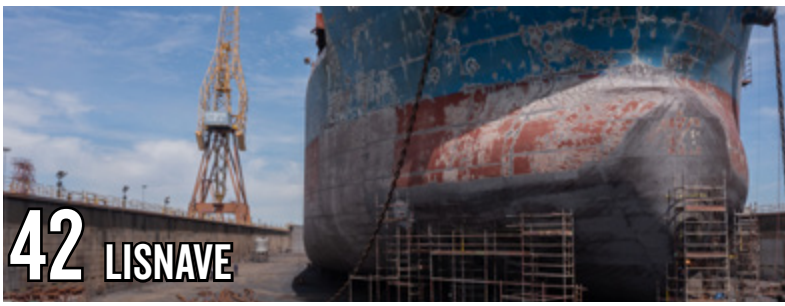
Masaharu Taniguchi

Num mundo cada vez mais conectado, a cibersegurança é uma preocupação central das empresas e entidades, públicas e privadas. A grande evolução da tecnologia traz várias oportunidades, porém, cria alguns desafios e um ambiente propício para ameaças virtuais. Os ciberataques são cada vez mais frequentes, abrangentes e disruptivos. A sofisticação destes ataques ganha proporções consideráveis e com fortes implicações para as empresas e quotidiano de todos nós. Enfrentar estas ameaças requer investimento por parte das organizações e preparação, muita preparação, baseada em treino adequado e conhecimento. Um dos temas em constante análise é a escassez de profissionais qualificados, uma realidade que afecta esta área como tantas outras. A Security Magazine foi conhecer a opinião de alguns especialistas sobre estas temáticas.
Nesta edição, damos a conhecer também a realidade da SALTO Systems, dedicada ao desenvolvimento de soluções de controlo de acessos, entre outros, e os investimentos do distribuidor Visiotech Portugal, que passa a contar com instalações próprias em Portugal. Em termos de lançamentos de novas ferramentas, destacamos o COSMO VMS da Nauta e o Geiss da E-coordina, as quais vêm revolucionar e ajudar os profissionais da segurança no terreno. Damos ainda os parabéns à Junheinrich Portugal, empresa dedicada à intralogística, nomeadamente equipamentos de movimentação de cargas, pelo seu 25º aniversário no país. Destacamos ainda o trabalho desenvolvido pela Lisnave, em Setúbal, ao nível da segurança no trabalho, numa área tão desafiante e perigosa como a reparação de navios, esses gigantes dos mares. Por fim, destacamos a última edição da Proteger, organizada pela APSEI, que pela primeira vez decorreu no Norte do país e que reuniu várias centenas de profissionais durante dois dias.
Boas Leituras.

RITA SOUSA
DIRECÇÃO EDITORIAL

RITA.SOUSA@SECURITYMAGAZINE.PT
LINKEDIN | www.linkedin.com/in/ritassousa

EDITORIAL



SUMÁRIO

FICHA TÉCNICA

DIRECÇÃO EDITORIAL
Rita Sousa

MARKETING & COMERCIAL
Vanesca Mendes, Alexandra Amaro, Sara Palma

GESTÃO DE EVENTOS & FOTOGRAFIA
Vanesca Mendes

PAGINAÇÃO
Security Magazine

Créditos
Freepik iStockphotos

Morada da Redacção
Av. Eng. Duarte Pacheco 248, 1ºE
2870-216 Alto das Vinhas - Portugal

Propriedade
Rita Simões de Sousa

Telefone
212314944 (Chamada rede nacional)

Email
geral@securitymagazine.pt

Publicidade e informações
geral@securitymagazine.pt

Notícias
redaccao@securitymagazine.pt

Periodicidade bimestral

Website
www.securitymagazine.pt

Assinatura anual papel e digital (seis edições) 119 euros + IVA. Gráfica: Print 24 - Alemanha. Email marketing EGOI

Lançamento
2018

Esta edição é especial e exclusiva, um suplemento do seu site Security Magazine - Revista dos Prossionais de Segurança e está disponível apenas para profissionais de segurança por assinatura.

Indisponível em banca.

SOCIAL MEDIA

@ SECURITYMAGAZINEPT/

@ SECURITYMAGAZINEPT/

@SECURIITY.MAGAZINEPT

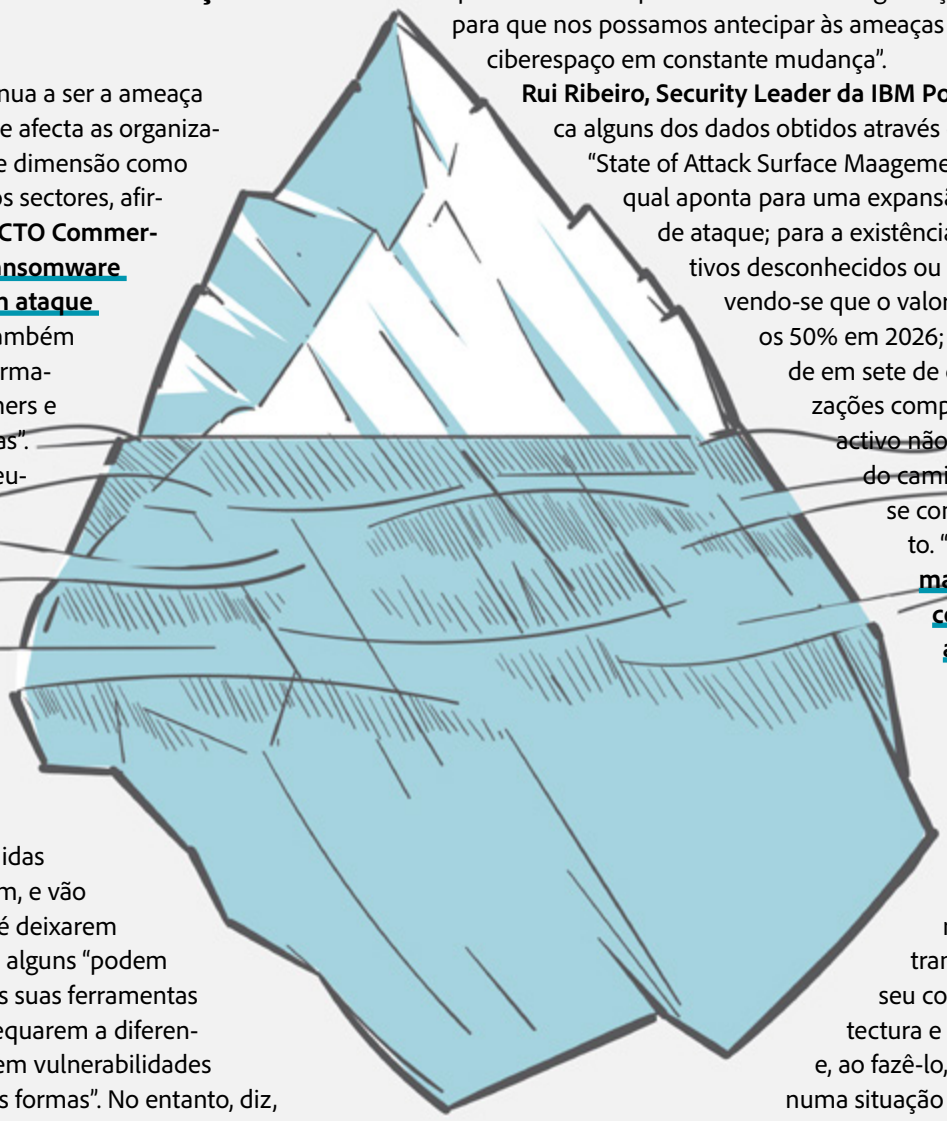
@ SECURITYMAGPT

SECURITY MAGAZINE SM

INFORMAR COMUNICAR INOVAR

ELEVAR A FASQUIA

A cibersegurança continua na ordem do dia das organizações, sendo hoje uma das principais preocupações dos seus gestores. A Security Magazine consultou a opinião de três especialistas sobre as ameaças iminentes e a evolução da superfície de ataque, a escassez de competências e a mudança da mentalidade.



"O ransomware continua a ser a ameaça mais prevalecente que afecta as organizações", tanto de grande dimensão como de pequena, em vários sectores, afirma **John Shier, Field CTO Commercial, da Sophos**. "O **ransomware é a última fase de um ataque bem-sucedido** que também inclui o roubo de informações, trojans, critominers e muitas outras ameaças". Segundo aponta, "a reutilização de técnicas de ataque existentes e o aparecimento de novos ataques são comuns no panorama de ameaças. Os cibercriminosos reutilizam frequentemente ferramentas e técnicas bem-sucedidas porque elas funcionam, e vão continuar a fazê-lo até deixarem de funcionar". Porém, alguns "podem modificar e adaptar as suas ferramentas e técnicas para se adequarem a diferentes alvos ou explorarem vulnerabilidades semelhantes de novas formas". No entanto, diz, "surgem novos métodos de ataque, à medida que a tecnologia evolui e os atacantes procuram continuamente novas formas de contornar as medidas de segurança". Perante a melhoria das defesas, **"vimos os cibercriminosos adoptarem drivers vulneráveis para contornar as ferramentas de Detecção e Resposta de Endpoints (EDR)**". Também são vistos "a imitarem grupos de Estados-nação, integrando as ferramentas e tácticas destes últimos nos seus manuais de ataque".

À medida que a superfície de ataque evolui, "é importante que os indivíduos, organizações e governos se mantenham vigilantes, implementem práticas de segurança robustas e invistam em inteligência sobre ameaças, monitorização proactiva e capacidades de resposta a incidentes", alerta. Avaliações de segurança regulares, gestão de patches, sensibilização dos colaboradores e parcerias com especialistas em cibersegurança "são cruciais para que nos possamos antecipar às ameaças emergentes no ciberespaço em constante mudança".

Rui Ribeiro, Security Leader da IBM Portugal, destaca alguns dos dados obtidos através do seu estudo "State of Attack Surface Maagement Report", o qual aponta para uma expansão da superfície de ataque; para a existência de 30% dos activos desconhecidos ou não geridos, prevendo-se que o valor aumente para os 50% em 2026; e para o facto de em sete de cada 10 organizações comprometidas, um activo não gerido foi parte do caminho crítico desse comprometimento. "**Esta situação materializa o que costumo chamar a »espargata tecnológica«**". Por exemplo, "as organizações começarem a passar workloads para a Cloud não tendo transformado o seu contexto, arquitectura e procedimentos e, ao fazê-lo, colocarem-se numa situação de sustentação muito difícil – ainda que por um período limitado". O risco associado a este processo é identificado no estudo da empresa, "Cost of a Data Breach", que refere que "**as organizações estão mais vulneráveis a ciberataques em momentos de transição na sua jornada para a Cloud**". Do ponto de vista de um atacante, "esta situação é claramente favorável – pois a um atacante basta encontrar um ponto de penetração, enquanto os defensores têm de manter sob vigilância todos os possíveis vectores". O responsável destaca que tem havido nos últimos anos "um enorme aumento do interesse dos atacantes sobre tecnologias OT – por via destas terem-se tornado progressivamente "ITizado" e estarem, cada vez mais, expostas –, e isso pode vir a ser traduzido em potenciais consequências cada vez mais reais

ICISSP 2024

10th International Conference on Information Systems Security and Privacy

ROME, ITALY | 26 - 28 FEBRUARY, 2024

Intrusion Detection and Response
Threat Awareness
Identification and Access Control
Privacy-Enhancing Models and Technologies
Security Architecture and Design Analysis
Web Applications and Services
Security Testing
Risk and Reputation Management
Privacy Metrics and Control
Authentication, Privacy and Security Models
Data and Software Security
Legal and Regulatory Issues
Security and Trust in Pervasive Information
Vulnerability Analysis and Countermeasures
Pattern Recognition
Information Hiding and Anonymity
Mobile Systems Security
Data Mining and Knowledge Discovery
Cryptographic Algorithms
Security Awareness and Education
Security Frameworks, Architectures and Protocols

The International Conference on Information Systems Security and Privacy is an event where researchers and practitioners can meet and discuss state-of-the-art research about the technological, social, and regulatory challenges that regard the security, privacy, and trust of modern information systems. The conference welcomes papers of either practical or theoretical nature, and is interested in research or applications addressing all aspects of trust, security and privacy, and encompassing issues of concern for organizations, individuals and society at large.

MORE INFORMATION AT: HTTPS://ICISSP.SCITEVENTS.ORG

UPCOMING SUBMISSION DEADLINES

REGULAR PAPER SUBMISSION: **OCTOBER 9, 2023**

POSITION PAPER SUBMISSION: **NOVEMBER 17, 2023**

SPONSORED BY: INSTICC

INSTICC IS MEMBER OF: WfMC, OMG

LOGISTICS: SCITEVENTS

PAPERS WILL BE AVAILABLE AT: SCITEPRESS DIGITAL LIBRARY

POST PUBLICATIONS: Springer Nature Computer Science, Communications in Computer and Information Science

IN COOPERATION WITH: AP2SI

PROCEEDINGS WILL BE SUBMITTED FOR INDEXATION BY: Scopus, Google Scholar, dblp, Semantic Scholar, Clarivate

Scan and connect to: icissp.scitevents.org

para os cidadãos". Em 2021, houve um aumento de 2.204% nas actividades de "reconhecimento " sobre dispositivos OT a partir da internet, recorda.

Marcelo Carvalheira, country manager da Fortinet Portugal, recorda o relatório "FortiGuard Labs Threat Landscape", no qual a empresa notou o reaparecimetno de nomes conhecidos ao nível do malware, wiper e botnet, incluindo o Emotet e GandCrab. O responsável destaca que "as cinco principais famílias de ransomware, de um total de 99 detectadas, foram responsáveis por cerca de 37% de toda a actividade de ransomware no segundo semenstre de 2022". Como sublinha, o malware mais proeminente foi o GandCrab, uma ameaça RaaS que surgiu em 2018. "Vimos que a maior parte das primeiras posições eram ocupadas por malware com mais de um ano. Alguns deles – como o Lazurus – existem há mais de 10 anos e são pilares da história da Internet", diz. Como aponta, "esta reunitilização de Código permite que os hackers se baseiam em resultados de sucesso anteriores, melhorando interactivamente os seus ataques e ultrapassando as barreiras defensivas". Como salienta, "**os cibercriminosos têm um espírito empreendedor** e estão constantemente à procura de formas de aumentar o valor dos actuais investimentos e conhecimentos em operações de ataque para ampliar a sua eficácia e rentabilidade". Além da reutilização de código, "estão a maximizar as oportunidades utilizando ameaças conhecidas e infraestruturas existentes". Por exemplo, "se olharmos para as ameaças de botnets em função da sua difusão, muitas das principais botnets não são novas – entre as cinco principais botnets observadas, apenas a RotaJakiro foi criada nos últimos dois anos". Como existe retorno do investimento, "continuam a explorar a actual infraestrutura botnet e a transformá-la em versões cada vez mais persistentes, utilizando técnicas altamente especializadas". A reutilização de código e a modularização possibilitada por um ecossistema de Crime-as-a-Service em expansão reforça a importância dos serviços de segurança que podem ajudar as empresas a afastar as ameaças com uma defesa coordenada e impulsionada por IA". De acordo com o relatório global de Ransomware de 2023, "apesar de uma economia em mudança, quase todas as organizações (91%) esperam aumentar os orçamentos em segurança no próximo ano".

Rui Duro, country manager da Check Point Software em Portugal, destaca que as ameaça "têm vindo a progredir a um ritmo extraordinário nos últimos anos. Tudo muito devido a uma maior sofisticação e capacidade de compreensão de oportunidades para potenciais ataques. As superfícies de ataque não estão a evoluir, elas mantém-se as mesmas, porém a abordagem às mesmas é que tem vindo a ser alvo de uma criatividade maquiavélica por partes dos cibercriminosos, que não deixaram de usar as antigas atividades de crime de engenharia social, e têm vindo a explorar também as falhas técnicas e humanas que se tornam cada vez mais sensíveis".

Escassez de competências

Para o responsável da IBM, o tema da inclusão, incluindo a diversidade de género, diversidade racial e neurodiversidade "são de facto abordagens interessantes (não só do ponto de vista da justiça, mas da sua eficácia), como fonte de captação de recursos para procurar endereçar a falta de competências". Mais do que procurar recursos técnicos, com competências de engenharia, **"as organizações precisam de procurar recursos com características individuais adequadas aos perfis em falta"**. Na verdade, "há quem refira que os profissionais destas áreas de Cibersegurança e Segurança da Informação têm "a certain brain wiring", ou seja, que têm uma forma de pensar única – o profissional de segurança é a pessoa que quando uma porta tem o letreiro "Puxe" pergunta-se: «O que acontece se eu empurrar?»" Segundo o responsável da IBM, "uma outra abordagem complementar é a de definir processos muito estruturados para certas actividades, atomizando-as de tal forma que recursos com menos conhecimento possam ser utilizados – isto pode ser particularmente verdade para sistemas grandes, em que a economia de escala possa ser alavancada". Dito isto, "estas abordagens requerem que as organizações tenham a capacidade de localizar estes perfis, e depois treiná-los para as competências necessárias – o que nem sempre acontece". Uma terceira dimensão, diz, "é a utilização de tecnologia diversa para aumentar as capacidades dos humanos, e desmultiplicar o esforço humano na identificação, protecção, detecção, resposta e recuperação dos ambientes (nomeadamente, IA Orquestração e Automação de processos)". Por fim, refere, "o próprio mercado está a encarregar-se de progressivamente resolver o problema, com o crescente interesse por cibersegurança, uma vez que há cada vez mais jovens interessados no tema – e que encontrarão um mercado de trabalho entusiasmado por os receber".

Sobre o problema da escassez de competências detectada na área da cibersegurança e segurança da informação, o responsável da Sophos destaca que são necessárias várias soluções em muitas frentes. "A diversidade e inclusão são estratégias muito importantes, e algumas estratégias adicionais incluem a colaboração com o meio académico para garantir um fluxo constante de profissionais qualificados quando saem das faculdades e universidades". Outra estratégia é a "**melhoria das competências ou requalificação dos actuais profissionais de TI, para que possam transitar para funções centradas na cibersegurança**". A automação poderá "aliviar alguma da carga de trabalho manual e aumentar as capacidades humanas". Como destaca, "é importante notar que colmatar o défice de competências de cibersegurança é um esforço a longo prazo que exige o empenho dos sectores público e privado", sendo que "a colaboração, investimento e uma abordagem abrangente são essenciais para desenvolver uma mão-de-obra especializada em cibersegurança capaz de se defender contra ameaças em constante evolução". "Como se não bastasse a preocupação de se anteciparem aos cibercriminosos, as organizações também estão a trabalhar para gerir outro risco: a

escassez de talentos", reforça o responsável da Fortinet. Neste sentido, diz, "o recrutamento e a retenção de profissionais qualificados exigirão, inevitavelmente, estratégias criativas entre as organizações que procuram preencher essas funções". Como sugestão deixa a aposta em formação contínua aos profissionais actuais, recrutar talentos inexplorados e estabelecer parcerias e recrutar junto de instituições de ensino superior, medidas nas quais a Fortinet está fortemente empenhada.

O responsável da Check Point indica que "de nada vale criarmos teses assentes em modismos, interesses e pressões sociais, quando o problema está no conhecimento básico. E para o conhecimento básico só a educação e formação contínua pode combater este problema".

O elo mais fraco

Os seres humanos desempenham um papel crítico na cibersegurança e são frequentemente designados como o "elo mais fraco". Como é que os empregadores podem elevar a fasquia para evitar a exploração do comportamento ou da psicologia humana? Será que as empresas devem avaliar o desempenho/consciência dos funcionários em matéria de segurança? O responsável da Sophos considera que "embora os seres humanos possam, de facto, ser fáceis de enganar, também podem actuar como uma primeira linha de defesa contra os ataques". Neste sentido, as equipas de segurança

"devem providenciar formação e sensibilização, mas também processos de execução fácil e irrepreensível para comunicar actividades suspeitas". Segundo aponta, **"confiar nos humanos para serem a única linha da frente de defesa contra os ataques nunca vai funcionar"**. Assim, sugere que "deve ser implementada tecnologia que limite o volume de ataques a que os humanos estão sujeitos e que detecte rapidamente actividades suspeitas quando os humanos falham". Em alguns casos, como o comprometimento de emails empresariais, "as mitigações são orientadas para os processos e não para a tecnologia. Todas estas vertentes devem ser consideradas aquando da implementação de um plano de defesa".

O responsável da Fortinet destaca que "ter pessoas, processos e tecnologias certas é uma componente vital de qualquer estratégia eficaz de gestão de riscos, incluindo os colaboradores que desempenham um papel crucial na segurança da empresa". De acordo com o Security Awareness and Training Global Research de 2023 da Fortinet, 81% dos ataques de

malware, phishing e/ou password ocorridos nas organizações no ano passado foram direccionados aos utilizadores.
"Embora os atacantes estejam constantemente a encontrar novas formas de se infiltrarem nas organizações, a realidade é que, normalmente, são os colaboradores – e não apenas a equipa de segurança – que estão na linha da frente quando se trata de travar os ciberataques", diz. Neste sentido, **"a força de trabalho tem potencial para ser uma das melhores defesas contra os ciberataques, mas isso só é possível se os colaboradores conhecerem e puderem identificar rapidamente os métodos comuns que os agentes de ameaças utilizam para obter acesso a uma rede**". Uma das melhores formas de garantir que os colaboradores têm esse conhecimento crucial é "implementar um programa de formação contínuo de conscientização cibernética".
"Com mais de 90% dos líderes a acreditar que o aumento da consciencialização dos colaboradores em matéria de segurança ajudaria a diminuir a ocorrência de ciberataques, é importante procurar formações que não só abranjam os aspetos básicos – como phishing, ransomware, utilização de redes sociais, utilização de dispositivos móveis ou engenharia social e segurança na cloud – mas que também permitam personalizar o conteúdo, como a inclusão de formação sobre táticas de ataque que sejam exclusivas a cada sector".
Para o responsável da IBM, "um sistema é tanto mais fraco quanto o mais fraco dos seus elementos". Como exemplo, aponta que numa experiência social realizada em Londres há cerca de 10 anos, permitia-se a utilizadores ter acesso a um hotspot wi-fi com base num conjunto de Termos & Condições, o primeiro dos quais era "doar o filho primogénito" ao fornecedor do serviço. Um número esmagador dos utilizadores que se registaram aceitaram estes T&C – porque inevitavelmente não leram o que estavam a assinar, ou seja assinaram um contracto sem ter a noção das suas consequências.
O primeiro princípio que as organizações devem implementar para "elevar a fasquia", é "procurar transformar os utilizadores de "elo mais fraco" em "primeira linha de defesa", e entenderem que esta jornada não se consegue exclusivamente com "formações em cibersegurança", mas com a criação de uma certa cultura de segurança generalizada, que começa pela valorização da informação a que os utilizadores têm acesso e da sua importância na sua defesa, bem como pela clara explicação das consequências de uma falha no processo, seja esta por que razão for".
Na IBM, "tenho tido várias experiências em que este tipo de mentalidade, quase obsessiva, vai sendo transmitida às novas contratações que, por sua vez, já nascem numa cultura de protecção da informação". Os componentes necessários à criação dessa cultura " passam acima de tudo pela capacidade de gerar o entendimento de que é responsabilidade do utilizador proteger a sua informação e, não menos importante, informar imediatamente em caso de potencial risco para a organização".
"**A existência de um contexto generalizado de segurança – por exemplo, a existência de uma segurança física e controlo de acessos eficaz com áreas reservadas – também dá forma a esta mentalidade"**, aponta. Finalmente, "a evolução desta cultura tem de ser permanentemente monitorizada, com testes frequentes a todos os utilizadores, exercícios diversos e um feedback honesto".Como conclui, "as organizações não devem só usar a cibersegurança para proibir, mas que a melhor forma de alterar processos e procedimentos é criar "caminhos de menor resistência" aos utilizadores".


MARCELO CARVALHEIRA, FORTINET

Ao proibir ou restringir alguma actividade, "a organização deve tentar compensar os utilizadores com formas mais fáceis de fazer o mesmo trabalho – para evitar o recurso a shadow IT ou a formas mais "criativas" de trabalhar, e respectiva cultura de informalidade que não se pretende".
Para o responsável da Check Point "as instituições devem desenvolver programas de formação contínua, que levem os seus colaboradores a tomarem uma consciência clara do risco que a cibersegurança acarreta, bem como programas de validação de conhecimento e de simulação periódica de conhecimento com testes, simulações, falsos ataques, que utilizem as mais recentes técnicas de ciberataque para treinar os seus colaboradores a estarem mais despertos e que possam agir corretamente aquando de enfrentar um ataque real. Estes programas, em conjunto com uma solução de cibersegurança completa e integrada permitirá reduzir a "fraqueza" humana".
A ter em conta as respostas dadas à Security Magazine pelos especialistas em matéria de cibersegurança, este é um mercado dinâmico, com uma grande margem de progressão e crescimento, mas também de aprendizagem para as empresas de uma forma transversal. A cibersegurança desempenha um papel crucial na protecção de informações e sistemas vitais no mundo conectado que hoje conhecemos. A consciencialização dos gestores está a mudar e tem aumentado nos últimos anos, à medida que mais pessoas reconhecem os riscos associados à exposição de dados e informação sensível, bem como aos impactos ao nível da interrupção de serviços e as suas consequências para a sociedade civil. Mas se, por um lado, aumenta a consciencialização, do outro lado, do cibercrime, aumentam também os ataques mais sofisticados, com novos ou antigos métodos, tendo em vista, nomeadamente, o lucro. Neste sentido, parece evidente que é essencial a colaboração entre Governos e o sector privado, entre especialistas do sector, tendo em vista enfrentar os actuais e futuros desafios do sector. Importa recordar que na cibersegurança, tal como noutra qualquer área da segurança, o desafio é contínuo e está em constante evolução e mutação, surgindo a cada dia novas e melhores práticas e estados de alerta.•


RUI DURO, CHECK POINT

EQUIPAS DE RESPOSTA A INCIDENTES

UNIÃO FAZ A FORÇA

Com maior ou menor dimensão há cada vez mais empresas e entidades a apostar em equipas de resposta a incidentes de segurança informática (CSIRT) ou equipas de reposta a emergências informáticas (CERT). Estas equipas contam com profissionais de IT que prestam serviços e apoio em matéria de avaliação, gestão e prevenção de emergências relacionadas com cibersegurança, bem como de coordenação dos esforços de resposta a incidentes.

Estas equipas podem estar inseridas em redes que são integradas por outras equipas de outras entidades, públicas ou privadas de diferentes sectores, as quais podem cooperar, trocar informações e criar laços de confiança entre si, no que toca à segurança informática. Estas redes revelam-se cada vez mais necessárias, tendo em conta a complexidade e desafios existentes no ciberespaço.

A primeira vez que o termo CERT foi utilizado remonta a 1988, pelo CERT Coordination Center, da Carnegie Mellon University, na sequência do Morris Worm que paralisou, na altura, uma boa parte da internet. Nessa altura, aquela Universidade criou a primeira equipa de resposta a emergências informáticas, sob contrato com o Governo americano. O termo evoluiu para um termo genérico de CSIRT, sendo hoje uma parte muito importante para as empresas, nomeadamente as de infra-estruturas críticas, tendo evoluído para a criação de centros de operações de segurança (SOC).

A nível europeu, a Agência da União Europeia para a Cibersegurança (ENISA) indica que existem 556 equipas, sendo Portugal o quinto país com maior número de equipas na UE.

A rede de CSIRTs é uma rede em que os membros podem cooperar, trocar informações e criar confiança. Os membros podem melhorar o tratamento de incidentes transfronteiriços e debater a forma de responder de forma coordenada a incidentes específicos.

A rede da ENISA de CSIRTs é composta por CSIRTs nomeadas pelos Estados-Membros da UE e pela CERT-UE ("membros da rede de CSIRTs"). A Comissão Europeia participa na rede na qualidade de observador. A ENISA apoia activamente a cooperação entre as CSIRT, assegura o secretariado e apoia a coordenação de incidentes mediante pedido.

A nível europeu a rede de CSIRT foi criada pela Directiva NIS 1 e reforçada pela Directiva NIS 2, que entrou em vigor em 2023, "a fim de contribuir para o desenvolvimento da confiança e promover uma cooperação operacional rápida e eficaz entre os Estados-Membros". A missão da rede de CSIRTs consiste em trocar informações, criar confiança, discutir e, sempre que possível, implementar uma resposta coordenada a um incidente, prestar assistência aos Estados-Membros na resolução de incidentes transfronteiriços; cooperar, trocar boas práticas e prestar assistência às CSIRT designadas para a divulgação coordenada de vulnerabilidades que possam ter um impacto significativo em entidades de mais de um Estado-Membro.

A ENISA está a impulsionar a rede de CSIRTs, fornecendo o secretariado, as infra-estruturas e as ferramentas que permitem uma cooperação eficaz.•

"QUEREMOS MEMBROS QUE PRETENDAM PROMOVER A CULTURA DE CIBERSEGURANÇA"

Com 15 anos em actividade, a rede nacional CSIRT conta hoje com 61 membros de vários sectores de actividade, desde a banca ao desporto, passando pela academia. A Security Magazine falou com Gonçalo Silva, que exerce funções no Centro Nacional de Cibersegurança e é representante do secretariado que dá suporte à rede, e Pedro Rodrigues, com funções no Banco de Portugal, e membro da comissão executiva da rede.

Security Magazine – Como nasceu a rede nacional CSIRT e como tem evoluído?

Gonçalo Silva – A rede nasceu em 2008, através de algumas pessoas que hoje já não trabalham efectivamente na rede, como o engenheiro Lino Santos, actual coordenador do CNCS. No fundo, teve como membros fundadores a NOS e a RCTS, onde originalmente existia a equipa de resposta a incidentes, o CERT.PT. Conjuntamente tiveram a ideia de constituir um conjunto de equipas de resposta a incidentes que se pudessem ajudar em caso de um acidente em larga escala. Depois da sua criação, foi definido um conjunto de objectivos. Importa referir que a rede não pretende ter empresas com carácter comercial, ou seja, não queremos membros com o objectivo de vender serviço.

Queremos membros que pretendam promover a cultura de cibersegurança, estabelecer laços de confiança entre os elementos, para que quando existir um acidente saibamos com quem podemos contar e contactar. Além disso, a rede pretende criar instrumentos para prevenção num cenário de grande dimensão, como o Wannacry, e promover indicadores e estatísticas.

A rede tem um conjunto alargado de equipas e produz anualmente um questionário que caracteriza os tipos de incidentes trabalhados pelos membros da rede nacional e as próprias equipas de resposta a incidentes, nomeadamente em termos de género, faixa etária, grau de formação, entre outros. Estes dados permitem à rede actuar e partilhar noutros fóruns em que está inserida indicadores relevantes para a definição da estratégia a seguir.

Destaco ainda que a rede participa do Conselho Superior de Segurança do Ciberespaço.

Refere que a rede não tem membros com uma vertente comercial. O que isso significa?

GS – O carácter da rede não é comercial e, sim, de partilha técnica, nomeadamente de experiências, análises forenses, indicadores de comprometimento relativamente a incidentes que ocorrem no ciberespaço de interesse nacional.

Pedro Rodrigues – A rede permite que face a um ciberataque com impacto relevante termos uma rede de suporte. Sabemos que provavelmente existirá um membro que passou por algo semelhante e pode ajudar-nos. Essa é uma das grandes mais-valias da rede do ponto de vista do utilizador.

A concorrência entre as diferentes entidades não tem espaço dentro da rede…

GS – Sim, essa é uma das coisas que nos caracteriza. Aqui não há concorrência. Estamos aqui como parceiros. Temos muito mais membros de empresas privadas do que de públicas, nomeadamente entidades prestadoras de serviços (managed services providers) que, apesar de serem concorrentes, partilham a experiência técnica. Essa é a mais-valia

que podemos dar uns aos outros. Os diferentes membros podem aprender com as boas-práticas implementadas noutras situações vividas por outros membros.

Com mais de 60 membros, contam com membros de vários sectores de actividade?
GS - Sim, temos na rede tudo aquilo que são sectores relevantes. Apenas não temos directamente a área dos transportes. Porém, temos membros da área da saúde, academia, desporto, reguladores, consultoras, operadoras, entre outras.

Como é que entidade pode juntar-se à rede?
GS – Qualquer entidade com uma equipa de resposta a incidentes e que cumpra com os requisitos de ser pessoa colectiva, ter uma comunidade para a qual garante que dá resposta a incidentes e fazer resposta a incidentes a um conjunto de incidentes tratados na nossa taxonomia. Todos os 61 membros têm como base essa taxonomia pois é importante falarmos todos a mesma língua. Além disso, a nossa taxonomia é a mesma promovida pela ENISA. Importa referir que os termos de referência e taxonomia são revistos anualmente de forma a serem actualizados.

PR – Os termos de referência são revistos anualmente. Porém, o princípio geral diz que é necessário ser recomendado por membros actuais para poder aderir à rede. Dessa forma existe uma responsabilização pela entrada de novos membros. Posteriormente, essa entrada está sujeita a uma votação pela Assembleia, tendo de existir maioria para que a entidade possa ser admitida.

Uma empresa que reúna tudo o que é necessário, mas não tenha recomendações de membros actuais não pode entrar?
GS – Uma empresa sem recomendações não consegue entrar na rede pois nem chega a votação. Todas as candidaturas são alvo de validação pelo secretariado e Comissão Executiva. Tem de existir essa garantia para termos a certeza que existe um membro que sabe que determinada entidade faz resposta a incidentes.
Com isso, conseguimos garantir que não tentam entrar membros com um objectivo comercial. Queremos que quem pertence à rede contribui com partilha técnica e leve alguma informação útil para o seu dia-a-dia.

PR – Gostaria de referir que não é possível termos como membros entidades que gerem os mesmos endereçamentos, domínios ou comunidade. Ou seja, ou a entidade tem a sua equipa própria ou subcontrata.

E no caso, por exemplo, de falarmos de uma multinacional que tem o SOC fora de Portugal e presta serviços a uma entidade portuguesa?
GS – Uma das coisas que obrigamos é a que a entidade tenha personalidade jurídica em Portugal. Podemos ter ao contrário, ou seja, multinacionais com uma equipa d resposta nacional que presta serviço a nível internacional a congéneres, algo que acontece muito no retalho e energia.

"HÁ UM OBJECTIVO DA REDE DE PARTICIPAREM EQUIPAS DE RESPOSTA A INCIDENTES DE ENTIDADES DE SECTORES COMPLETAMENTE DIFERENTES. COMECEI A INTEGRAR AS REUNIÕES EM 2011, NA ALTURA NA EDP, E O QUE MAIS VALORIZEI E CONSIDERO MAIS IMPORTANTE É A PARTILHA DE CONTACTOS, CONHECIMENTO, EXPERIÊNCIA E INFORMAÇÃO"

Pedro Rodrigues, Banco de Portugal e membro da Comissão Executiva da rede nacional CSIRT

Quando um dos membros sofre algum ataque há envolvimento da rede?
GS - Se houver necessidade de alguma entidade, esta pode contar com a rede para resolver e ajudar. Dependerá do tipo de incidente e capacidade de cada membro, sendo que há membros com uma maior capacidade de resposta do que outros. No caso do Wannacry, por exemplo, o CERT.PT actuou como ponto focal e todas as entidades da rede consultavam a nossa sala de situação virtual para verem o que estava a acontecer.

No fundo, quais as grandes vantagens de pertencer à rede?
GS – Um dos grandes objectivos de pertencer à rede é beber daquilo que podemos disponibilizar tecnicamente, a partilha de indicadores de comprometimento de campanhas ou actividade maliciosa em curso e a frequência em workshops que promovemos todos os anos. Além disso, permite ter um chat para partilha de informação ou pedidos de esclarecimento sobre o que está a acontecer no momento, ter uma lista de distribuição para receber alertas emitidos pelo CNCS ou o CERT.PT e receber as diferentes campanhas em curso, vindo de alguns parceiros europeus. Possibilitamos tudo isso aos membros que aderem.
A rede já tem representatividade no Conselho Superior de Segurança do Ciberespaço e contribui para a partilha de ideias para a nova estratégia nacional de cibersegurança. Além disso, já participamos em alguns fóruns de discussão para partilha de informação. •

MEMBROS DA REDE

RCTS CERT, NOS, NOWO, CIBERDEFESA - EMGFA, ALTICE, CLARANET, CIPHER, UNIVERSIDADE DO PORTO, ONICOMMUNICATIONS, IP TELECOM, MILLENIUM BCP, CEMAH, IGFEJ-IP, EDP, INESC, SGMAI-RNSI, CAIXA GERAL DE DEPÓSITOS, PT SERVIDOR, VODAFONE, LAYER 8, CERT.PT, NOVO BANCO, BANCO DE PORTUGAL, BANCO CTT, SIBS MULTICERT, DNS.PT, AXIANS, UNIVERSIDADE DO MINHO, UTAD, CYBERSAFE, S21SEC, OUTSYSTEMS, TRUPHONE, UNIVERSIDADE DA BEIRA INTERIOR, SANTANDER, EURONEXT, UNIVERSIDADE DE AVEIRO, SECURNET, UNIVERSIDADE DE ÉVORA, WARPCOM, EY, SLBENFICA, HARDSECURE, SPMS, FIDELIDADE, REN, SOANE, GALP, UNIVERSIDADE DO ALGARVE, INSITTUTO POLITÉCNICO DE BRAGANÇA, JERÓNIMO MARTINS, ÁGUAS DO DOURO E PAIVA, CAIXA AGRÍCOLA, ISCTE, ÁGUAS DO NORTE, ART RESILIA, AGEAS PORTUGAL, POLITÉCNICO DA GUARDA, LUZ SAÚDE, ORAMIX E AUTORIDADE TRIBUTÁRIA.

AMEAÇAS CIBERNÉTICAS: VAMOS DEFENDER A NOSSA NAÇÃO?

As ameaças cibernéticas são um perigo real e crescente para as sociedades. Nesta era digital, estamos todos interligados, e com isso, advém o risco de atores maliciosos utilizarem a Internet, para espalhar o medo e perturbar a ordem, gerando o caos nas sociedades modernas. Desde roubo de identidade a violações de dados, passando pela interrupção de serviços vitais para as comunidades, estas ameaças podem ter implicações de grande alcance para indivíduos, empresas e Governos.

Nos últimos anos, a ameaça da cibercriminalidade tornou-se proeminente. A comunidade cibercriminosa está a visar cada vez mais os setores público e privado, sem grande distinção, roubando informação sensível e perturbando as operações de forma altamente disruptiva. Além disso, na VisionWare, temos comprovado toda a complexidade e polivalência dos recentes ciberataques, que podem ser utilizados para espalhar informação e propaganda errónea, resultando em agitação social, caos e instabilidade política.

O que observamos é que ninguém está a salvo. Nem mesmo as infraestruturas críticas (energia, telecomunicações, sistemas de transporte, saúde, etc.) dos países ocidentais, já bastante debatidas e cuja segurança exalta preocupações crescentes, tanto para os governos como para os cidadãos.

À medida que a tecnologia avança, o mesmo acontece com a sofisticação dos atores cibernéticos maliciosos. Estes, para além de continuarem a explorar vulnerabilidades aplicacionais ou tecnológicas, apostam cada vez mais na interligação das fraquezas do fator humano – isto é, na engenharia social – com o intuito de tornar o ciberataque mais eficaz e de menor tempo de atuação, sempre com vista à obtenção de um acesso ilegítimo a identidades, e por aí em diante.

Para mitigar estas ameaças, governos e empresas privadas devem tomar medidas sérias e céleres para proteger as suas infraestruturas tecnológicas de suporte à atividade digital. Basta pensarmos na percentagem expressiva de infraestruturas críticas e/ou setores vitais, em Portugal, que estão nas mãos dos privados...

Os Estados europeus têm-se posicionado como moderadores, contudo, todos sabemos que os moderadores não ganham debates. A lógica é idêntica no âmbito da cibersegurança. É assim crucial, que governos e empresas trabalhem em conjunto, para partilhar informações e recursos, a fim de melhor detetar e responder de forma eficaz e preventiva a ameaças cibernéticas.

O ciberespaço não pode ser visto como antigamente; hoje, é um campo (e batalha) de interesses, mas, além disso, é também um campo de guerra. Por isso, é tempo de agir e proteger-nos a nós próprios – às nossas sociedades e costumes –, às nossas empresas e às nossas nações, dos perigos eminentes da cibercriminalidade e do ciberterrorismo. Temos de passar a assimilar que, com a evangelização da convivência no mundo cibernético, também as ameaças cibernéticas vieram para ficar.

Sobre a VisionWare: VisionWare - Vídeo Institucional | 2022 - Versão em Português - YouTube

BRUNO CASTRO,
FUNDADOR E CEO DA VISIONWARE SISTEMAS DE INFORMAÇÃO SA.

Licenciado em Engenharia Eletrotécnica desde 2000, pela Faculdade de Ciências e Tecnologia da Universidade de Coimbra, e Mestre em Engenharia Informática (Segurança Informática), pela mesma faculdade, no ano seguinte. Especialista nas temáticas da Segurança da Informação, Cibersegurança e Investigação Forense. Está credenciado NATO-SECRET e EU-SECRET, e faz parte do grupo de auditores de segurança credenciado pelo Gabinete Nacional de Segurança. É atual membro da European Society of Criminology.

visionware

Challenging an Unsafe World

LEALDADE | DISCRIÇÃO | DEDICAÇÃO

SOBRE

A nossa missão é contribuir para o Sucesso dos nossos clientes, aumentando a sua cultura e maturidade em Segurança da Informação.

SERVIÇOS

- CYBERSECURITY
- SOC & CSIRT
- FORENSIC INVESTIGATIONS
- PRIVACY & LEGAL
- ETHICS & CORPORATE COMPLIANCE
- STRATEGIC INTELLIGENCE
- PROFESSIONAL SERVICES
- TRAINING | VISIONWARE ACADEMY

SCAN ME

VISIONWARE.PT

visionwaresi

geral@visionware.pt

+351 225 323 740

PORTUGAL
Porto | Lisboa

CABO VERDE
Praia | Mindelo

"SEM A CAPACIDADE DE CIFRAR E DECIFRAR DADOS, NÃO HAVERIA COMUNICAÇÕES SEGURAS NA INTERNET"

Os mecanismos de cifra de dados utilizam algoritmos matemáticos para transformar informações legíveis numa forma ilegível e ininteligível, chamado "texto cifrado", em oposição ao "texto em claro". Estas operações são fundamentais para proteger a confidencialidade dos dados durante a comunicação ou armazenamento, permitindo a transmissão segura de dados pela Internet e garantindo a proteção de informações armazenadas em dispositivos eletrônicos.

Sem a capacidade de cifrar e decifrar dados, não haveria comunicações seguras na Internet, incluindo serviços bancários online, e-mails, compras, chamadas de voz e conversas em aplicações de mensagens instantâneas, como WhatsApp ou Signal. Além disso, não seria possível armazenar com segurança dados bancários, médicos, fiscais, segredos comerciais ou propriedade intelectual. A cifra de dados desempenha também um papel fundamental na preservação da liberdade de expressão, protegendo comunicações e permitindo a comunicação e a partilha de forma segura, sem medo de monitorização ou censura, o que pode significar a diferença entre a vida e a morte em países onde a liberdade de expressão e os direitos digitais não sejam um facto, onde estejam em risco ativistas de direitos humanos, comunidades marginalizadas ou perseguidas, e dissidentes políticos, entre outros.

Nos últimos anos, várias ações políticas surgiram com o objetivo de enfraquecer os mecanismos de cifra usados pelos cidadãos, não se limitando apenas a regimes não democráticos, mas também presentes nos EUA (com o EARN-IT), Reino Unido (com a Online Safety Bill) e União Europeia (com a proposta de Regulamento de combate ao abuso sexual infantil). Estas propostas de lei e regulamentação obrigarão as empresas fornecedoras de serviços online a enfraquecer os mecanismos de cifra usados, a fim de permitir o acesso aos dados dos cidadãos e a implementação de mecanismos de vigilância automáticos, afetando todos os cidadãos, não apenas aqueles que já são suspeitos de cometer ilegalidades.

É importante que os cidadãos entendam que a linha de raciocínio "não tenho nada a esconder, podem ver tudo o que faço" não é correta e falha por vários motivos. O direito à privacidade é fundamental para a autonomia, liberdade e dignidade humana. Mesmo que não tenhamos nada a esconder, não é correto sermos monitorados e escrutinados sem motivo. Também devemos considerar a ameaça de abuso de poder, já que permitir que governos ou empresas tenham acesso indiscriminado aos nossos dados pessoais pode levar à manipulação, discriminação, perseguição e repressão. Além disso, devemos estar cientes dos efeitos a longo prazo, pois as nossas opiniões, comportamentos e interesses podem mudar ao longo do tempo, e a exposição contínua das nossas atividades permitirá que outros formem um perfil detalhado de quem somos e possam utilizar esses dados contra nós no futuro.

Por fim, a cifra de dados é um garante da liberdade de expressão e pensamento. Se estivermos constantemente sob vigilância ou sob o ônus de enfrentar consequências por partilhar nossas opiniões, ideias divergentes não serão partilhadas, e não haverá debates abertos ou capacidade de expressar livremente opiniões. A ameaça ao jornalismo é também um dos pontos chave nesta discussão, uma vez que sem cifra de dados não há forma de proteger fontes nem de garantir investigações seguras.

A cerca de um ano das comemorações do 50º aniversário do 25 de Abril, é cada vez mais fundamental estarmos informados sobre questões de privacidade e segurança digital, compreendendo os riscos associados à vigilância e aos ataques à privacidade, de modo a não repetir na sociedade online os mesmos erros e ameaças que os portugueses sentiram durante o Estado Novo.

POR JORGE PINTO, CO-FUNDADOR E PRESIDENTE DA AP2SI

OPINIÃO

C-DAYS

CIBER SEGURANÇA | MAIS CONFIANÇA

14-16 JUN'23

CENTRO DE CONGRESSOS DA ALFÂNDEGA DO PORTO

MAIS CONFIANÇA

CNCS Centro Nacional de Cibersegurança PORTUGAL

U.PORTO

CHECK POINT · claranet · cybersafe · devoteam Cyber Trust · FORTINET · edp · CLAROTY · CROWDSTRIKE · okta · VECTRA · homeostase · Westcon · zscaler · LAYER8 · NOS · paldata · CLOUDFLARE · redShift · SECURNET · warpcom

MEDIA PARTNER: IT SECURITY · SECURITY MAGAZINE

JORGE PINTO

"AS AMEAÇAS NO CIBERESPAÇO ESTÃO EM CONSTANTE EVOLUÇÃO"

Numa entrevista à Security Magazine, Jorge Pinto, co-fundador e presidente da AP2SI, aborda a temática das ameaças iminentes no ciberespaço, bem como da falta de competências e sensibilização. "A falta de competências nas áreas ligadas à segurança da informação e cibersegurança é, também, um desafio persistente", diz.

Security Magazine - Fale-nos um pouco sobre as ameaças iminentes que espreitam no espaço cibernético. Como é que a superfície de ataque está a evoluir?

Jorge Pinto - As ameaças no ciberespaço estão em constante evolução, acompanhando também a evolução das tecnologias. A superfície de ataque tem se expandido devido ao aumento da conectividade e da digitalização e da presença online de organizações e indivíduos.

No campo tecnológico, alguns dos principais desafios são já bem conhecidos como ataques de malware e ransomware, ataques de engenharia social como phishing, acesso não autorizado a dados, e ataques de negação de serviço distribuído (DDoS). Outros desafios como as ameaças persistentes avançadas (APTs) estão a ganhar terreno à medida que os Estados e organizações criminosas melhoram e evoluem as suas capacidades de explorar o ciberespaço para os seus fins. Além disso, com a proliferação de dispositivos ligados à Internet das Coisas (IoT), continuam a surgir novas vulnerabilidades e pontos de entrada para ataques nos mais variados sectores, desde a indústria à saúde, passando pelas cidades inteligentes. Por final gostaríamos de destacar também o panorama social, em particular as temáticas ligadas à desinformação e iliteracia digital, que apresentam um enorme potencial para contribuir para o enfraquecimento das instituições democráticas e da sociedade através da veiculação de notícias falsas, informação descontextualizada ou incompleta e até campanhas executadas por actores estatais.

A espionagem empresarial está a aumentar, tal como a actividade de agentes patrocinados pelo Estado. Qual é o maior problema?

Ambos são bastante relevantes. A espionagem empresarial e a actividade de agentes patrocinados pelo Estado, bem como a criminalidade organizada, representam problemas de segurança que não podemos ignorar. As empresas e instituições do Estado sempre foram alvos preferenciais para o roubo de propriedade intelectual, segredos comerciais e informações sensíveis. A situação não mudou, mas agravou-se em grande medida devido à falta de percepção do risco aliada a investimentos desalinhados com as estratégias de negócio ou com as necessidades de protecção, num contexto de avanço tecnológico em que o tradicional perímetro de segurança se tem esbatido cada vez mais.

Além dos ganhos económicos, cobiçados em medida similar por organizações pouco éticas, criminosos ou Estados, é preciso lembrar que os agentes associados a Estados dispõem de acesso a recursos consideráveis e têm uma maior motivação para obter informações estratégicas visando, entre outros objetivos, a obtenção de vantagens geopolíticas e económicas.

Um grande problema na área da infosec é a falta de competências. A inclusão, nomeadamente através da diversidade de género, racial e neurodiversidade, é apontada como uma estratégia importante para colmatar esta questão, porém o problema mantém-se. Na sua opinião, quais as suas ideias para fazer frente a esta questão?

A falta de competências nas áreas ligadas à segurança da informação e cibersegurança é, também, um desafio persistente. A AP2SI trabalha com os seus parceiros para fazer frente a essa questão, executando ou promovendo iniciativas que visem atrair mais jovens para estas áreas, ou estejam focadas na requalificação.

São várias as estratégias que podemos seguir. Alguns exemplos são programas de formação financiados, bolsas de estudo, prémios de mérito, bem como actividades de mentoria. Acreditamos também que é necessário promover temas como a inclusão e diversidade, através do incentivo à participação de mulheres, minorias raciais e pessoas neurodiversas em áreas relacionadas com a cibersegurança. As empresas podem também apostar em fomentar ambientes mais inclusivos, em requalificar os seus profissionais e assegurar salários que permitam manter os profissionais e evitar a fuga para o estrangeiro. Além disso, é fundamental que as instituições de ensino adequem os seus programas de forma a capacitar os alunos nos temas da literacia digital, por forma a que entendam a importância destas temáticas na sua vida pessoal e na sua futura vida profissional.

Daquilo que é o seu conhecimento, quais são as tecnologias emergentes e tendências no domínio da segurança e que oportunidades e desafios são gerados pelas mesmas?

No domínio da cibersegurança, algumas das tecnologias emergentes estão ligadas aos avanços tecnológicos em áreas como a inteligência artificial e machine learning, a computação em nuvem, a criptografia avançada, os dispositivos da IoT. Qualquer uma destas áreas tem crescido bastante nos últimos anos e irá influenciar a forma como trabalhamos a segurança de sistemas e dados, bem como a protecção de dados pessoais.

Estes avanços trazem com eles excelentes oportunidades para quem trabalha em cibersegurança, por exemplo na melhoria dos mecanismos de detecção e resposta a ameaças, automatização de processos de segurança, fortalecimento dos mecanismos e tecnologias de criptografia, bem como no aumento da protecção de organizações e indivíduos. No entanto, como qualquer tecnologia, também trazem desafios como a rápida evolução das tácticas dos criminosos exigindo uma constante adaptação das estratégias e soluções de segurança, o aumento de complexidade e interconectividade dos sistemas de informação que obriga a uma maior atenção na sua gestão e implementação, não esquecendo também os temas relacionados com a conformidade com legislação e regulamentação que as organizações necessitam conhecer e acomodar nas suas operações. Por último, ainda no tema dos desafios, não podemos deixar de referir que, independentemente dos avanços, é necessário que as tecnologias respeitem a privacidade dos indivíduos e que não haja discriminação, viés ou abusos na sua aplicação.

Pode comentar-nos qual o estado actual da sensibilização de uma forma geral em matéria de cibersegurança e o estado de preparação para uma ciberameaça?

De uma forma geral, estamos mais bem preparados do que estávamos há 10 ou 20 anos atrás. Apesar de ainda haver um longo caminho a percorrer, a sensibilização em matérias relacionadas com a privacidade, a segurança da informação e a cibersegurança tem aumentado e vemos já resultados desse aumento.

No que diz respeito aos cidadãos, cada vez mais pessoas estão cientes dos riscos associados ao ciberespaço e à sociedade online, apesar de ainda existirem lacunas de conhecimento e prevalência de práticas inseguras. Entendemos que é necessário um esforço conjunto entre Estado e Sociedade Civil para alcançar aqueles que têm baixa literacia digital e dificuldade em compreender os riscos de uma sociedade cujo funcionamento está cada vez mais assente em sistemas de informação. Acreditamos que, quanto mais pessoas estiverem conscientes, mais o assunto será discutido e difundido, resultando numa maior adoção de boas práticas.

No que diz respeito a empresas e organizações, estas estão mais cientes dos riscos, principalmente devido à divulgação cada vez maior sobre ciberataques e crimes na internet pelos meios de comunicação. No entanto, ainda existem disparidades significativas na forma como lidam com esses riscos. Poucas integram a exposição aos riscos digitais na sua estratégia de negócio e operação, independentemente do tamanho da organização. Ainda são menos as que possuem um responsável ou uma equipe dedicados a 100% às funções de segurança da informação e cibersegurança. Algo que prevemos que mude brevemente por força da legislação e regulamentação.

A nível mundial temos assistido a uma proliferação de instituições e associações que têm trabalhado para que estas temáticas estejam, cada vez mais, embebidas na nossa sociedade.

Em Portugal, do lado do Estado não podíamos deixar de mencionar o trabalho levado a cabo pelo Centro Nacional de Cibersegurança (CNCS), a Polícia Judiciária (PJ) e a Procuradoria-Geral da República (PGR). Do lado da Sociedade Civil gostaríamos de destacar, além da AP2SI, o trabalho do ISACA Lisbon Chapter, da Women4Cyber Portugal e da Associação dos Profissionais de Proteção de Dados (APDPO), associações com as quais colaboramos regularmente.•

SANS INSTITUTE

The most trusted resource for information security training, cybersecurity certifications, and research.

O recurso mais fiável para formação em segurança da informação, certificações de cibersegurança e investigação.

O Mais Alto Padrão em Educação em Cibersegurança

Os nossos formadores são profissionais experientes que também se destacam na orientação de outros. São líderes respeitados na área da cibersegurança que partilham investigação, ferramentas e análises de incidentes com o mundo e trazem conhecimentos práticos e colaborativos à nossa comunidade.
Juntamente com os nossos alunos e colaboradores da comunidade, esses formadores dinâmicos fazem da SANS a organização educacional envolvente e de alta qualidade que é.

150+
extraordinary SANS-certified instructors

"Fiz vários cursos ao longo da minha carreira e muitos deles eram online. Nada, incluindo cursos caros de nível universitário, estava ao mesmo nível como a formação SANS. É densa, rica e imediatamente aplicável. Se o aluno levar o que aprendeu para o seu local de trabalho, irá distinguir-se imediatamente. Já estou ansioso pela minha próxima oportunidade de formação SANS, e recomendo-a vivamente"
-Dave Brock, Lytx Inc.

Vários Formatos de Formação

Encontre a opção que melhor se adapta ao seu horário, orçamento e estilo de aprendizagem preferido.

OnDemand
Treine em qualquer lugar e hora com quatro meses de acesso on-line. Receba formação dos mesmos formadores SANS de topo que ensinam nos nossos eventos de formação ao vivo - trazendo a verdadeira experiência SANS até si. Desfrute de acesso a laboratórios práticos repetíveis e suporte premium ao vivo de especialistas no assunto

Live Online
Evite deslocações e assista às sessões de transmissão interactiva em directo directamente do seu formador SANS, com muitas das actividades que os alunos SANS adoram nos eventos de formação presenciais.

In-Person
Experimente os cursos SANS ministrados por formadores de renome mundial em locais seleccionados, com laboratórios práticos para praticar as suas competências num ambiente focado e imersivo sem distracções, além de oportunidades para trabalhar em rede com outros profissionais de cibersegurança.

Private Courses
Forme-se com os seus colegas nas instalações da sua organização e discuta livremente questões e objectivos específicos do seu ambiente.

Summits
Participe em eventos especiais SANS de um ou dois dias com apresentações de especialistas que abrangem um único tópico de interesse para a comunidade de cibersegurança.

Ranges
Prepare-se para funções reais de TI e cibersegurança com cenários de aprendizagem interactivos que desenvolvem competências que podem ser aplicadas imediatamente no trabalho.

Se é novo na SANS ou não tem a certeza da área temática ou do nível de competências a seleccionar para o seu próximo curso de formação, a SANS oferece pré-visualizações gratuitas de cursos de uma hora através da nossa plataforma OnDemand.
Pré-visualize os nossos cursos em sans.org/demo

Tecnologia, Atacantes e Técnicas de Defesa Cibernética Mudam Rapidamente - por vezes em dias

Os nossos cursos, laboratórios, conteúdos e certificações oferecem as técnicas mais avançadas de ensino, laboratórios, conteúdo e certificações que são CONFIADOS por organizações em todo o mundo.

- PERITOS: Formados por peritos que passam por anos de formação e de ensino. Apenas os melhores dos melhores são convidados a ensinar.

- CONTEÚDO: A tecnologia, técnicas de ataque e capacidades de defesa estão a mudar rapidamente. O conteúdo dos cursos SANS é continuamente actualizado.

- HABILIDADES: Os laboratórios do mundo real são arquitectados, concebidos, preparados e testados - continuamente.

- VALIDAÇÃO DA FORMAÇÃO: As certificações GIAC acompanham o ritmo dos conteúdos e competências, garantindo aos empregadores que os seus funcionários podem actuar no mais recente ambiente de ameaças.

"A SANS é de confiança. A SANS cumpre o que promete. A SANS nunca aceita nada menos do que as melhores técnicas, capacidades e formadores em todo o mundo. É preciso muito para que a SANS mantenha o título de "Fonte Mais Fiável de Formação, Certificação e Investigação em Cibersegurança e Pesquisa" em todo o mundo. Não vamos mentir. É difícil. Nós cumprimos essa promessa. Sabemos que que a sua organização depende disso e levamos o nosso trabalho a sério. E adoramos saber que o que fazemos é importante".
-Rob Lee, Director de Currículo da SANS

The SANS Promise

You will be able to use the skills you've learned in our training and programs immediately in your work.

Poderá utilizar as competências que aprendeu na nossa formação e programas imediatamente no seu trabalho.

137,000+
GIAC Certifications Issued
Certificações GIAC emitidas

30+
Countries Featuring SANS Training Events
Países que apresentam eventos de formação SANS

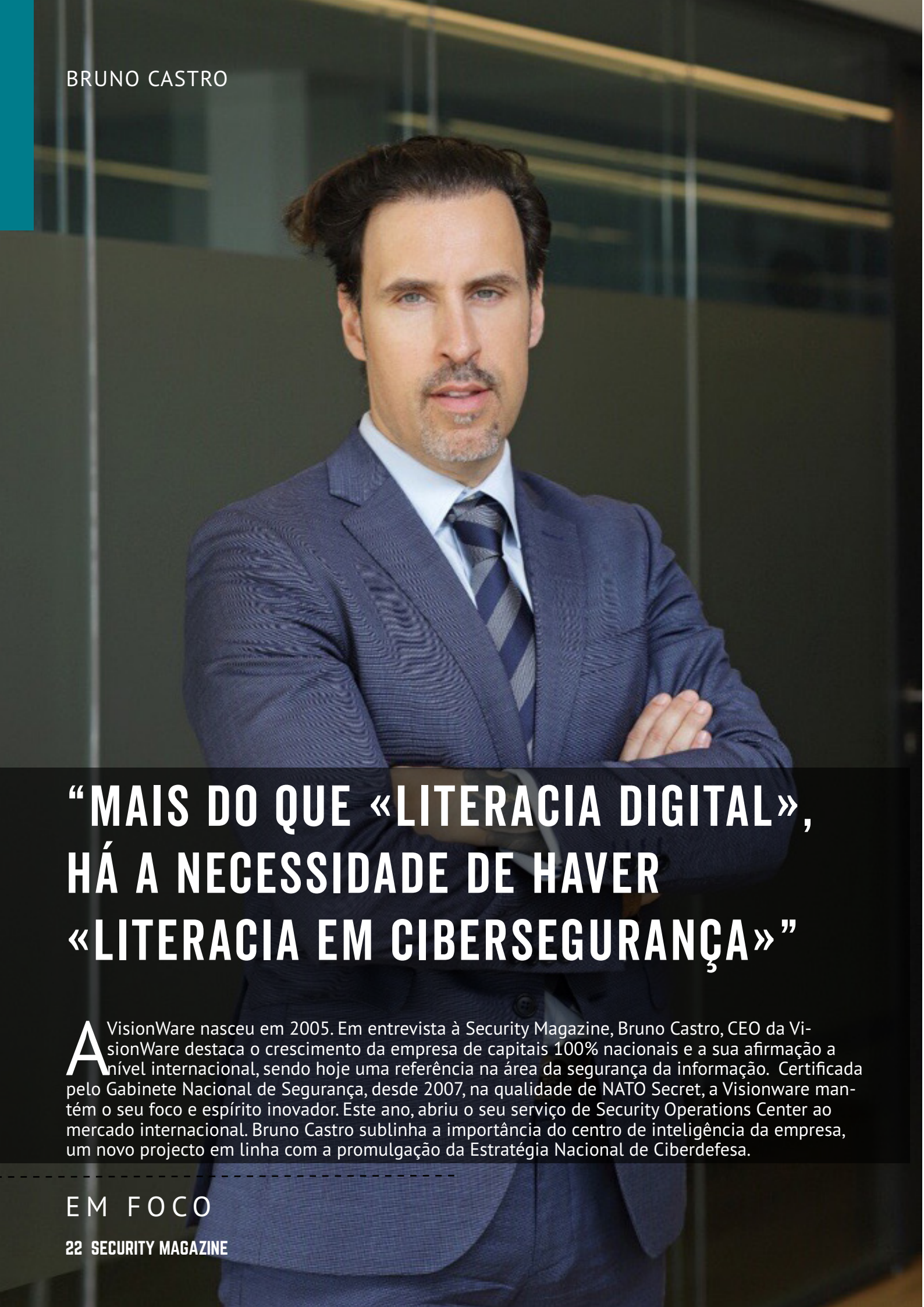
40,000+
SANS Students Per Year
Estudantes SANS por ano

85+
Cybersecurity Courses
Cursos de cibersegurança

40+
GIAC Certifications
Certificações GIAC

150+
Certified Instructors
Formadores Certificados

BRUNO CASTRO



“MAIS DO QUE «LITERACIA DIGITAL», HÁ A NECESSIDADE DE HAVER «LITERACIA EM CIBERSEGURANÇA»”

A VisionWare nasceu em 2005. Em entrevista à Security Magazine, Bruno Castro, CEO da VisionWare destaca o crescimento da empresa de capitais 100% nacionais e a sua afirmação a nível internacional, sendo hoje uma referência na área da segurança da informação. Certificada pelo Gabinete Nacional de Segurança, desde 2007, na qualidade de NATO Secret, a Visionware mantém o seu foco e espírito inovador. Este ano, abriu o seu serviço de Security Operations Center ao mercado internacional. Bruno Castro sublinha a importância do centro de inteligência da empresa, um novo projecto em linha com a promulgação da Estratégia Nacional de Ciberdefesa.

Security Magazine - A VisionWare nasceu em 2005, numa altura em que ainda não se falava muito da temática da cibersegurança. O que motivou a criação desta empresa e como foram esses primeiros anos?

Bruno Castro - A VisionWare foi idealizada no sentido de tornar-se um projecto empresarial orientado exclusivamente à cibersegurança. Assim, acaba por ser idealizada e criada em 2005, no meio de um cenário de crise iminente, onde tudo indicaria que não seria o melhor momento para aventuras empresariais. Contudo, e essencialmente, devido à coragem dos seus fundadores, à adopção de uma estratégia de especialização numa única área de actuação – cibersegurança -, ou seja, sermos verdadeiros especialistas, e por fim, com alguma dose de loucura à mistura, adoptamos o nosso playground ao mercado internacional. Foi assim que, quase 18 anos depois, se assume como uma empresa de capital 100% português, referência internacional na área da segurança de informação e com um espírito irrequieto de constante inovação face aos novos desafios que esta área está constantemente a exigir.
Importa reforçar que, desde o seu início, a VisionWare trabalhou para ser reconhecida pela comunidade internacional e pelo sector de Segurança da Informação, obtendo 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. A estratégia e objectivo sempre foram claros para nós.
Em 2006 expandimos os escritórios para Lisboa e partir daí nunca mais parámos. A crescente importância e tendência da cibersegurança em todo o mundo mostrou que a VisionWare estava no caminho certo. Em 2007, vencemos o primeiro projecto internacional, em Cabo Verde, lançando a nossa presença nos Países Africanos de Língua Oficial Portuguesa, a qual se mantém sólida até hoje.
Desde a sua génese, foi evidente que para promover a maturidade na segurança da informação, esta deveria ser abordada de forma holística. Neste sentido, a partir de 2016, e depois de uma década de experiência acumulada, a garantir que as nossas áreas centrais, e de origem, estavam devidamente consolidadas - cibersegurança, compliance e investigação forense -, a VisionWare avançou para o desenvolvimento e implementação de áreas independentes e complementares como a privacidade, inteligência e criação de uma área de academia para aliar uma componente crítica e emergente de formação num tema no qual ainda hoje existe falta de literacia. Com o aumento da cibercriminalidade e incremento na procura de apoio na mitigação e recuperação a ciberataques, por parte de todo o mercado, a VisionWare assistiu a um crescimento bastante considerável, facto que obrigou a uma aposta na área de recrutamento face à necessidade de responder rapidamente às solicitações do mercado e, assente na dinâmica de inovação, e criação de novas unidades de negócio orientadas para vertentes alternativas do mundo da segurança.

O que vos distingue no mercado?

Se tivesse de evidenciar as principais características que nos distinguem no mercado, apontaria as seguintes: especialização e conhecimento na área da segurança, experiência comprovada em lidar com situações de crise ou desastre, e a nossa inquietude na inovação de novos conceitos ou conhecimentos e na audácia de "atirarmo-nos" para o mercado, também sem fronteiras, tal como o próprio mundo cibernético. Actualmente, a VisionWare está presente em diferentes geografias, tendo alcançado dimensão mundial através dos inúmeros projectos internacionais. Tem conquistado a confiança dos clientes nacionais e internacionais e o reconhecimento da comunidade e das principais entidades reguladoras do sector.

A VisionWare apostou em Cabo Verde. Como decorreu o processo de internacionalização e como avalia esta aposta?

A VisionWare está presente em Cabo Verde desde 2007, data do primeiro projecto neste país, onde detemos uma presença contínua e cada vez mais sólida – no sentido de evoluir o nível de maturidade de segurança em Cabo Verde, - essa tem sido a principal motivação com a nossa presença neste país. Na realidade, e após mais 15 anos, já somos todos também um pouco "cabo-verdianos". Existe uma relação de amizade profunda com Cabo Verde, que em primeira instância, pela "morabeza" com que sempre fomos recebidos, mas também pelo que temos vindo a colaborar e aprender com este país. A VisionWare, apesar de operar em quase todos os continentes, não tem mais nenhuma geografia com este tipo de relação. É um caso único. A VisionWare avaliou o nível de segurança de mais de 30 organizações em Cabo Verde nos últimos 15 anos, tendo passado, muito provavelmente, pela maioria dos sectores empresariais. Actualmente, soma mais de 20 clientes, em formato de colaboração continuada. Alguns deles colaboram em estreita relação de parceria connosco há mais de 10 anos, desde o Estado passando à banca, seguradoras, comunicações, área farmacêutica ou energia. Trabalhamos numa área muito na curva da onda e somos obrigados a estar constantemente a evoluir. Nos últimos dois anos, nomeadamente após este número enorme de ciberataques, criámos uma equipa de inteligência que está constantemente a monitorizar, quer o submundo da internet, quer alguns grupos cibercriminosos com especial apetência para os sectores de actividade dos nossos clientes.
Contamos com mais de 20 colaboradores na cidade da Praia, estando em conclusão uma nova vaga de recrutamento para mais 10 a 15 novos colaboradores para os escritórios na capital do país, para responder ao crescimento do negócio. Estamos a reforçar a equipa da Praia, com previsão de começar a abertura do escritório em São Vicente, e com um novo processo de recrutamento só para esta localização. Na Praia, temos tido uma boa adesão, até pela boa parceria que temos com o Governo de Cabo Verde através de uma colaboração muito estreita e activa com a sua Secretaria de Economia Digital e o NOSi [Núcleo Operacional da Sociedade de Informação], com possibilidade de recrutar mais pessoas e talentos cabo-verdianos formados pelo próprio NOSi, sendo isso uma grande mais-valia para o acelerar da resposta às necessidades de crescimento da VisionWare no panorama internacional.
Cabo Verde tem evoluído imenso nestes 15 anos em termos de segurança e a sua capacidade de resistir até à recuperação

ao desastre. Prova disso foi o que aconteceu com a rede do Estado em que o NOSI, juntamente com os outros parceiros, connosco incluídos, recuperou de um ataque tão devastador há dois anos. Os próximos desafios passarão por manter esse nível de crescimento e consolidação do sector no país.

Qual a mais-valia de a VisionWare ser credenciada pela NATO? O que isso significa em termos práticos?

A VisionWare é certificada pelo Gabinete Nacional de Segurança (GNS), desde 2007, e credenciada na qualidade de NATO SECRET, o que nos permite obter um grau de notoriedade e reconhecimento com o selo e chancela de elevada qualidade de uma instituição tão prestigiada quanto a NATO. É algo único e exclusivo. Consolidou-nos ainda mais como referência internacional em matéria de segurança da informação. É comum participarmos em projectos via NATO, um asset de valor inestimável para a VisionWare. Por exemplo, através de consórcios internacionais onde esta certificação e referência tornam a VisionWare um parceiro de relevo para abordagens a projecto de cariz internacional. Em Portugal, acaba por ser também actualmente um dos factores que nos diferencia, distingue e posiciona na linha da frente face à nossa concorrência.

Obter a credenciação junto do GNS constituiu um passo gigante e muito inovador para a altura (isto ainda, no ano 2007), por duas grandes razões. Em primeiro lugar, pelo que fazíamos a nível individual, já que éramos considerados peritos especializados em cibersegurança e investigação forense operando regularmente junto das autoridades, nessa altura. Em segundo, pelo facto de termos obtido a credenciação via NATO, algo que transformou a VisionWare num caso único em Portugal, ao nível de empresas a actuar no sector da cibersegurança com este tipo de credenciação.

Também no âmbito da sua unidade de formação, a VisionWare Academy, nas disciplinas associadas à sua área de competência, é ainda certificada pela DGERT como entidade reconhecida para a formação certificada. É também conhecida pelo seu know-how nas áreas de Strategic Intelligence e no decorrer dos últimos anos, a VisionWare estabeleceu igualmente um posicionamento contínuo junto dos grupos privados da indústria que prestam assessoria junto da Comissão Europeia, no âmbito de projectos R&D, em matéria de segurança informática.

A cibersegurança tem sido colocada como uma prioridade para muitas empresas. No entanto, a sofisticação dos ataques foi ampliada e os grupos de cibercrime organizado continuam a lucrar. É possível salientar algumas das actividades cibercriminosas tradicionalmente organizadas e os seus impactos de longo prazo?

Nestes últimos quase 20 anos de VisionWare, nunca tivemos tantas solicitações de ajuda para responder e investigar a situações, muitas vezes de desastre, oriundos de ciberataques bem-sucedidos, como agora. Estes ciberataques, desenvolvidos em vários formatos, e cada vez mais complexos, sofisticados e com elevado grau de sucesso, estão tipicamente focados no roubo de dinheiro ou dados "valiosos", resultando de múltiplos factores associados.

Por um lado, o cenário pandémico veio colocar mais pessoas, muitas sem formação, a viver no mundo cibernauta. Por outro, o ambiente de teletrabalho promoveu um certo descuido face às medidas de segurança, o que faz com que, todos, mesmo os mais formados, estejam "menos alerta" para eventuais ameaças ou comportamentos suspeitos.

Os níveis de maturidade de segurança variam de organização para organização, mas o factor humano é normalmente a maior fragilidade. As pessoas precisam ser formadas para responderem a esta nova realidade e poderem novamente conviver com o mundo cibernauta, com tudo o que acarreta, de forma ponderada e responsável. Mais do que "literacia digital", há a necessidade de haver "literacia em cibersegurança".

É fundamental avaliar o risco da organização, levantar necessidades e determinar prioridades que poderão passar pela escolha de outra tecnologia que não a que está a ser utilizada ou pela implementação de processos novos, mais rígidos e, ao mesmo tempo, mais alinhados com a sua realidade. Além disso, é preciso treinar a organização, dando formação aos colaboradores e auditando-a regularmente, stressando-a, para que esteja preparada para responder às ameaças cibernéticas, quando estas chegarem, porque mais tarde ou mais cedo vão chegar. Após uma cobertura mediática e crescente awareness a este tema, acabam por ser visíveis alguns resultados e mudanças urgentes de mentalidade, ainda que, insuficientes. Na VisionWare, temos registado um número avultado de solicitações de empresas, as quais começam a preocupar-se com a questão da segurança da informação e da cibersegurança, colocando-as no topo das suas prioridades de gestão. Finalmente, o chip e o mindset dos administradores das empresas, que detêm o poder de decisão, está a mudar, pelo que as autoridades competentes terão, de facto, um gigantesco desafio pela frente, dada a rápida adaptação a uma nova realidade de cibercrimes.

Importa salientar que, além da quebra ou total perda de actividade decorrente dos negócios após um incidente, existem os elevados danos reputacionais da marca/entidade em causa, para além de, dependendo do grau de seriedade do ataque à organização, o mesmo incidente por vezes levar até à falência de muitas empresas, em particular, as PME's.

O ser humano é apontado frequentemente como o elo mais fraco no que toca à cibersegurança. Como é que os empregadores podem elevar a fasquia para evitar a exploração do comportamento ou psicologia humana? Como podemos ter uma abordagem mais integrada no que à segurança diz respeito? Considera que as empresas deveriam avaliar o desempenho e consciência dos seus funcionários em matéria de segurança?

A actividade diária da VisionWare em acções de investigação forense tem vindo a demonstrar que o factor 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. A expressão "conhecimento é poder" tem vindo a ganhar força, e quanto mais informados os utilizadores estiverem sobre os riscos que advêm do abuso das suas credenciais, e da possibilidade iminente da usurpação da sua identidade, mais conscientes estarão sobre a importância de mantê-las seguras. O ser humano é o elemento mais frágil de um sistema de segurança e as estatísticas demonstram que a maioria dos ataques acontecem por intermédio dos seus funcionários. Sendo assim, é crucial investir em programas de treino dos utilizadores, sendo esta uma das estratégias mais compensadoras que as organizações podem levar a cabo.
Recomendo vivamente as seguintes estratégias a ser adoptadas, de modo a "educar" e disciplinar os utilizadores a manter as suas credenciais seguras:
- Consciencialização em matéria de Segurança: devem ser promovidos regularmente, programas de consciencialização em segurança cibernética, através de palestras, workshops, newsletters informativas ou materiais educativos, com a finalidade de alertar aos utilizadores sobre o uso indevido ou comprometimento das suas credenciais;
-Exemplo de histórias e casos reais: partilhar exemplos de acontecimentos reais de casos em que as credenciais foram comprometidas e do desfecho negativo desses casos, auxilia no processo de maior consciencialização dos utilizadores;
-Políticas de segurança claras: as políticas de segurança da informação devem ser claras e comunicadas de forma transparente aos funcionários;
- Acções de treino sobre tecnologias de autenticação: incentivar o uso de medidas de autenticação mais seguras, tais como, a autenticação multifactorial, uso de passphrases em vez de passwords ou uso de sistemas gestores de passwords. Explicar aos utilizadores os benefícios dessas tecnologias e instruí-los sobre como usar correctamente essas mesmas funcionalidades;
- Disponibilizar suporte e orientação: fornecer sempre que necessário, suporte e orientação aos utilizadores em relação à segurança das suas credenciais.
É essencial educar continuamente a organização e disponibilizar um espaço para o esclarecimento de dúvidas, promovendo discussões abertas sobre o tema, de forma a garantir que os colaboradores estejam actualizados e cientes das melhores práticas para manter as suas credenciais seguras.
A (correcta) gestão individual das credenciais será sempre o primeiro passo para a boa gestão de acessos e privilégios.

Na sua perspectiva, qual o estado geral de sensibilização para a cibersegurança e o estado de preparação para uma ciberameaça ao nível das nossas organizações?

Não existem fórmulas mágicas ou uma vacina milagrosa contra ciberataques. É um mito urbano que me parece já estar fora de moda. A chave do sucesso será, sempre, a prevenção, e, cada vez mais, a capacidade de resposta após um ciberataque com sucesso. Não me canso de reforçar este ponto. Prevenção e investir em modelos de segurança contínuos, conhecer bem as infra-estruturas, e sobretudo, "stressar" constantemente os sistemas, procurando falhas e fragilidades, corrigindo-as de forma perseverante, de modo a minimizar a possibilidade de a organização vir a sofrer contra quaisquer tentativas de ciberataques. Acrescento algo que tem vindo a ser muito relevante, e prende-se com o facto de conhecer a nossa real capacidade de recuperação a um ciberataque que virá ser cada vez mais fundamental para a gestão de uma organização nos dias de hoje.
Temos assistido semanalmente – se não, diariamente - a uma intensificação e sofisticação de ciberataques na sociedade portuguesa. Estes ataques, transversais a quase todos os principais sectores da nossa sociedade – telecomunicações, saúde, banca, transportes, educação -, têm causado muita turbulência, visto que, em certos casos, também tem implicado um impacto directo para o core business das 'vítimas', e por inerência, ao próprio sector onde actuam.
O crime cibernético tem sido aquele que mais tem aumentado desde o início da pandemia, tanto ao nível do volume de ataques registados como de denúncias, reforçando que estas situações continuam sem conseguirem ser travadas pelas entidades competentes e, nelas, estão incluídas não só as autoridades que investigam este tipo de ataques, como as próprias empresas que continuam a não dar o devido valor ou investimento a esta área de actuação.
Face ao incremento quase explosivo do número de ciberataques, nomeadamente com sucesso, infelizmente, as autoridades não dispõem de recursos necessários para responder a todas as solicitações.
Além de mais ataques, e com maior taxa de sucesso, são cada vez mais complexos e sofisticados, e, portanto, obrigam a um esforço muito superior no processo da sua e investigação.
Seguir o rasto da pegada digital deste tipo de grupos criminosos, que actuam de forma encoberta, prolongada no tempo, e tecnicamente aprimorada, é cada vez mais exigente – tecnologicamente, na capacidade de resposta e conhecimento especializado envolvido - para quem tenta investigar e prevenir este tipo de ciberataques.

As autoridades competentes estão perante um enorme desafio, que, além da capacidade de resposta, ainda se prende com o binómio técnico vs know-how especializado. Eventualmente, poderemos associar grupos cibercriminosos especializados por sector de actividade, como a saúde, indústria, ou a administração pública, onde a sua actuação é cada vez mais personalizada ao sector e com uma maior probabilidade de sucesso e eficácia. A aposta terá de ser sempre pela via da crescente literacia de todos os cidadãos, independentemente da sua função/cargo, visto que, qualquer um de nós poderá ser vítima de um ataque malicioso ou fraudulento. O factor humano continua a ser um dos grandes responsáveis pela consumação das ameaças e estas tanto podem vir de fora, como dentro da própria organização.

O Estado e a Administração Pública e demais organismos e entidades estatais deverão ser os primeiros a preconizar e implementar medidas de segurança diárias e fazer respeitar as demais normas e directivas nacionais e internacionais, com vista ao cumprimento de uma maior segurança cibernética.

A cibersegurança constitui um dos componentes indispensáveis face à conformidade com a lei da protecção e privacidade de dados. As duas caminham lado a lado e em consonância harmoniosa como garantia da conformidade e compliance com os demais processos associados, por exemplo, ao respeito pelo cumprimento do RGPD, quer por empresas privadas, quer, muito assim se espera, pelo sector público, enquanto modelo de conduta.

A meu ver, e no que diz respeito a estas matérias, o PRR - Plano de Recuperação e Resiliência português - confere à Administração Pública uma oportunidade única de transformação digital e de crescente capacitação a este nível, pelo que, há que saber aproveitar, para que possamos tirar o máximo partido do potencial associado à economia dos dados. Deve ser instituído (e monitorizado) um processo para testar, apreciar e avaliar de forma periódica, a eficácia real das medidas técnicas e organizativas, de modo a garantir a segurança do tratamento. Deverá ainda ser acautelado um plano de contingência em caso de violação de segurança que defina as medidas de eliminação/mitigação de riscos, procedimentos a adoptar, comunicação à CNPD e informação aos demais titulares dos dados.

Como é que a VisionWare se está a preparar para os novos desafios que emergem e crescem no mercado em matéria de cibersegurança, nomeadamente IA, machine learning, novas formas de trabalho, digitalização, actividades de agentes patrocinados por Estados... ?

A Inteligência Artificial (IA) é um dos campos de desenvolvimento tecnológico mais importantes da actualidade. Como muitos referem, pode ser aplicada para melhorar a qualidade de vida de todos os seres humanos, em vários aspectos. Por meio de computadores, robôs, dispositivos móveis e outros meios tecnológicos, pode ser usada para ajudar a resolver problemas humanos e aumentar a produtividade, tornando o mundo mais conectado. Além disso, e mesmo sendo este um dos campos mais controversos, a pode ser utilizada para ajudar na redução da criminalidade, aumentando a segurança pública. Será uma aliada na melhoria da educação, saúde e assistência social, bem como útil na melhoria dos sistemas de transporte, tornando-os mais seguros e eficientes.

Contudo, face ao desenvolvimento actual que temos assistido da IA, esta levanta-nos sérios dilemas. Não só éticos e morais, mas também securitários. Veja-se que, recentemente, mais de 1000 especialistas ligados à IA e empresários de renome das tecnologias - incluindo Elon Musk -, mas não só -, assinaram uma carta que pede "uma pausa de seis meses no desenvolvimento de sistemas gigantes de IA". Os signatários argumentam que é necessária esta pausa para que "os potenciais riscos à segurança sejam estudados e controlados". Isto levanta-nos várias questões tais como: que problemas poderemos encontrar, que ameaçam a segurança das nossas comunidades, à medida que desenvolvemos a IA para o benefício da sociedade? O tema é muito amplo e complexo.

> O QUE ESTÁ HOJE EM JOGO É A NOSSA SEGURANÇA ENQUANTO INDIVÍDUOS, AS NOSSAS EMPRESAS E INSTITUIÇÕES, E, NÃO MENOS IMPORTANTE, OS VALORES DEMOCRÁTICOS.

Um relatório recente da Europol fez um alerta sobre os riscos representados por estas "novas tecnologias". Ora, de acordo com este estudo, as redes de telecomunicações de quinta geração (5G), a criptografia quântica e a IA, se forem parar "às mãos erradas", podem dificultar bastante o trabalho de investigação dos agentes das forças de segurança. Não basta ser reactivo para enfrentar tão grande evolução na tecnologia e na criminalidade. Para continuar relevante, a polícia precisa prever quais, entre as tecnologias emergentes, serão as efectivas armas de escolha dos cibercriminosos. **O 5G será um grande desafio para os investigadores porque dificultará a identificação de aparelhos móveis usados em crimes**, já que a configuração das redes 5G significa que a informação será fragmentada, tornando o acesso aos dados, um processo muito mais complexo. Por sua vez, a IA pode ser descrita como uma "faca de dois gumes", ou seja, ela torna as aplicações mais inteligentes entre si através de recursos como a aprendizagem de máquina, mas por esse mesmo motivo, serve para personalizar e automatizar sistemas automatizados de ciberataques, como aqueles que distribuem vírus e phishing. A criptografia quântica vai pelo mesmo caminho — isto é, criada para codificar fortemente as redes e evitar invasões, pode, nas mãos de criminosos digitais, quebrar qualquer tipo de segurança e facilitar ciberataques mais sofisticados. Na IoT, continuam igualmente a surgir vulnerabilidades de projecto, as quais necessitam de uma resolução antes da sua utilização. Abordando o caso mais paradigmático: o "novo" chatbot da Open-AI - o ChatGPT -, foquemo-nos apenas na dimensão

que a VisionWare opera: a cibersegurança. A emergência da tecnologia da IA foi sempre recebida com um certo cepticismo e incerteza, e não é difícil perceber porquê. Quando apresentada com uma forma de tecnologia tão avançada que pode fazer o seu próprio pensamento, temos de dar um passo atrás necessário mergulhando directamente para dentro.
Embora tornando as nossas vidas muito mais fáceis e ágeis em muitos aspectos, a tecnologia da IA que possuímos hoje e continuamos a melhorar pode ter consequências terríveis para o futuro da cibersegurança - daí a existência do malware ChatGPT. Falo sobre os riscos da utilização do ChatGPT e que um programa melhorado como este pode ser perigoso nas mãos erradas. O programa de IA pode escrever código instantaneamente e de acordo com dados recentes, o ChatGPT também pode elaborar um programa malicioso bastante convincente. O malware é basicamente código malicioso.
Muitas redes subterrâneas na darkweb já levaram à utilização do chatbot para eliminar malware e facilitar ataques de ransomware. Estas preocupações são ainda mais prementes, quando os gigantes da indústria estão dispostos a investir fortemente em tecnologia de IA.
Parece-me evidente que **vivemos tempos muito desafiantes no campo da (inovação da) segurança cibernética, quando a nossa aliada IA acaba por se revelar a principal inimiga de quem nos protege**.
Na VisionWare acreditamos que **é crucial investir na implementação de um modelo de segurança que seja evolutivo, dinâmico e contínuo**, abordando todos os sectores da segurança, nomeadamente, tecnologia, procedimentos e pessoas.
É vital que as organizações conheçam em detalhe o seu nível de risco, e quais as suas fraquezas, para que possam investir correctamente, e caso não seja possível, saibam precisamente onde residem as suas fragilidades, de modo a promover acções imediatas de mitigação. A aposta em acções de sensibilização e formação das pessoas, para que estas estejam conscientes e não se transformem elas próprias em veículos de ameaça face a este novo paradigma de risco cibernético é por isso, urgente.

Quais as grandes novidades e investimentos traçados pela VisionWare para 2023?

A VisionWare continua em franco crescimento, até pela própria conjuntura do mercado, actuando em diversos sectores da segurança, e, portanto, o desenvolvimento de estruturas de sustentabilidade do nosso crescimento aliando sempre a necessidade de investimento na inquietude que a inovação obriga, será esse, o nosso principal objectivo para os próximos dois anos. Isto é, manter o nível de crescimento da VisionWare, apostando no desenvolvimento contínuo de serviços inovadores na disciplina de segurança, de acordo com as exigências do sector, garantindo, em simultâneo, a sustentabilidade financeira da empresa.
Este ano, e pelo que tem vindo a ocorrer mundialmente, a VisionWare abriu (sem restrições) o seu serviço de Security Operation Center (SOC) ao mercado internacional. Este serviço tem como objectivo implementar uma "guarda inteligente", com total abrangência, em modelo permanente (24/7) à totalidade da infra-estrutura digital da organização.

A (CORRECTA) GESTÃO INDIVIDUAL DAS CREDENCIAIS SERÁ SEMPRE O PRIMEIRO PASSO PARA A BOA GESTÃO DE ACESSOS E PRIVILÉGIOS.

O VisionWare Threat Intelligence Center, surge como um novo projecto em linha com a promulgação da Estratégia Nacional de Ciberdefesa, anunciado pelo Governo português, e conta com especialistas das áreas de intelligence e cibersegurança, que efectuam a monitorização, análise e report urgente, em tempo real, para responder aos novos desafios e ciberameaças à segurança das instituições públicas e privadas.
O objectivo desta nova solução passa por estudar, reportar e alertar as instituições públicas e privadas, dos perigos da cibercriminalidade, desinformação, misinformation e deepfake, de forma a compreender as mais diversas origens das ciberameaças à segurança das empresas e organizações e combatê-las.
Para mim, o que está hoje em jogo é a nossa segurança enquanto indivíduos, as nossas empresas e instituições, e, não menos importante, os valores democráticos. O nosso novo Centro de Inteligência surge em consonância plena com o apelo do Governo, para provocar uma maior atenção da sociedade civil face ao perigo iminente das novas ameaças e riscos globais. Este Centro produzirá relatórios geopolíticos relacionados com as ameaças em estudo, monitorização de actores de risco, notificações em tempo real, sempre que dados de as instituições ficarem comprometidos, e ainda, a produção de relatórios de análise e estudo perante as principais ameaças e actores, divididos por tempo e sector de risco.
Como próximo passo, torna-se fundamental capacitar as autoridades de ferramentas (e conhecimento) para o constante controlo e monitorização da deepweb/darkweb (identificação de leaks), análise de riscos de cibersegurança das infra-estruturas críticas, profiling de determinados indivíduos através de técnicas de humint, detecção e defesa de ciberataques e a monitorização e supervisão contínua de determinados grupos cibercriminosos.
Através do incremento contínuo do volume de negócio internacional, conseguimos formalizar uma operação fixa em África – através de Cabo Verde – e na Europa – junto da Comissão Europeia, em projectos essencialmente de R&D, na vertente de segurança e privacidade. Além disso, e até pela exigência e dinâmicas do sector onde nos posicionamos, procuramos ser uma empresa que procura persistentemente as melhores soluções (tecnológicas ou não) para os clientes, respondendo às suas necessidades, mas principalmente, antecipando as tendências de mercado.
Em termos de futuro, queremos crescer mais, ser a principal referência no sector da segurança de informação, e operar worldwide, com abordagens e soluções sempre à frente do mercado e da concorrência, continuando precisamente com a mesma inquietude que tínhamos na nossa génese, em 2005•

PEDRO CÂNDIDO

"A INOVAÇÃO É UM DOS PILARES DO CRESCIMENTO DA SALTO"

A SALTO Systems é um importante player no mercado na área de controlo de acessos. Presente no mercado português desde 2005, a empresa detém escritórios em Lisboa e Porto. À Security Magazine, Pedro Cândido, Partner Channel Development Manager da SALTO Systems Portugal , destaca que "2023 será uma no promissor com oportunidades para consolidar a nossa posição no mercado". O responsável acredita que o futuro do controlo de acessos será marcado por soluções em cloud, autenticação facial, IoT, Inteligência Artificial e soluções moveis.

Security Magazine – Como e quando surgiu a SALTO no mercado português e qual a estrutura que dispõe no país em termos de instalações e RH?

Pedro Cândido – A SALTO Systems iniciou a actividade em Portugal em 2005, estabelecendo-se como SALTO Systems Portugal. Actualmente, a empresa conta com uma estrutura consolidada no país, com escritórios em Lisboa e no Porto e uma equipa de profissionais altamente qualificados que prestam suporte técnico, comercial, marketing e atendimento ao cliente.

Como avalia a evolução da empresa em Portugal em termos de crescimento e como encara o ano de 2023?

A evolução da SALTO Systems em Portugal tem sido muito positiva, com um crescimento contínuo e sustentável ao longo dos anos. Acreditamos que 2023 será um ano promissor, com oportunidades para consolidar a nossa posição no mercado de controlo de acessos e expandir a nossa presença em novos sectores e verticais.

Qual o peso que o mercado português representa na SALTO em termos globais?

Portugal é um mercado estratégico para a SALTO Systems, representando uma fatia importante do nosso negócio global. A empresa tem investindo continuamente no país, tanto em recursos humanos quanto em infra-estrutura, para atender às necessidades específicas dos clientes portugueses.

Observando os verticais, no segmento por exemplo do hospitality e dos espaços de co-working, é possível dar-nos alguns exemplos de case studies que considere relevantes em Portugal?

A SALTO Systems tem trabalhado em diversos projectos e verticais relevantes em Portugal. Devido à nossa ampla gama de soluções de hardware e software, assim como à grande capacidade de adaptação e compatibilidade universal, podemos enquadrar-nos em praticamente qualquer tipo de projecto, independentemente do sector e condições que apresenta. Nos últimos anos temos desenvolvido importantes projectos na área de hospitality, espaços de coworking, universidades, hospitais, bem como na indústria.

Como é que a SALTO tem assistido e respondido a esta passagem e procura de soluções físicas e convencionais para digitais ao nível do controlo de acessos? Exigiu alguma adaptação do vosso posicionamento?

A SALTO Systems tem acompanhado a evolução do mercado e a procura por soluções digitais de controlo de acessos. A empresa tem investido continuamente em pesquisa e desenvolvimento de tecnologias inovadoras para responder às necessidades dos clientes e oferecer soluções cada vez mais eficientes e seguras. O nosso foco é conseguir adaptar uma fechadura electrónica a qualquer tipo de porta, sem a necessidade de uma grande intervenção. Essa transição exigiu adaptação no nosso posicionamento e oferta, o que foi realizado com sucesso.

Como olha para evolução da área de controlo de acessos? Que tendências, na sua opinião, marcarão o futuro deste segmento?

A área de controlo de acessos está em constante evolução, impulsionada pela procura do mercado e surgimento de novas tecnologias, pelo que a tendência é que as soluções se tornem cada vez mais digitais e integradas, permitindo uma gestão mais eficiente e automatizada. Algumas das tendências que acreditamos que marcarão o futuro deste segmento incluem soluções em cloud, autenticação facial, o IoT, a inteligência artificial (IA) e soluções móveis. Por isso, o grupo SALTO tem crescido e adquirido empresas tecnológicas que possam responder a estas tendências.
Além disso, a segurança e a privacidade de dados serão cada vez mais valorizadas pelos clientes, impulsionando a criação de soluções mais robustas e confiáveis.

Considera que as soluções baseadas na cloud e com recurso a smartphones serão a grande aposta do futuro? Caso afirmativo, quanto tempo considera que teremos uma migração total para essa tipologia de soluções digitais?

Sim, acreditamos que as soluções em cloud e com recurso a smartphone serão uma grande aposta para o futuro do con-

trolo de acessos. A cloud permite uma maior flexibilidade e escalabilidade, permitindo aos utilizadores acederem aos sistemas de controlo de acessos de qualquer lugar, a qualquer momento e a partir de qualquer dispositivo.
No entanto, é importante lembrar que a adopção total de soluções em cloud pode depender de vários factores, como a disponibilidade de tecnologia e infra-estruturas adequadas, custos e preocupações com a segurança. Além disso, muitas organizações podem preferir manter os seus sistemas de controlo de acessos locais por motivos de conformidade ou segurança.

Tendo por base uma empresa que quer fazer o salto para soluções digitais, como as que a SALTO disponibiliza, que tipo de adaptação e investimento terá de fazer?
Para uma empresa fazer a transição para soluções digitais de controlo de acessos, como as oferecidas pela SALTO, é necessário um investimento em termos de infraestrutura e equipamentos. A empresa terá que avaliar a sua situação actual em termos de controlo de acessos e identificar quais áreas precisam de ser actualizadas.Alguns dos equipamentos e soluções digitais que a SALTO oferece incluem fechaduras electrónicas, leitores murais, software de gestão de acesso e monitorização, pelo que é necessário que a empresa tenha pessoas com conhecimentos para poder manter e administrar o sistema de controlo de acessos.
A adaptação da empresa também pode envolver algumas mudanças na cultura organizacional em termos de processos internos, pois é importante garantir o sucesso da transição para uma solução digital de controlo de acessos. Por fim, o investimento total dependerá do tamanho e complexidade do projecto, bem como do tipo de solução escolhida. A SALTO oferece soluções personalizadas e pode trabalhar com a empresa para identificar as melhores opções de acordo com as suas necessidades e recursos.

Considera que o mercado do controlo de acessos é competitivo? Em que medida, a SALTO se distingue da sua concorrência?
Sim, o mercado de controlo de acessos é bastante competitivo e existem várias empresas que oferecem soluções similares às da SALTO. No entanto, a SALTO tem uma posição de destaque no mercado devido à sua qualidade e oferta de soluções tecnológicas inovadoras e personalizáveis, que são projectadas para atender às necessidades específicas de cada cliente. A empresa investe continuamente em pesquisa e desenvolvimento, com o objectivo de continuar a oferecer soluções de controlo de acessos avançadas, seguras e fáceis de usar. Um dos grandes destaques da SALTO é termos um software integrado com vários outros softwares de gestão de controlo de acessos. Além disso, a SALTO possui uma ampla rede de distribuidores em todo o país, o que permite que a empresa ofereça serviços de instalação e suporte técnico por todo o território nacional. A SALTO também dispõe de plataformas tecnológicas em cloud, que permite aos clientes gerir os seus sistemas de controlo de acessos remotamente e em tempo real. Em resumo, o principal fator que diferencia a SALTO da concorrência é a sua qualidade e abordagem centrada no cliente. A empresa está comprometida em fornecer aos seus clientes soluções personalizadas e um excelente suporte ao cliente, desde o primeiro contacto até à implementação e manutenção do sistema.

Qual a importância da inovação no crescimento da SALTO? Que investimentos estão a fazer a esse nível?
A inovação é um dos pilares do crescimento da SALTO. A empresa está sempre à procura de novas formas de melhorar as suas soluções de controlo de acessos para se manter na vanguarda da tecnologia. A SALTO entende que a inovação é uma parte essencial da sua estratégia de negócio e investe significativamente em pesquisa e desenvolvimento para garantir que os seus produtos e serviços atendem às necessidades em constante evolução dos clientes.
Neste momento, a SALTO já é um conjunto de nove empresas, adquirindo recentemente a TouchByte, para acompanhar toda a tendência do mercado.•

MARCOS PAULO LIMA

VISIOTECH APOSTA NO MERCADO NACIONAL

A Visiotech é um distribuidor europeu de segurança electrónica que nasceu há 15 anos. Em Junho deste ano a empresa dá mais um passo no seu crescimento através da inauguração da sua nova filial em Portugal. Marcos Paulo Lima, country manager Portugal & PALOP da empresa, falou com a Security Magazine sobre os principais desafios e investimentos da empresa.

Security Magazine – Fale-nos da Visiotech e do que oferece ao mercado europeu?

Marcos Paulo Lima – A Visiotech é uma empresa europeia de distribuição de sistemas de segurança electrónica. O nosso forte sempre foi CCTV – câmaras e gravadores. Temos 15 anos de empresa e, ao longo desses anos, começamos com o CCTV e fomos progredindo, tendo introduzido as marcas de intrusão, controlo de acesso e videoporteiro. Temos o portfólio completo de uma empresa típica de distribuição de material de segurança eléctrico, passando pela parte do incêndio. A Visiotech é 100% europeia, tem a estrutura principal em Espanha e filiais em Portugal, França e Itália, – os quatro mercados mais antigos que trabalhamos, apesar de estarmos presentes em 65 países ao nível de clientes. Temos departamentos em Espanha, França, Itália, Norte de África e Norte da Europa. A empresa conta com 270 funcionários e uma facturação de 140 milhões de euros no ano passado. Somos a maior empresa de segurança electrónica na área distribuição da Europa Ocidental. Gostamos de ter as pessoas dentro da empresa. Nesse sentido, temos 40 funcionários no armazém, 10 pessoas no marketing e quatro tradutores que são professores de idioma e damos curso de idiomas aos nossos funcionários. Temos 40 milhões de euros em stock, o que nos permite ser muito dinâmicos e rápidos na resposta aos clientes. Fazemos cerca de 20000 envios por mês de material. Temos acordos estratégicos com empresas grandes de transporte, o que nos permite ter um bom preço, agilidade e preferência na entrega. Todo o material que chega a Portugal é proveniente de Espanha e entregue em 24 h nas principais cidades. Temos uma agilidade e capacidade de entrega difícil de encontrar na concorrência, a qual não consegue ter a nossa dimensão. Os grandes fabricantes têm o seu material fabricado na China. A Visiotech, quando compra material, compra dois ou três contentores de 40 pés para todos os mercados onde trabalha.

Quais as principais marcas que representam?

Na parte do CCTV, somos distribuidores oficiais da Hikvision, o maior fabricante do mundo de sistemas de segurança, com a facturação de aproximadamente 10 bilhões de dólares. Somos representantes oficiais da toda a gama Pro. Além disso, temos uma marca própria, a Safire, a terceira marca mais vendida depois da Hikvision e Dahua. na Península Ibérica.

Ter uma marca própria, obriga-vos também a ter um departamento focado na inovação e desenvolvimento?

Sim, exactamente. É algo que conseguimos fazer e que não é normal, ou seja, um distribuidor ter uma marca própria.

O fabrico dessa marca é vosso?

Escolhemos um fabricante estratégico com qualidade para fabricar material. Todo o desenvolvimento e marketing é nosso.

Passando para a área de intrusão, qual a vossa oferta?

Na parte da intrusão, somos distribuidores em Portugal, Espanha, França e Itália da Ajax. A Ajax tem um sistema de intrusão com e sem fio e domina completamente o mercado europeu. É um fabricante muito dinâmico que lança constantemente novos produtos. Em Portugal e Espanha, é o sistema de intrusão sem fio mais usado. Somos distribuidores há mais de cinco anos dessa marca e a empresa que mais know how tem no produto. Igualmente temos um stock gigantesco porque trabalhamos com todos os mercados europeus. Noutros países somente uma empresa tem a distribuição para um país. Não há nenhuma empresa que tenha dois países em simultâneo na Ajax. A Visiotech conseguiu fazer um acordo com a Ajax e nos quatro países tem a distribuição da marca.

Nas restantes áreas, que marcas destacaria?
No que tange ao videoporteiro temos a ZKTeco, um fabricante que domina o mercado de videoporteiro na parte da indústria. Destacaria também a Akuvox e a Safire. Na parte do incêndio temos a Carrier, fabricante americana de grande dimensão.

Estão abertos à distribuição de novas marcas?
Com certeza. Somos uma empresa dinâmica e temos de testar constantemente produtos que são lançados. Este é um mercado de tecnologia e os fabricantes estão sempre a inovar. A cada seis meses a um ano morre um produto e nasce outro produto novo. Actualmente, com a Inteligência Artificial, a analítica de vídeo está muito forte e os fabricantes lançam novos produtos com essa tecnologia incorporada e muito na área do IP. O analógico está a morrer e poucas instalações novas são feitas com analógico. Tudo o que é obra nova é com tecnologia IP, a inteligência está dentro da câmara, a qual permite esse aperfeiçoamento continuo do hardware.

Que novos projectos estão previstos para Portugal?
Queremos fazer a inauguração oficial da nossa filial em Portugal a 1 de Junho, convidando os nossos clientes para que conheçam um pouco mais da nossa estrutura. Queremos ter uma presença física em Portugal, tal como temos noutros países. Teremos um showroom, com todos os nossos produtos, que permitirá aos clientes testar e conhecer os produtos. Teremos uma sala de formação, onde daremos formações periódicas a cada 15 dias, de forma que os clientes possam ter conhecimentos para prestar um bom serviço ao cliente final. A Visiotech é um parceiro dos clientes instaladores, profissionais da segurança. O objectivo é dar todas as ferramentas para que os nossos clientes possam oferecer um excelente serviço ao cliente final, tanto doméstico como empresarial. Nesse sentido, é muito importante que o cliente tenha todos os conhecimentos para prestar um bom serviço ao cliente final e este se sinta reconhecido e veja que pagou o valor justo.

Este investimento em Portugal irá fazer com que tenham uma equipa no país?
Há cerca de 10 anos que trabalhamos com o mercado português. A equipa já existe e tem 15 pessoas só para o mercado português. Na filial teremos um técnico e um comercial interno. Os nossos delegados de zona usarão a filial, por exemplo, para levar clientes e mostrar material. A filial vai permitir-nos aproveitar os clientes que temos e a estrutura de pessoal, fornecendo melhores condições de formação, recepção de produtos para reparação, entre outras coisas.

Quando salienta a parte da formação, está prevista também a presença de parceiros para essas formações?
Sim, a ideia é trazer fabricantes para darem formação na nossa filial, sendo que temos formações marcadas para Junho e Julho. Queremos que os clientes possam adquirir conhecimento e tenham o know how suficiente para fazer a instalação com sucesso nos seus clientes.

Com esta filial, terá de dividir o seu tempo entre Portugal e Espanha?
Com certeza. A ponte aérea entre Lisboa, Porto e Madrid será muito mais frequente, pois sou responsável pela equipa inteira e, como tal, necessito de dar acompanhamento e ferramentas aos funcionários do departamento português, para que possam alcançar os objectivos muito ambiciosos da empresa. A Visiotech é muito ambiciosa e sempre quer crescer e consegue-o. Temos uma média de crescimento nos últimos cinco anos de 40%, o que é completamente fora da realidade da média das outras empresas do sector. Estes resultados devem-se ao facto de pensarmos, acreditarmos, sonharmos e concretizarmos. Há muito trabalho das pessoas e investimento da empresa e estamos a colher bastantes frutos disso. Somos líderes em Portugal e Espanha, o que não é fácil pois somos uma empresa de 15 anos que, com uma forma diferente de trabalhar, conseguiu chegar aqui.

A que se deve esses resultados que refere? A inovação e espírito jovem são factores importantes?
É um pouco de tudo. É uma empresa jovem, que chega com vontade de fazer diferente, ser dinâmica e que procura constantemente fabricantes para ter os melhores produtos. Não temos produtos por ter, ou seja, somente incorporamos na gama um produto que acreditamos que é muito dinâmico e inovador e não estamos presos às marcas tradicionais. Aliado a isso, temos um armazém em Madrid com 10.000m2. Destaco também a presença no mercado europeu, que nos permite trocar ideias e sinergias com os departamentos de França, Itália, Alemanha… A tecnologia não nasce no mundo inteiro de forma unificada. Há uma empresa que desenvolve e implementa num determinado país e depois a replica noutros países. Ser uma empresa europeia permite-nos perceber o que funciona em determinado país. Por exemplo, hoje, em Espanha, as principais empresas de alarme não são de segurança, mas, sim, de telecomunicação.

Já se assiste a essa tendência em Portugal também.
Sim, a segunda empresa que mais instala alarmes em Portugal é a NOS que fez a parceria com a Securitas. Em Espanha, isto acontece há um ano, antes de qualquer coisa acontecer em Portugal. Como parceiros das empresas de telecomunicações alertei para o facto de isso vir a acontecer aqui. Em França e Itália ainda nenhuma empresa de telecomunicações deu esse passo, mas irá acontecer e os meus colegas desses países já estão a preparar-se. Essa é uma vantagem da Visiotech, poder ver o que acontece noutros mercados e rapidamente movimentar-se e replicar noutros mercados.

Como olha para 2023?
2023 será um grande ano, marcado pela inauguração da filial e estabilização da Visiotech no mercado nacional. Estamos a fazer grandes investimentos no marketing. Este ano é definitivo para a Visiotech no que tange ao mercado português, com incorporação de novas pessoas, sendo que planeamos finalizar o ano com 20 pessoas em Portugal. É um investimento grande no mercado português e definitivo para nós.•

SEGURANÇA E SAÚDE NO TRABALHO

INTERSAFE CHEGA A PORTUGAL

A Intersafe, empresa de segurança no trabalho e EPI, acaba de chegar a Portugal através do Grupo Lyreco, com o objectivo de consolidar o seu plano de expansão na Europa.

A Intersafe, empresa de segurança no trabalho e EPI, acaba de chegar a Portugal através do Grupo Lyreco, com o objectivo de consolidar o seu plano de expansão na Europa.
A Intersafe dispõe de um portfólio com mais de 13.000 referências, incluindo produtos e serviços de algumas marcas do sector, tais como 3M, Panter, Mendi, Velilla, Portwest, Deltaplus, Monza, Bollard, Bollé, Ansell, JSP, Isalline, Normaluz, Honeywell, Uvex, Irudek, etc. O seu compromisso com a segurança no local de trabalho complementa-se com uma oferta de soluções integrais que incorporam serviços de protecção ocular, auditiva, da cabeça, respiratória, das mãos, assim como roupa de trabalho especializada e calçado de segurança laboral Através da sua rede de distribuição própria, a Intersafe fornece um serviço de entregas em 24 horas em qualquer ponto de Portugal continental.
A Intersafe, fundada na Holanda em 1934 como especialista em óculos de segurança graduados, foi adquirida pela Lyreco em 2018 para reforçar o seu compromisso com o sector da segurança no trabalho. Como parte do plano de expansão internacional, em 2023 a Lyreco introduz a Intersafe em Portugal e Espanha, territórios em que tem a ambição de "posicionar-se como líder no mercado de segurança no espaço de trabalho dentro dos próximos quatro anos"."Com o lançamento da Intersafe, a Lyreco continua a impulsionar o nosso plano de expansão global GREAT 26 e um dos seus pilares: o crescimento do segmento da segurança no trabalho. Nos próximos quatro anos, o nosso objectivo é quadruplicar o nosso volume de negócios neste segmento para liderar o mercado de equipamentos de protecção individual e de segurança em Portugal", explica **Gabriel Mops, Director Geral da Lyreco Ibéria**.A direcção da Intersafe fica a cargo de Ramón Abella, profissional com mais de 20 anos de experiência a liderar projectos de expansão de negócios e há mais de 10 anos a conduzir equipas de vendas na Lyreco. Ramón Abella reporta directamente à Direcção Geral da empresa.
"Já passou uma década desde o lançamento da divisão industrial da Lyreco. Ao longo deste período, assistimos ao crescimento significativo desta área de negócio dentro da empresa para se tornar numa das mais importantes para a Lyreco. Ao integrar a Intersafe nesta divisão, a Lyreco reforça a sua forte aposta na segurança no trabalho e estabelece o objetivo de ser líder europeu em segurança no trabalho e EPI", conclui **Ramón Abella, Diretor da Intersafe Ibéria**.

AJAX SYSTEMS INTEGRADA NA PLATAFORMA DA DESICO

A Desico, empresa dedicada ao desenvolvimento de sistemas de controlo informatizados, integrou dispositivos Ajax no Vigiplus PSIM, uma suite de aplicações para centros de controlo. Esta plataforma adapta-se a qualquer instalação, integrando sistemas de intrusão e incêndio, controlo de acessos, CCTV, intercomunicadores, public adress, monitorização de redes IP, equipamentos técnicos ou elementos IoT.
"A integração com a Desico é um marco, uma vez que responde a uma procura do próprio mercado, pois é uma das plataformas mais consolidadas em Espanha", afirma **Roberto Otero, Director Técnico da Iberia Ajax Systems**.
A integração do Vigiplus permite adicionar diferentes dispositivos Ajax a uma única plataforma. O sistema sincroniza-se com todos os estados dos detectores ligados, permitindo o envio de ordens de uma forma intuitiva e simples para o operador.
O armar de grupos ou o bypass de zonas são algumas das funcionalidades implementadas. Foram integradas opções de pesquisa de imagens, bem como funcionalidades de auto-configuração através do descarregamento de dados sobre grupos e zonas a partir da nuvem.
"A nível técnico, vale a pena destacar a segurança da conectividade com o ambiente de nuvem Ajax e a utilização de filas SQS (Simple Queue Service) da AWS para obter os eventos gerados pelo painel de controlo", explica **Jordi Artigas Mestres, Director Adjunto do departamento de software da Desico**.•

O PAPEL DAS EQUIPAS DE SEGURANÇA PRIVADA NO REGIME GERAL DA PREVENÇÃO DA CORRUPÇÃO

O fenómeno da corrupção ofende a essência da democracia e os seus princípios fundamentais, designadamente os da igualdade, transparência, livre concorrência, imparcialidade, legalidade, integridade e a justa redistribuição de riqueza.O Decreto-Lei 109/E de Dezembro de 2021 tem publicado no seu anexo o Regime Geral da Prevenção da Corrupção (RGPC), que prevê a obrigatoriedade da sua implementação, em todas as organizações dos setores público, privado e social, que tenham mais do que 50 trabalhadores, e nos casos das Autarquias, as que tenham mais do que 10000 habitantes.
O RGPC prevê a nomeação de um responsável pelo cumprimento normativo e instrumentos de combate à fraude e à corrupção, que incluem a implementação de um plano de prevenção de riscos de corrupção e infracções conexas, um código de conduta, um canal de denúncias, a formação e comunicação, procedimentos de controlo interno e procedimentos de avaliação prévia de entidades terceiras. Também estão previstas coimas para a ausência, ou para a ineficiência da implementação deste sistema de conformidade nas organizações.
Qual o impacto e a intervenção das equipas de Segurança na conformidade das organizações com este diploma? O Impacto é enorme e decisivo nas mais diversas vertentes, nomeadamente, na exemplaridade e como intervenientes na operacionalização e vivência da conformidade.
No que respeita ao instrumento do RGPC, canal de denúncias, a Lei n.º 93, de 2021, que estabelece o Regime Geral de Proteção de Denunciantes de Infrações (RGPDI), no ponto n.º 2, do artigo 11º prevê:
2 - No seguimento da denúncia, as entidades obrigadas praticam os atos internos adequados à verificação das alegações aí contidas e, se for caso disso, à cessação da infração denunciada, inclusive através da abertura de um inquérito interno ou da comunicação a autoridade competente para investigação da infracção, incluindo as instituições, órgãos ou organismos da União Europeia. Entende-se assim, que as organizações devem dotar-se dos recursos necessários para desenvolverem investigações internas dentro dos limites consagrados na Lei. Neste sentido, quando necessário, devem ser formadas pessoas e dotá-las com os meios para assegurar a conformidade com esta Lei.
Quem nas organizações estará mais apto para conduzir, ou contribuir para estas investigações?
A Auchan desde 2018, ano em que, por via da Loi Sapin 2, Lei francesa que combate a fraude e a corrupção (similar ao RGPC), sendo uma filial de uma multinacional francesa, teve de implementar a conformidade com esta lei em Portugal. Neste sentido, foi criada a função de Segurança Económica que integra a Direcção Nacional de Segurança da Auchan e que tem a responsabilidade de assegurar a conformidade de vários desses instrumentos, nomeadamente, a pré-avaliação de entidades terceiras, a resposta ao canal de denúncias, a prevenção, deteção e investigação de fraude e a formação, principalmente aos quadros mais expostos à corrupção.

O processo de implementação ofereceu vários desafios que foram ultrapassados, em grande parte, devido ao ecossistema das várias funções e processos já implementados na Direcção de Segurança da Auchan, no seu Centro Nacional de Segurança. Também foi criada a função de analista de segurança económica, que tem como principais funções:
• Analisar os dados de entidades terceiras: fornecedores de produtos, prestadores de serviços ou outros parceiros. Estes dados têm origem em diferentes fontes internas e externas, em que se incluem sistemas agregadores de bases de dados com informações ao nível internacional. Comparar esses dados com o relatório inicial fornecido pelas entidades terceiras. Detectar anomalias, incluindo as discrepâncias entre a informação fornecida pela entidade terceira e a pesquisada nas diferentes fontes de informação. Elaborar um relatório que é usado para formular um parecer os riscos da relação entre a Auchan e as entidades terceiras, baseado nas análises efetuadas.
• Dar seguimento às denúncias recebidas, efectuando, sempre que necessário, investigações internas.
• No âmbito da prevenção e detecção e investigação de fraude: extrair, preparar e processar os dados provenientes, principalmente dos sistemas de gestão da empresa e reportar as potenciais situações de fraude, usando técnicas e modelos avançados de estatística e de visualização. Efectuar entrevistas de investigação interna e elaborar o relatório com as conclusões da investigação, para responsabilização e melhor conhecimento do método de fraude e o consequente apoio à sua prevenção.
Esta é uma experiência que entendemos ser importante partilharmos, porque pode contribuir para apoiar a implementação do RGPC nas mais diversas organizações, em que as Equipas de Segurança poderão protagonizar funções de relevância, aumentando e valorizando as suas funções, neste caso específico, de segurança de bens.

LUIS FONSECA, ENCARREGADO DA PROTEÇÃO DE DADOS E COORDENADOR DE SEGURANÇA ECONÓMICA DA AUCHAN RETAIL PORTUGAL

FERNANDO LUÍS SILVA

SEGMON APOSTA EM NOVA SEDE

A Segmon, empresa dedicada às áreas de SCIE e segurança electrónica, está a construir, na zona de Coimbra, a sua nova sede. As obras estarão concluídas em Agosto e darão à empresa uma maior operacionalidade e crescimento.

À Security Magazine, **Fernando Luís Silva, director-geral** da empresa, avançou que a construção da nova sede arrancou em 2021, devido "há necessidade de espaço e de condições que já se fazia sentir há uns anos", estando esta aposta enquadrada no plano de investimentos sólidos e seguros que a Segmon havia iniciado. A nova sede permitirá "uma maior operacionalidade dos serviços centrais da empresa, permitindo, por exemplo, aumentar os quadros ao nível da engenharia e formação, bem como uma qualidade superior nas condições de trabalho oferecidas aos seus colaboradores".

A conclusão das novas infra-estruturas está prevista para Agosto deste ano. O investimento irá materializar-se numa área de cerca de 900m2, distribuídos por três pisos, destacando-se a localização privilegiada, "numa zona da cidade de Coimbra que permite uma excelente acessibilidade e visibilidade, pois encontra-se junto a uma das saídas do IC2 na zona Norte da cidade, integrada num parque industrial municipal".

Reforço da frota

Os investimentos da Segmon têm passado também pela sua frota de veículos. Fortemente focada na escolha e composição da sua frota, Fernando Luís Silva explica que a empresa conta com 24 veículos, nomeadamente viaturas oficina, com diferentes graus de equipamento, e veículos ligeiros de passageiros (alguns a GPL). Desde Janeiro, a Segmon conta com uma viatura 100% eléctrica, essencialmente para apoio aos serviços administrativos e engenharia.

O director-geral da empresa sublinha que a vida útil média de cada viatura não ultrapassa os cinco anos, sendo que a empresa está muito atenta às emissões de CO2 e consumos, aspectos "sempre levados em conta na altura da sua aquisição". Como demonstração desse cuidado, destaca a evolução positiva entre 2014 e 2021 relativamente aos litros de combustível consumidos por cada 1000 euros de vendas. Em 2014, a empresa contabilizou 26,7l de gasóleo por cada 1000 euros. Já em 2021, o valor reduziu para os 18,8l por cada 1000 euros em vendas. Recorde-se que a Segmon tem a certificação ISO 14001 implementada desde 2012.

"A segurança não pode esperar"

O responsável explica que a empresa nasceu em Junho de 2006, fruto da cisão entre sócios da Mimi – Manutenção e Instalação de Materiais de Incêndio, Lda., com sede em Faro e filiais em Coimbra e Leiria. "Este processo, deu origem à Segmon, em Coimbra, com filial em Faro, e à Inovaseg, Lda. com sede em Leiria, entretanto insolvente em 2007". A Segmon tem como sócios fundadores Fernando Luís Silva, gestor de empresas, Paulo Vasconcelos, engenheiro electromecânico, e Pedro Grilo, engenheiro electrotécnico.

"Herdando toda a experiência dos seus promotores, em 2006, a Segmon elege como seu «core» o após venda na segurança contra incêndio em edifícios (SCIE), dando igualmente muita atenção às novas possibilidades que vão surgindo na seguran-

ça electrónica, como seja o CCTV", explica.
A Segmon, conta, "começa por inovar ao oferecer no mercado contractos de manutenção preventiva na SCIE, normalmente com a duração de cinco anos (coincidindo neste período com as acções obrigatórias ao nível dos extintores, substituição do agente extintor, e na RIA, com os testes hidrostáticos nas mangueiras e agulhetas), com pagamentos iguais em cada um desses cinco anos, e abrangendo todas as valências da SCIE, bem como na segurança electrónica, detecção de intrusão CCTV, etc".
Além do após venda, a Segmon actuou sempre na área das obras de SCIE, junto dos novos clientes e dos. "Iniciou igualmente a promoção de formações ao nível de SCIE, quer integrando essas acções nos contractos de manutenção, quer fazendo-as de forma isolada". Posteriormente, obteve a acreditação destas acções de formação junto da DGERT.
O responsável destaca que a Segmon sempre teve "a ambição de ser uma empresa de dimensão nacional" e sempre entendeu que "a segurança não pode esperar e tem de estar próxima do seu cliente". Por esta razão, optou por estar fisicamente em Coimbra, Faro, Caldas da Rainha e Viseu, permitindo-lhe posicionar-se a cerca de 1h30 de qualquer ponto de Portugal continental.

Um ano de crescimento

2023 será um ano de crescimento para a Segmon, tendo como objectivo atingir um volume de vendas de 2,5 milhões de euros. Este valor "faz parte do plano de crescimento traçado para 2019", o qual "deveria ter o seu início em 2020" e que permitiria à empresa chegar aos 3 milhões de euros de volume de vendas em 2022. Porém, a pandemia, "alterou muita coisa", relembra. "No nosso caso, (a pandemia) fez com que 2020 e 2021 fossem anos de «paragem» deste plano", tendo-se iniciado em 2022 o primeiro ano desse plano", o qual terminará em 2024, ano em que a empresa estima alcançar um valor de 3 milhões de euros em vendas.
"A Segmon, como a conhecemos e concebemos, só pode crescer pelo caminho de uma maior penetração geográfica pois, neste momento, não nos parece, de todo, que um aumento de oferta de produtos ou serviços seja um caminho aconselhável", avança. Como acrescenta, "temos de ser bons (muito) no que fazemos e não nos devemos dispersar em outras áreas (...)".
A empresa deve "perseguir uma muito maior penetração no mercado do Algarve, na zona da Grande Lisboa e na zona de Viseu, sendo que em Coimbra o objectivo é muito mais o da manutenção e melhoria do mercado existente".
O director-geral explica que "em cada uma destas áreas há objectivos comerciais diferentes que se adaptam ao estágio de desenvolvimento de cada uma destas filiais", assim como "objectivos estratégicos diferentes". Isto porque, justifica, se em Lisboa o foco passa pela conquista de clientes de dimensão e implantação nacional e de grandes dimensões, já em Faro a aposta passa pela diversificação do mercado actual para áreas económicas pouco exploradas, pois "basicamente só se tem «vivido» com a hotelaria". Por fim, em Viseu os objectivos passam por ganhar quota de mercado em todos os mercados "pois é a filial mais recente", refere.•

EM PALMELA

CEDROS ASSINA PROTOCOLO PARA FORMAÇÃO DE MARÍTIMOS

A Cedros assinou hoje, nas suas instalações em Quinta do Anjo, Palmela, o protocolo relativo à formação de marítimos, tendo contado com a presença do Secretário de Estado do Mar.

À Security Magazine, Luís Coelho, director-geral da Cedros, explicou que este "é o fechar de um ciclo relativo à certificação para a formação de marítimo, sendo um processo que requer o acordo da DGRM". Como apontou que este é também "o início de um ciclo". Como explicou, "há uns anos a Cedros decidiu avançar com um processo de internacionalização cá dentro, ou seja, criar um centro de formação internacional que capte negócio estrangeiro". Actualmente, o centro já capta 80% de formandos estrangeiros, provenientes sobretudo da Europa.
Com esta nova oferta formativa, a STCW, a empresa entra noutro nicho de mercado, sendo importante recordar que quem anda numa embarcação tem de possuir esta formação. As maiores infra-estruturas e oferta formativa da Cedros estão localizadas em Palmela, onde a empresa se encontra desde 2007. Além destas instalações, a Cedros conta com instalações no Porto e um acordo há cinco anos com o Politécnico de Beja que lhe permite ter infra-estruturas e formação com os técnicos daquela instituição. Além disso, a Cedros ministra formação na casa do cliente ou em ambiente híbrido..

EU-OSHA REVELA AS ÚLTIMAS TENDÊNCIAS SOBRE SST

A Agência Europeia para a Segurança e a Saúde no Trabalho (EU-OSHA) lançou esta semana o seu relatório de referência Segurança e saúde no trabalho na Europa: estado e tendências 2023 na Cimeira da UE sobre Segurança e Saúde no Trabalho (SST) de 2023, em Estocolmo.

O relatório apresenta uma análise exaustiva do estado e do contexto da SST na União Europeia ao longo dos últimos anos e fornece informações sobre as tendências emergentes. "Por exemplo, entre 1998 e 2019, os acidentes de trabalho não mortais diminuíram 58% na UE, enquanto os acidentes mortais acidentes mortais diminuíram 57%. A melhoria das medidas de prevenção, juntamente com a evolução económica e as mudanças na força de trabalho contribuíram para estas reduções. No entanto, a maior parte desta diminuição ocorreu antes de 2010 e os números têm vindo a estagnar nos últimos anos", refere o **Director Executivo Interino da EU-OSHA, William Cockburn**. O relatório apresenta igualmente uma panorâmica das potenciais melhorias, da estagnação e da ambiguidade e ambíguos, bem como áreas de preocupação como os tipos de trabalho não normalizados, o cumprimento incompleto da regulamentação em matéria de SST ou a inactividade física, bem como os desafios futuros.
Nicolas Schmit, Comissário Europeu para o Emprego e os Direitos Sociais, congratulou-se com o relatório:
"A saúde e a segurança no trabalho são uma parte essencial das actividades de qualquer organização. As mudanças no local de trabalho causadas pela crise da COVID-19, pelas transições ecológica, digital e demográfica, bem como pelo progresso científico e e tecnológica, levaram a Comissão a adoptar, em Junho de 2021, um novo quadro estratégico da UE para 2021-2027 em matéria de saúde e segurança no trabalho, em Junho de 2021. O relatório da EU-OSHA "Segurança e saúde no trabalho na Europa: estado e tendências 2023" fornece uma análise essencial dos aspectos que melhoraram nos locais de trabalho em toda a UE, mas também onde ainda temos muito trabalho a fazer". A EU-OSHA espera que esta publicação tenha um impacto significativo nas futuras políticas e abordagens para futuras políticas e abordagens para salvaguardar a segurança e a saúde dos trabalhadores na Europa. Os dados podem ser facilmente visualizados e analisados país a país, utilizando a ferramenta de visualização de dados do Barómetro SST.
Este evento, co-organizado pela Comissão Europeia e pela Presidência sueca da UE, reúne instituições da UE, Estados-Membros, parceiros sociais e outras partes interessadas. A EU-OSHA está a colaborar activamente com os participantes nos debates sobre os primeiros ensinamentos retirados do Quadro Estratégico da UE, incluindo os progressos alcançados na abordagem da "visão zero" em relação às mortes relacionadas com o trabalho. Outros tópicos incluem a saúde mental na vida activa, o papel dos parceiros sociais, os efeitos das ondas de calor e das alterações climáticas no domínio da SST e a avaliação das estratégias nacionais de SST. No contexto do "Impacto das alterações climáticas e das ondas de calor na SST", a EU-OSHA apresenta um guia sobre SST e stress térmico que fornece orientações práticas sobre como gerir os riscos associados ao trabalho no calor e informações sobre o que fazer se um trabalhador começar a sofrer de uma doença ou problema de saúde relacionado com o calor.

SICUREZZA 2023 DECORRE EM NOVEMBRO EM MILÃO

A SICUREZZA 2023 está agendada para 15 a 17 de Novembro. Com mais de 250 empresas registadas, provenientes de mais de 20 países, e mais de 80% da área de exposição já ocupada, já se estabeleceu como um centro internacional e totalmente representativo da gama global de produtos de merchandising.
A SICUREZZA 2023 é um ponto de referência primordial para os profissionais de segurança e prevenção de incêndios. A SICUREZZA já conta com mais de 250 empresas registadas de 20 países diferentes e mais de 80% da área de exposição já ocupada.
As marcas confirmadas incluem importantes regressos e várias novas entradas, representando 30% da assistência. O projecto de recrutamento de compradores internacionais

arrancou da melhor forma, com a adesão de 25 países e, sobretudo, com uma presença reforçada da Europa de Leste, da Bacia do Mediterrâneo, do Médio Oriente e da África do Norte e do Sul. A digitalização, os sistemas inteligentes integrados e personalizados serão o foco central de todo o evento, a fim de proporcionar aos profissionais e às realidades de todo o sector a oportunidade de falar e, ao mesmo tempo, de se relacionar: CCTV, Detecção de Intrusão, Prevenção de Incêndios, Controlo de Acessos, Segurança Passiva, Cibersegurança.

MARINA DE VILAMOURA AVANÇA PARA SISTEMA DE VIDEOVIGILÂNCIA

Daqui a um ano, a Marina de Vilamoura, no Algarve, passará a ter um novo sistema de videovigilância. Neste sentido, o Município de Loulé e a Guarda Nacional Republicana assinaram um protocolo que prevê a criação desta medida tendo em vista o reforço da segurança de pessoas e bens e tranquilidade pública.

Daqui a um ano, a Marina de Vilamoura, no Algarve, passará a ter um novo sistema de videovigilância. Neste sentido, o Município de Loulé e a Guarda Nacional Republicana assinaram um protocolo que prevê a criação desta medida tendo em vista o reforço da segurança de pessoas e bens e tranquilidade pública.

Além dos locais públicos na zona envolvente da Marina, a implementação, activação e gestão deste sistema irá alargar-se também às vias de acesso a este espaço de recreio náutico, nomeadamente Av. Cerro da Vila, Av. Engº João Meireles, Av. Da Marina, Av. Tivoli, R. do Clube Náutico, R. do Sol, Estrada de Quarteira, Largo do Cinema e R. das Estrelas. São áreas de passagem, permanência e convivência de um elevado número de pessoas, sobretudo de muitos turistas que visitam Vilamoura ao longo de todo o ano, e, como tal, mais passíveis da ocorrência de situações que ponham em causa a segurança. Gerido exclusivamente pela GNR, o sistema proposto prevê a instalação de 42 câmaras de vídeo e mais de meia centena de sensores para recolha de informação. O centro de monitorização ficará alojado no quartel da GNR em Vilamoura, sendo possível a sua visualização na sala de situação do Comando Territorial de Faro. O investimento é do Município de Loulé e ronda os 900 mil euros. "Se tudo correr bem em termos do concurso público", prevê-se que possa entrar em funcionamento no Verão de 2024, como garantiu o **autarca Vítor Aleixo**, na informação disponível no site da Câmara de Portimão.

Mas durante a celebração deste protocolo de cooperação, que nasce do diálogo de vários anos entre as duas instituições, o presidente da câmara quis sublinhar que a privacidade dos cidadãos não será posta em causa. "A protecção de dados e a 'anonimização' é uma garantia, até porque a Lei assim o prevê e, portanto, a privacidade das pessoas será sempre salvaguardada".

Apesar de alguma "resistência inicial" do autarca quanto à implementação deste sistema, as dificuldades por parte da tutela em aumentar o número de efectivos e, por outro lado, os "bons exemplos" de Portimão e Olhão com um sistema idêntico levaram Vítor Aleixo a mudar de ideias e avançar para a videovigilância.

"Vamos esperar que tudo corra bem e que essa seja uma mais-valia para prevenir e fazer diminuir a delinquência. Para uma região turística, geradora de tanta riqueza, a componente da segurança é extremamente sensível", notou.

Por seu turno, **Carlos de Almeida, responsável pelo Comando Territorial da GNR de Faro**, explicou que a videovigilância irá "optimizar os recursos disponíveis", permitindo privilegiar o "empenhamento operacional flexível que proporciona uma resposta pronta e oportuna, constituindo-se como um importante mecanismo complementar da actividade policial nas dimensões preventiva e reactiva".

"Este protocolo vem reforçar ainda mais a excelente relação entre a Guarda Nacional Republicana e o Município de Loulé na procura de mais e melhores soluções para que o concelho continue a ser um espaço de segurança e tranquilidade, e se afirme cada vez mais como um município de vanguarda", considerou o comandante da GNR no Algarve.

Numa segunda fase do projecto a ideia das duas entidades cooperantes é estender a videovigilância à própria cidade de Quarteira visto tratar-se também de uma "área urbana de grande concentração humana". Um anúncio feito no dia em que Quarteira celebrou 24 anos de elevação a cidade. •

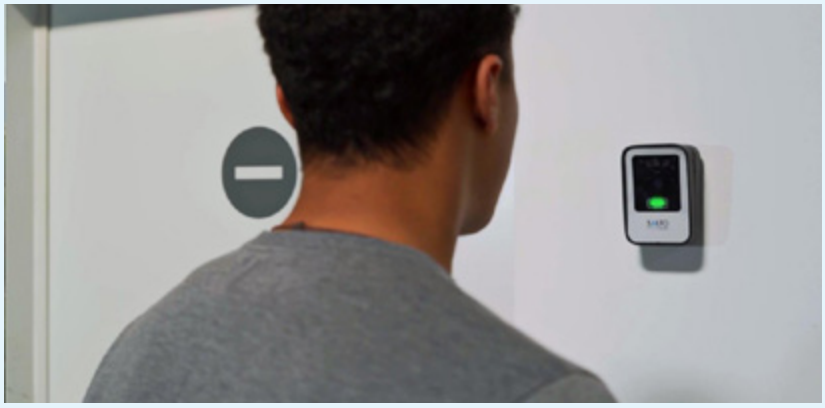
VW AUTOEUROPA SALIENTA IMPORTÂNCIA DE AGVS PARA A SEGURANÇA

A fábrica da Volkswagen, em Palmela, utiliza AGV (veículos guiados automaticamente) nas suas instalações. Os primeiros chegaram à fábrica portuguesa para o processo de abastecimento de motores e caixas a partir do supermercado para a linha de motores, ainda antes do início de produção do Scirocco em 2007 e 2008.
Como aponta no seu site, o futuro já começou há muito tempo. "Estamos no advento da quarta era dos AGV. Actualmente, temos um total de 70 AGV no processo de abastecimento de contentores Just in Time e Just in Sequence e de alguns processos de montagem e 15 AGV no processo de abastecimento de peças à linha de construção de carroçarias". Com sensores e câmaras, estes veículos "são como um assistente de direcção de confiança. Mantêm sempre um olho atento na rota para garantir a segurança, reduzindo o risco de acidentes de trabalho e a fluidez dos abastecimentos e da operação".

AUCHAN RETAIL PORTUGAL ADQUIRE VIATURA DE SEGURANÇA PARA PLATAFORMA

A Auchan Retail Portugal anunciou que adquiriu uma nova viatura de segurança, 100% eléctrica, para a sua plataforma logística na Azambuja.
O veículo é, segundo a empresa, "muito compacto, versátil e flexível". O veículo Goupil, pertencente ao grupo Polaris, conta com uma autonomia de 90km, cabine de dois lugares, largura de 1200mm, velocidade de 50km/h e zero emissões de carbono. A carroçaria, superestrutura e equipamentos foram desenvolvidos e montados em Portugal.
"Esta é a primeira viatura eléctrica na Europa a reunir este conjunto de características, estando totalmente adaptada para responder eficazmente em operações de segurança e combate a incêndio num curto raio de acção",
O veículo "está preparado para aumentar os níveis de prevenção e melhorar, também, a capacidade de resposta e prontidão operacional da equipa de segurança, nas diferentes tipologias de ocorrências".
A aquisição desta viatura "é um exemplo claro da preocupação da Auchan com a protecção do meio ambiente, uma vez que esta não só utiliza uma fonte de energia limpa, como também fomenta a economia local e a sustentabilidade da sua cadeia de abastecimento", acrescenta. A Auchan investe na modernização e optimização da sua Plataforma Logística para "garantir uma operação sustentável e eficiente, utilizando tecnologias avançadas, práticas de gestão ambiental e logística reversa para minimizar o impacto ambiental e promover uma cadeia de abastecimento mais sustentável". •

SALTO INTRODUZ O CONTROLO DE ACESSOS POR RECONHECIMENTO FACIAL ATRAVÉS DA AQUISIÇÃO DA TOUCHBYTE



A SALTO Systems, um dos principais fornecedores de soluções inteligentes de controlo de acessos eletrónico, confirma a sua aposta na tecnologia de reconhecimento facial para controlo de acessos com a aquisição da TouchByte. A TouchByte é uma empresa britânica pioneira no controlo de acessos sem contacto que utiliza sistemas avançados de reconhecimento facial.

A SALTO Systems, um dos principais fornecedores de soluções inteligentes de controlo de acessos eletrónico, continua a apostar no reconhecimento facial e na tecnologia biométrica como o controlo de acessos do futuro. Nos últimos anos, a empresa decidiu acelerar o desenvolvimento destas soluções de controlo de acessos sem contacto através de uma série de investimentos estratégicos.

O impacto da transformação digital na sociedade conduziu a uma transformação completa, que se reflete nas utilizações e comportamentos dos utilizadores, dentro e fora das áreas profissionais, pessoais e de lazer. Setores inteiros foram reinventados e os nossos ambientes de trabalho, casas, escolas, infraestruturas sociais, de saúde e atividades de lazer evoluíram juntamente com a incorporação do reconhecimento facial no quotidiano. As chaves inteligentes, as identidades digitais e o reconhecimento facial estão a tornar-se normalizados em todos os setores e áreas de aplicação, com o reconhecimento facial a emergir como uma tecnologia fundamental para satisfazer as necessidades do mercado.

Em 2022, a SALTO Systems adquiriu a Cognitec, uma empresa líder com mais de 20 anos de experiência no desenvolvimento no domínio do reconhecimento facial. Este passo já era significativo para melhorar as soluções de controlo de acessos da SALTO através da tecnologia biométrica para oferecer uma experiência de acesso inteligente sem contacto. Ao integrar o famoso algoritmo FaceVACS, desenvolvido pela Cognitec, em dispositivos inteligentes e sistemas de controlo de acessos, a SALTO irá incorporar todo um novo portfólio de produtos para permitir outras utilizações numa multiplicidade de aplicações e setores.

Agora, esse momento está mais próximo do que nunca. Com a recente aquisição da TouchByte, uma marca inovadora de tecnologia dedicada ao desenvolvimento de soluções de reconhecimento facial, a SALTO pretende acelerar o desenvolvimento e o tempo de colocação no mercado da primeira e mais avançada solução de controlo de acessos por reconhecimento facial alimentada pelo algoritmo da Cognitec através das soluções, produtos e plataforma de gestão facial da TouchByte.

A adição da TouchByte ao grupo SALTO reforça o compromisso da SALTO para com a inovação e o desenvolvimento de novas tecnologias. "A aquisição da TouchByte é mais um passo no nosso esforço para integrar novas tecnologias no mercado do controlo de acessos", afirmou Marc Handels, Diretor de Tecnologia e Inovação da SALTO Systems, acrescentando que "com a nossa futura solução de reconhecimento facial, pretendemos fornecer aos nossos clientes e parceiros um método seguro e rápido de acesso sem contacto aos seus edifícios e instalações.

A utilização da tecnologia biométrica não é uma coisa do futuro, a SALTO está ansiosa por ver o que o futuro reserva para a tecnologia biométrica e como esta pode continuar a trazer valor aos seus clientes e parceiros, bem como novas oportunidades para a gestão e controlo de acessos de qualquer tipo de instalação.

CARLOS DIAS

NAUTA FAZ LANÇAMENTO MUNDIAL DE COSMO VMS

A NAUTA lançou recentemente, a nível mundial, o software COSMO VMS. Este "é um sistema de gestão de vídeo, bastante avançado e robusto, que levou vários anos a desenvolver e que iremos comercializar a nível global", disse Carlos Dias, director-geral da NAUTA, disse à Security Magazine durante a conferência Proteger.

Como afirmou, tal como o COSMO, o COSMO VMS "leva-nos para um patamar que, a nível mundial, não tem muitos concorrentes", e, como tal, "permite que os integradores e clientes possam ter uma oferta única e que potencie os sistemas já instalados para um patamar de segurança raramente visto". O software "transforma meros sistemas de segurança num potente sistema que integra desde o ar condicionado, energia, segurança, gestão de pessoas, ocorrências, manutenção e marketing, entre outros, tudo debaixo de uma mesma plataforma, independentemente da marca dos equipamentos instalados". Face ao COSMO, o qual a Security Magazine já teve oportunidade de ver em funcionamento no World of Wine, Carlos Dias explicou que "este é um módulo novo de gestão de vídeo que tem desde as analíticas sobre o que está a ocorrer no momento ou gravado (localmente, na nuvem ou de forma híbrida), inteligência artificial e machine learning".
O responsável da empresa não teve dúvidas em afirmar que a nível mundial apenas três ou quatro empresas conseguiram apresentar uma solução destas.Sendo uma empresa portuguesa, "é fantástico o que a equipa de desenvolvimento do COSMO conseguiu alcançar, com muitos anos de trabalho, persistência e resiliência, permitindo-lhe apresentar estes módulos, onde muitas das funcionalidades são únicas a nível mundial".
Como apontou, "temos tido uma receptividade fantástica por parte dos integradores e verticais, como a banca, retalho e transportes", uma vez que o sistema permite "numa única plataforma ter a gestão de vídeo e analíticas, fundamentais para a gestão do negócio, utilizando já os sistemas instalados e elevando esses sistemas a um outro patamar".
Em relação ao COSMO, Carlos Dias explicou que o software conta com clientes em Portugal, EUA, Dubai, Moçambique, Angola, Espanha, França e Roménia, bem como em Inglaterra, país que utiliza o COSMO para gestão do seu Serviço Nacional de Saúde e onde a empresa detém um centro operacional. Neste momento, a NAUTA continua a investir. "Estamos a recrutar mais pessoas – programadores e BDM, em Portugal", referiu. Relativamente a novas contratações, Fernando Pereira assumiu recentemente a direcção do COSMO. "O Fernando tem muitos anos de experiência de liderar projectos, nomeadamente na Siemens e Motorola, tendo larga experiência na implementação de redes 3G e 4G em Portugal e na Noruega", avançou Carlos Dias. Além disso, "irá trazer uma continuidade, assim como uma nova abordagem na área da indústria, automação, IoT, machine learning e Inteligência Artificial pois esse será o próximo patamar em que estamos a apostar cada vez mais".
Além do lançamento mundial do COSMO VMS, a NAUTA destacou, na Proteger, as mais recentes novidades do seu portfolio. "A Elkron, com o novo sistema integrado, com vídeo porteiro, videovigilância e app gratuita, entre outros e a 2N, maior fabricante mundial de vídeo porteiros e controlo de acessos".•

E-COORDINA LANÇA FERRAMENTA PARA GESTÃO INTEGRADA DE SST

A e-coordina lançou recentemente no mercado português o GeISS, uma ferramenta informática para Gestão Integrada de Segurança e Saúde no Trabalho.

O GeISS destina-se a todas as empresas, com foco especial na indústria, construção civil e obras públicas. João Gonçalves, consultor da e-coordina, avançou à Security Magazine, à margem da conferência Proteger, que "o GeISS tem dois módulos – segurança no trabalho e saúde no trabalho" e, no fundo, permite gerir o departamento de segurança de forma interactiva, adaptando-se às diferentes realidades das empresas.

Ao nível da segurança no trabalho tem como funcionalidades, por exemplo, a avaliação de riscos, avaliação ergonómica e psicossocial. Disponibiliza um portal do colaborador, permite a gestão de EPI, disponibiliza informação sobre formação, prevenção de acidentes, possibilita a planificação de acções preventivas, registo de medições e avaliações sanitárias (iluminância, ruído, poeiras, entre outros), retirada de relatórios e estatísticas de toda a informação inserida, bem como gestão de planos de emergência e medidas de auto-protecção, realização de auditorias e visitas de segurança e, com o uso do telemóvel, a circulação pelos diversos postos de trabalho e realização de registos.

Já no módulo de saúde, **João Gonçalves, consultor da empresa,** destaca a importância da protecção de dados. Este módulo permite fazer a integração com outros utilizadores, nomeadamente com empresas de medicina externa; permite dar permissões de acesso a determinados campos e a criação de um historial clínico; assim como disponibilizar um portal do trabalhador com toda a informação sobre o seu posto de trabalho e empresa.Esta ferramenta possibilita, de forma interactiva, aceder à planta da empresa e navegar pela mesma, identificando todos os postos de trabalho e os riscos associados a esse posto ou a determinada zona. Além disso, cruza-se com todos os sistemas de medidas de auto-protecção, desde a videovigilância, detecção e extinção de incêndios, controlo de acessos por reconhecimento facial, entre outros.


JOÃO GONÇALVES, CONSULTOR DA E-COORDINA PORTUGAL

Como explica **Ana Barreira, directora da e-coordina Portugal**, "o GeISS abrange vários departamentos das empresas e, além disso, a e-coordina desenvolve para a construção civil os mapas, algo obrigatório a ter em obra e a transmitir ao dono de obra".


ANA BARREIRA, DIRECTORA DA E-COORDINA PORTUGAL

A entrada de João Gonçalves na e-coordina acompanha o lançamento do GeISS. "O João foi coordenador de segurança e obra durante mais de 20 anos e, sendo alguém com conhecimentos técnicos, conseguirá fazer uma abordagem às empresas diferente, bem como um enquadramento da importância deste tipo de serviços numa empresa", sublinhou Ana Barreira.

Já para João Gonçalves, "este é um desafio muito aliciante e uma lufada de ar fresco depois de 20 anos ligado ao sector da construção". Tendo trabalhado do outro lado do cliente, João Gonçalves destaca a evolução vivida no sector da construção ao longo dos anos. "Antes tínhamos projectos de construção feitos em 12 meses, onde passavam 20 empresas. Hoje esse mesmo projecto é feito em 6 meses com as mesmas 20 empresas. Ou seja, há uma concentração muito maior de empresas num período muito reduzido, sendo que os recursos são os mesmos, ou até menos, para fazerem o mesmo trabalho. Começa a dar-se prioridade à gestão documental, que é puramente administrativa, e deixa de fazer-se segurança e prevenção de riscos porque os técnicos estão presos à cadeira a compilar documentos e introduzir dados (...)".

Sobre a participação na Proteger 2023, Ana Barreira sublinhou que "é importante estarmos neste evento para continuarmos a nossa rede de contactos e captação de potenciais clientes. Ao mesmo tempo, apercebemo-nos da diferença do trabalho realizado durante estes cinco anos. Hoje, 90% das pessoas já conhecem a e-coordina. Era importante para nós esta validação e, obviamente, darmos a conhecer os novos produtos que temos no mercado", nomeadamente o GeISS e o E-transport.

"Era importante percebermos a nossa própria evolução e imagem ao longo destes anos na área da segurança no trabalho. Sinto que tem sido muito reconfortante e há uma validação do trabalho desenvolvido".•

LISNAVE EMPENHADA COM A SEGURANÇA DOS COLABORADORES

A Lisnave é hoje um dos principais estaleiros navais do mundo. Está localizada na Mitrena, em Setúbal, e faz reparação de navios de até 700.000 toneladas de pórtico, possuindo seis docas secas, as maiores com 450m de comprimento e 75m de boca, oito cais acostáveis com 1400m lineares no total e 1,5 milhões de m2. Aqui trabalham, num dia normal, cerca de 2000 pessoas.

Durante o evento realizado na Lisnave, a que a Security Magazine assistiu, N**uno Santos, administrador-delegado da empresa**, destacou que na Lisnave e na indústria naval no geral há "um ambiente muito perigoso". Aqui há "pessoas e máquinas a partilhar as mesmas vias, muitas cargas suspensas (temos 19 guindastes, um pórtico, dezenas de pontes rolantes e semi pórticos, entre outros) e muitas fontes de energia potencial concentrada (sob forma eléctrica, fluídos sob pressão, peças e fluídos a alta temperatura e cabos em tensão)". Além disso, "há sempre uma grande pressa para entregar os navios, existindo espaço para que se facilite em termos de segurança. Porém, não permitimos que isso aconteça pois, para a Lisnave, a segurança está primeiro e sem ela não se faz o trabalho".Face a esta realidade, há dois anos, a empresa implementou o objectivo de zero acidentes que, "sendo relevante, não é um objectivo atingível num tempo razoável", disse. Com a implementação deste objectivo, a empresa passou a registar todas as ocorrências, tendo visto os números a aumentar. "Parece um contra-senso, agora que estamos implementar uma cultura de segurança mais forte, os indicadores estão a piorar, mas sabemos a causa e não vamos baixar os ombros", sublinhou.

A indústria naval de forma geral tem "milénios", é "muito tradicionalista, com tudo o que tem de bom e mau", sendo que "a cultura de segurança chegou primeiro a outras indústrias e só depois à indústria naval. Temos um longo caminho a percorrer".

"Temos de reforçar a cultura de segurança na Lisnave e estamos a fazer acções nesse sentido", destacou o administrador-delegado. A empresa disponibiliza equipamentos de protecção colectiva e individual a todos os colaboradores e aposta nas acções de formação, sensibilização, verificação constante pelos técnicos de segurança e responsabilização. Hoje "estamos a ser mais duros nesse aspecto e pessoas que não cumpram (regras e normas de segurança) sujeitam-se a processos disciplinares se forem trabalhadores próprios e a verem o cartão de acesso ao estaleiro suspenso ou cancelado se forem subcontratados".

Como apontou o responsável, "a verificação do cumprimento de normas de segurança faz parte da nossa matriz de avaliação de desempenho". A empresa está ainda a implementar um projecto para ter certificação 45001 ainda este ano.

A Lisnave decorre dos estaleiros da antiga CUF, em lisboa. Em 1961 foi constituída como Lisnave, ainda em Lisboa. Depois em 1967 passa para Cacilhas, estaleiro desactivado em 2000. O estaleiro na Mitrena, Setúbal, foi inaugurado em 1974, com o nome de Setenave. Em 1997 a Lisnave passa para Setúbal, abandonando a construção naval e passando a fazer só reparação naval. Hoje tem uma pequena participação pública de 3%, repara em média 100 navios por ano e conta com um volume de negócios de 120 milhões de euros •

JUNGHEINRICH PORTUGAL COMEMORA 25º ANIVERSÁRIO

A Jungheinrich Portugal, subsidiária da multinacional alemã Jungheinrich, comemora 25 anos de actividade no país. No futuro a empresa avança que "continuará a apostar no desenvolvimento de soluções de última geração de forma a dar resposta às necessidades da intralogística".

Mário Reis assumiu o cargo de managing director da Jungheinrich Portugal há dois anos. Ser o primeiro português à frente desta organização é para Mário Reis "desafiante", adianta à Security Magazine. Porém destaca a importância da equipa, a qual "tem sido extraordinária e ajudou-me a trilhar este caminho. Sem eles nada disto seria possível".

"Celebrar 25 anos é um motivo de grande orgulho e alegria. Orgulho por que vemos o resultado do nosso trabalho e esforço durante todos estes anos. Alegria por podermos contar com a ajuda de tantos Clientes e Parceiros, que acreditaram em nós, que aprofundaram as relações e que nos desafiaram a fazer mais e melhor", adianta.

Quantos aos próximos 25 anos, aponta que a empresa "tem uma perspectiva de crescer de forma contínua, a qual faz parte do nosso conceito de sustentabilidade. Quanto maior o crescimento mais capacidade há para se investir na própria empresa, no desenvolvimento, nos colaboradores e no seu desenvolvimento e capacitações".

O grupo Jungheinrich aposta numa política de proximidade com o mercado, sendo a Jungheinrich Portugal uma das 42 filiais próprias do grupo. O mercado português é dinâmico, apresenta um crescimento positivo e tem um potencial futuro, pelo que continuará a ser um país estratégico para o grupo alemão.

"Graças à sua estrutura sólida e apesar das interrupções nas cadeias de abastecimento globais que se desenvolveram no início da pandemia de coronavírus e, posteriormente, agravadas em 2022 pela guerra Rússia-Ucrânia, a Jungheinrich conseguiu manter, graças a uma gestão eficaz dos fornecedores, a produção e a entrega dos seus equipamentos em Portugal".

Para acompanhar o aumento do seu volume de negócios, a Jungheinrich Portugal fez diversos investimentos ao nível das suas infraestruturas. Em 2015 inaugurou as instalações da sua sede em Mem Martins, com uma área de 4 mil m2, num total de 700 mil euros. Já em 2018, mudou a delegação do norte do Mindelo para a zona industrial da Maia, para um espaço de 650 metros quadrados estrategicamente localizado pela proximidade do Aeroporto Internacional do Porto e do Porto de Leixões. Simultaneamente, tem investido de forma contínua no alargamento da frota de aluguer e de usados, em equipamentos inovadores, na diversificação de serviços, na contratação de novos colaboradores e na formação da sua equipa.

No que diz respeito à tecnologia, a Jungheinrich tem conseguido dar resposta às necessidades das empresas no mercado nacional, naquilo que são as tendências do sector: digitalização; automação e conectividade, de forma a optimizar os fluxos de materiais e processos de trabalho na área da intralogística. Continua também empenhada no desenvolvimento de soluções ambien-

talmente sustentáveis, tendo reduzido em mais de 25% as emissões de CO2 em toda a sua gama de produtos. Nesse sentido, e com os olhos postos no futuro, a empresa tem respondido ao mercado com soluções exclusivamente eléctricas. Na última década, a Jungheinrich apostou grandemente na criação de uma solução integrada de equipamento com bateria e carregador desenvolvidos em conjunto e que garante um maior aproveitamento energético e sustentabilidade. É exemplo, a linha Jungheinrich PowerLine com empilhadores exclusivos para tecnologia de iões de lítio. Estes equipamentos são mais compactos, ágeis e ergonómicos. Responsável pela introdução, em Portugal, das baterias de iões de lítio (Li-Ion), a Jungheinrich Portugal disponibiliza desde 2019 a venda de equipamentos usados com esta tecnologia. Para prestar um serviço de assistência de excelência lançou ainda no ano passado as carrinhas do serviço pós-venda "Energy-Van", dedicadas à reparação de baterias de equipamentos de movimentação de carga, com forte enfoque na tecnologia de Li-Ion.
Também a automação tem sido uma prioridade quer na movimentação quer no armazenamento de cargas, até como forma de colmatar a falta de mão de obra e a necessidade consequente de soluções mais sustentáveis mesmo do ponto de vista social da empregabilidade e a necessidade de implementar uma melhor gestão de stocks.
O uso de veículos autónomos como AGV e AMR será cada vez mais generalizado.
O recondicionamento de equipamentos sempre foi uma área de negócio importante e que terá um crescimento nos próximos anos. É uma forma reconhecida de reduzir efeitos de emissões de gazes como também de preservar para o futuro recursos importantes e estimular uma economia circular. Os equipamentos recondicionados da Jungheinrich mantêm os padrões de qualidade do equipamento, com utilização dos materiais e peças correctos para o efeito no sentido de proporcionar a boa manutenção, segurança e performance para a utilização duradoura do equipamento.
Também a segurança tem sido uma prioridade, com o continuo desenvolvimento de equipamentos mais seguros e ergonómicos. A par de sistemas de segurança adaptados, a Jungheinrich desenvolveu o conceito de consultoria e aconselhamento de protecção de 360 graus que permite abranger as cinco áreas de perigo no armazém: pessoas; mercadorias; equipamentos de armazenamento; máquinas e dados.
O leque de serviços é vasto para uma boa adaptação aos requisitos e operação de cada cliente em particular.
Destaque para o serviço de peças Jungheinrich online em que via website é possível a qualquer hora realizar a encomenda de uma peça de reposição e para uma disponibilização da mesma em 24 horas. As peças de reparação são entregues de um dia para o outro directamente nas carrinhas dos Técnicos. Naturalmente todos os serviços de manutenção preventiva e correctiva são modulares e disponíveis para os clientes, incluindo as verificações de segurança. A gestão dos pedidos de assistência é feita por uma Equipa que funciona num sistema de call center.
Os serviços digitais têm conhecido um interesse cada vez maior, como a aplicação Call4Service em que o cliente pode aceder a partir de qualquer dispositivo a uma comunicação com assistência técnica Jungheinrich.
Quanto ao aluguer de equipamentos, a Jungheinrich Portugal reforçou a sua frota disponível, como resultado do aumento da procura gerado pela pandemia.
O aluguer apresenta-se como uma solução para combater a descapitalização, mantendo a flexibilidade necessária para efetuar os ajustes necessários à manutenção das necessidades financeiras das empresas. •

"O NOSSO OBJECTIVO É DIFUNDIR A CULTURA DE SEGURANÇA"

A Proteger 2023 decorreu em Santa Maria da Feira, numa organização da Associação Portuguesa de Segurança (APSEI). A Security Magazine associou-se ao evento como media partner.

À Security Magazine, **Carlos Dias, presidente da APSEI**, destacou que a ida para a região Norte resulta dos objectivos traçados pela actual direcção, bem como dos pedidos feitos pelos associados e pelo mercado. A aposta no Norte é para manter, segundo sublinhou, podendo decorrer noutras cidades tanto no Norte como no Sul, numa periodicidade anual. A próxima edição da Proteger decorre em Lisboa em 2024.
"O principal deste evento são as conferências e as áreas temáticas e técnicas, as quais são a parte básica da APSEI e da Proteger", disse. Apesar de a área de exposição ter forte destaque no evento, Carlos Dias sublinhou que esta é "complementar" à conferência, onde a organização procura "dar visibilidade ao que mais moderno se faz nalgumas das principais valências da APSEI, nomeadamente, segurança electrónica e protecção passiva e activa, bem como de alguns parceiros institucionais".
Como apontou, as quatro áreas mais focadas nas conferências – transporte mercadorias perigosas, segurança electrónica, segurança activa e passiva e segurança e saúde no trabalho – estiveram representadas por "empresas de referência". O presidente da APSEI, destacou que "a Proteger é uma conferência" e como associação de segurança, "o nosso objectivo é difundir a cultura de segurança em Portugal".
Com este objectivo presente, a associação tem a decorrer o projecto Segurança 4.0, co-financiado pelo Portugal 2020, que visa a capacitação digital da APSEI e dos associados para permitir mais ferramentas digitais. "No mercado da segurança, quem procura mais informação procura-a em formato digital, e a APSEI não tinha informação disponível, nem no seu site ou a quem a quisesse buscar, por isso tivemos de adaptar o site e criar o Observatório Nacional da Segurança, que é permanentemente actualizado com tudo o que tem a ver com os vários sectores da segurança", esclareceu.
Já no caso do projecto Portugal Safe, também co-financiado e desenvolvido pela associação, visa a internacionalização da própria APSEI e também a melhoria da imagem do sector fora de Portugal, criando oportunidades de negócio aos associados. "Temos criado oportunidades vivas e hoje (primeiro dia do evento) assinamos protocolos com o mercado de Marrocos, Emirados Sharjah e Dubai, que nos abre o mercado da Arábia Saudita". Estes protocolos foram celebrados com câmaras de comércio, universidades, nomeadamente de Casablanca, institutos politécnicos e organizações.Como adiantou, "o mercado de Marrocos está a uma hora de Lisboa e tem necessidades de segurança muito

CARLOS DIAS, PRESIDENTE DA APSEI

grandes, estando em construção 8 milhões de m2 de hospitais, centros comerciais e áreas públicas. Ou seja, há imensas oportunidades para as empresas portuguesas".

O mesmo se aplica nos Emirados Árabes Unidos e a Arábia Saudita. "Como associação temos de criar oportunidades de riqueza para os associados (...). Se os associados tiverem maior capacidade financeira, conseguem fazer melhores investimentos, pagar melhores ordenados e criar condições diferentes para os seus colaboradores. Esse é um dos objectivos da associação e desta direcção".

Na liderança da APSEI durante a pandemia, estando actualmente no seu segundo mandato, Carlos Dias destacou a importância da associação durante esse período de "desafios incríveis".

O responsável destacou o papel da associação durante a "crise das máscaras", a qual disse, ter sido "provocada artificialmente".

Durante esse período, "a APSEI interveio junto das entidades para que isso não acontecesse", relembrou. O responsável recordou também a situação vivida no transporte de matérias perigosas, como os combustíveis, quando não poderia haver renovações de licenças situação que poderia levar à paralisação do país. Acontecimento no qual "a APSEI teve um papel fundamental" pois, acima de tudo, "tem de fazer o seu papel de ajudar o país".

Sobre os actuais desafios, Carlos Dias referiu que "apesar de haver várias vozes discordantes, nomeadamente por haver uma Proteger no Norte, a resposta está dada" e os números falam por si. "O futuro é para continuar", disse, pois, acima de tudo "trabalhamos para o bem dos associados".

ALGUNS DEPOIMENTOS

Além das conferências que decorreram ao longo dos dois dias sobre temas variados, a área de exposição contou com a presença de algumas das principais empresas na área. À Security Magazine falou com alguns expositores sobre a sua opinião sobre esta edição da Proteger e as novidades apresentadas ao mercado..

Ana Barreira, responsável da e-coordina Portugal, destacou a importância da participação pela segunda vez na Proteger. A responsável destacou a relevância do evento para a captação de novos contactos e a validação do mercado relativamente ao trabalho desenvolvido pela empresa nos últimos cinco anos. Em termos de novidades, a empresa lançou o novo módulo e-transport e o GEISS destinado ao mercado de SST (ver artigo).

Carlos Dias, enquando representante da Nauta destacou a importância da Proteger. "É a única conferência e exposição de segurança para profissionais em Portugal", sendo que "a Nauta como lídeer de mercado teria de estar presente". O responsável destacou que num único espaço, durante dois dias, foi possível contactar centenas de clientes.

Em termos de novidades, a empresa apresentou o novo software COSMO VMS (ver artigo).

Ricardo Pereira, da Axis Communications, destacou que a empresa apresentou uma renovação quase integral do portfolio em termos de chipset, com vista a ter analíticas deep learning directamente na câmara. Essa é uma das grandes apostas da equipa de gestão de produto, ou seja, colocar toda a analítica e inteligência no extremo e ao mesmo tempo tornar o produto mais eficiente do ponto de vista energético.

As evoluções têm como foco principal baixar o consumo poe de todos os equipamentos. o responsável destacou a nova câmara com radar, com a composição de câmara e radar onde o objectivo é fazer uma protecção perimetral dos dois algorítmos para confirmação da detecção e redução de falsos positivos. A empresa apresentou ainda novos produtos na área do áudio, associado ao vídeo, analítica de vídeo, controlo de processos, protecção de pessoas e análise perimetral.

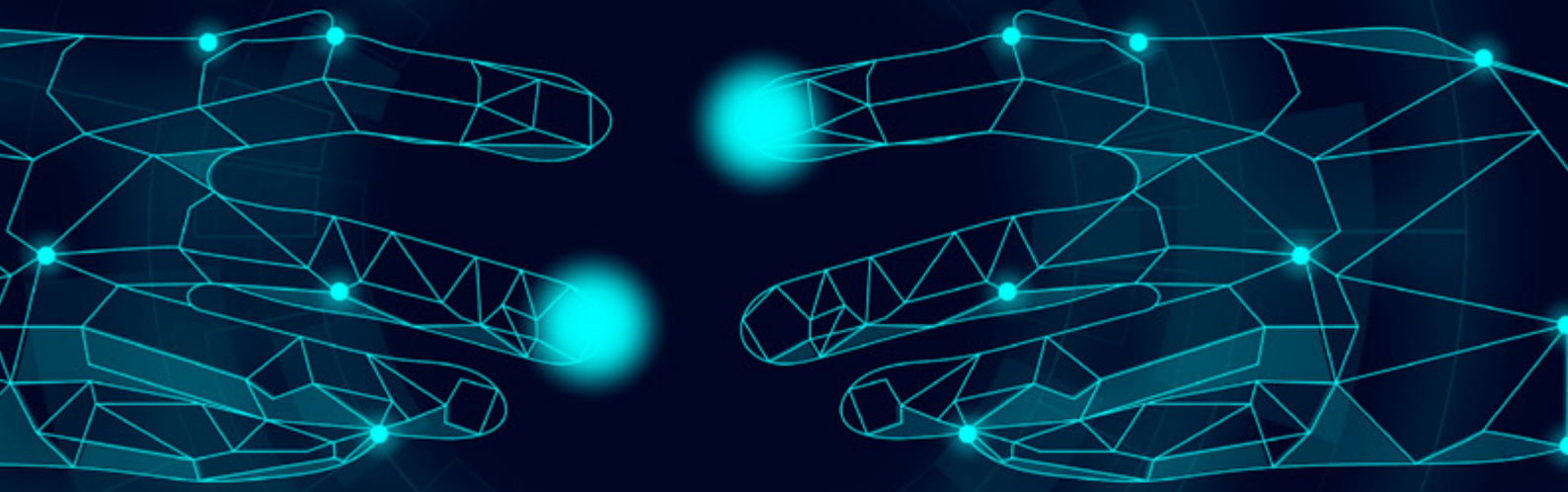
David Sardinha, da Hikvision Portugal, destacou a importância de participar na proteger, que é "muito mais do que uma feira, com uma componetne muito profissional".

Em termos de novidades, a empresa apresentou os videowalls, muito relacionados com as centrais de gestão e de segurança.

A empresa apresentou pela primeira vez barreira físicas (tourniquetes), controlo de acessos com controlo facial e focou-se também na analítica de vídeo ligada ao retalho, com mapas de calor, com identificação de género e faixa etária das pessoas.

A Proteger regressa no próximo ano a Lisboa. •

SECURITY MAGAZINE
REVISTA DOS PROFISSIONAIS DE SEGURANÇA



SECURITY MEETUP

CONVERSAS SOBRE SEGURANÇA

LISBOA

+ INFO: GERAL@SECURITYMAGAZINE.PT