Bruno Castro, VisionWare: «Os níveis de maturidade de cibersegurança variam de organização para organização, mas o factor humano é normalmente a maior fragilidade»

hrportugal.sapo.pt/bruno-castro-visionware-os-niveis-de-maturidade-de-ciberseguranca-variam-de-organizacao-para-organizacao-mas-o-factor-humano-e-normalmente-a-maior-fragilidade

October 2, 2023

Segundo dados do DarkFeed/DeepWeb Intelligence Feed, 2023 Top Targeted Countries, Portugal está na mira da comunidade cibercriminosa. Para Bruno Castro, Fundador & CEO da VisionWare, e especialista em Cibersegurança e Análise Forense, mais do que literacia digital, as empresas devem apostar na literacia em cibersegurança, independentemente da função ou cargo dos colaboradores.

Por Tânia Reis

Nasceu de um sonho de adolescência e, actualmente, é uma das grandes referências globais, no âmbito da Segurança da Informação. A comprová-lo está a recente distinção ouro na categoria Cibersegurança, dos Selos de Maturidade Digital (SMD), tendo sido a primeira tecnológica a alcançar tal feito.

Como nasce a VisionWare?

A VisionWare foi idealizada por mim, há muitos anos, ainda eu era um adolescente, no sentido de poder vir a criar um projecto empresarial orientado unicamente para o tema da cibersegurança. A empresa acaba por ser fundada em 2005, no meio de uma crise, onde tudo indicaria que não seria o melhor momento para aventuras empresariais, contudo, essencialmente devido à coragem dos seus fundadores, à adopção de uma estratégia de especialização numa única área – cibersegurança – e com alguma dose de loucura à mistura, assumimos como nosso playground a geografia internacional.

Actualmente, operamos em modo worldwide, detemos mais de 200 clientes activos, e em 2022, a facturação rondou os 4M€, contando à data de hoje com perto de 100 colaboradores (entre os escritórios de Porto e Lisboa, cidade da Praia, em Cabo Verde). De salientar também outro dado relevante, desde 2020 até ao presente, a VisionWare aumentou o número de colaboradores do sexo feminino em 27%, representando agora 36% do total dos seus recursos humanos. Fruto de uma aposta na contratação e retenção de talento feminino, orgulhamo-nos de ter 26% dos cargos de liderança e gestão ocupados por mulheres.

E qual é a sua missão?

A nossa missão é contribuir para o sucesso dos clientes, aumentando a sua cultura e maturidade digital em matéria de Segurança da Informação. Sinto orgulho em dizer que foi uma empresa pioneira em 2005 e somos actualmente uma das grandes referências globais, no que se refere à actividade no âmbito específico da Segurança da Informação.

A VisionWare ultrapassou fronteiras e hoje, está presente em diferentes geografias tendo alcançado dimensão mundial através dos seus inúmeros projectos de relevo, seja em solo-mode ou joint-ventures internacionais. Temos conquistado a confiança dos clientes nacionais e internacionais, e o reconhecimento da comunidade e das principais entidades reguladoras do sector. O nosso foco passa sempre por zelar pelo bem mais precioso das organizações – a sua informação – auxiliando e orientando diariamente as melhores práticas que visam mitigar riscos desnecessários e criar um ambiente de negócio mais seguro.

Porquê o foco na segurança de informação?

Desde a génese da VisionWare, sempre foi evidente que, para promovermos a maturidade na segurança da informação, esta deveria ser abordada de uma forma holística. Neste sentido, a partir de 2016, e depois de uma década de experiência acumulada, a garantir que as áreas centrais – cibersegurança, compliance e investigação forense – estavam devidamente consolidadas, avançámos para o desenvolvimento e implementação de áreas independentes e complementares como a privacidade, a inteligência e a 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.

A VisionWare actua em toda a componente de Segurança da Informação, e disponibiliza serviços especializados em todas as matérias que envolvam a “disciplina mãe”. Podemos evidenciar a área de cibersegurança e compliance nos vários normativos e regulamentos aplicados pela UE ou pelo sector, privacy & legal (incluindo os serviços de encarregado de protecção de dados pessoais, implementação de RGPC e respectivos canais de denúncia/whistleblowing, avaliação de risco e conformidade, gestão de incidentes de violação de dados, entre outros), SOC (Security Operations Center) & CSIRT (Computer Security Incidente Response Team), investigação forense, Professional Services e VisionWare Academy (serviços de formação). Ainda, e como unidade mais recente, disponibiliza serviços de Strategic Intelligence & Risk Analysis, isto é, análise estratégica de contexto sociopolítico, geopolítico, legal e securitário; classificação de risco social, sanitário, político e securitário; formação para a capacitação de tomada de decisão em contexto de risco e criticidade; e ainda, acompanhamento digital de ativos críticos e análise reputacional em ambiente OSINT (Open Source Intelligence).

Como analisa a realidade portuguesa? Estamos no bom caminho ou a ficar para trás?

Portugal está no top 10 dos países que mais sofreram ataques ransomware só no primeiro mês de 2023, facto que não marcou de forma positiva o arranque deste ano na perspectiva da segurança de informação. De acordo com dados divulgados através do DarkFeed/DeepWeb Intelligence Feed, 2023 Top Targeted Countries, em Fevereiro alertámos precisamente para o facto de o país estar em 7.º lugar, numa altura em que se assinalou o ciberataque à Vodafone.

Para precaver os perigos desta tendência mundial em crescimento, e pelo facto de Portugal estar na mira da comunidade cibercriminosa, a VisionWare lançou no final do ano passado o centro pioneiro de operações e análise a ameaças cibernéticas à escala mundial, denominado VisionWare Threat Intelligence Center. Este novo centro desenvolve-se em consonância com o apelo do Governo para uma maior atenção da sociedade civil face ao perigo iminente das novas ameaças e riscos globais. Para nós, os ataques cibernéticos são as novas armas usadas contra a segurança como um todo, para atacar infraestruturas críticas nas sociedades e colocar em causa a estabilidade de uma nação. A criação deste novo serviço, altamente inovador, permite agregar especialistas que, através de um modelo sólido de análise em tempo real, respondem às necessidades dos clientes e parceiros, em Portugal, mas também pelo mundo.

A aposta terá de ser sempre pela via da crescente literacia de todos os cidadãos, independentemente da sua função/cargo, visto que, qualquer um 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.

Os níveis de segurança da informação dependem de vários factores, como o sector, a dimensão da empresa e até o orçamento disponível. Quais os "requisitos mínimos" que qualquer negócio deve cumprir?

Nestes últimos quase 20 anos de VisionWare, nunca tivemos tantas solicitações de ajuda para responder e investigar 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 de 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 de ser formadas para responder 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.

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 agora 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 infraestruturas, e sobretudo, "stressar" constantemente os sistemas, procurando falhas e fragilidades, corrigindo-as de forma perseverante, de modo a "blindar" a organização contra quaisquer eventuais tentativas de (ciber) ataques. Em simultâneo, e através de tecnologia, procedimentos, mas também através de testes de stress, testar vezes sem conta a nossa capacidade de recuperação a um incidente de segurança que possa implicar desastre global na organização. O conhecer a nossa capacidade de recuperação a um ciberataque é fundamental para a gestão de uma organização nos dias de hoje.

Desenvolvem projectos com clientes internacionais. Que diferenças encontra nessas geografias comparativamente a Portugal?

Não vejo assim nenhuma grande diferença ao nível da exposição do risco. Os ataques que temos em Portugal, existem em Cabo Verde, Espanha ou Bélgica, por exemplo. Não nos podemos esquecer que o cibercrime é global, não é regional. É tipicamente feito por sectores de actividade.

Das várias áreas onde actuam – cibersegurança, compliance, privacidade, etc.– qual considera ser mais crítica e urgente no tecido empresarial português?

Todas estas áreas de actuação querem-se complementares e convergentes, e todas elas estão interrelacionadas para "blindar" os sistemas de segurança da informação de uma organização, empresa, entidade, etc. Contudo, se tivesse de eleger apenas uma, e pensando especificamente no tecido empresarial português e no conjunto das nossas PME, actualmente existem uma série de obrigações e a necessidade do cumprimento de directivas nacionais e europeias inerentes à implementação e gestão dos canais de denúncia/lei Whistleblowing – obrigatórios para todo o tipo de empresas, públicas ou privadas, com 50 ou mais colaboradores – a qual acredito que não esteja a ser cumprida e executada na íntegra pela grande maioria destas empresas.

Sabemos que existem muitas empresas que já "compraram" um software para a implementação destes canais de denúncia nas suas respectivas organizações, contudo, essa gestão obriga ao cumprimento não apenas da "aquisição" desse software como também efectuar a gestão e implementação de algumas medidas, nomeadamente, no que diz respeito à elaboração de programa de cumprimento normativo, à adopção e implementação com muito maior envolvimento e esforço do que a instalação de um "mero" software em formato de "vacina mágica". É precisamente contra este tipo de abordagens que a VisionWare se posiciona no mercado. Temos de adoptar, sempre que necessário, a tecnologia disponível na medida (apenas) das necessidades e acoplar os serviços e experiência para cumprir adequadamente o que realmente se pretende para a dita organização.

Quais considera que vão ser os grandes desafios futuros na área da informação?

Teremos grandes desafios decorrentes essencialmente de três vertentes: 1) ciber resiliência, 2) protecção e 3) privacidade de dados.

Em termos de futuro, no que diz respeito à VisionWare, continuamos precisamente com a mesma irrequietude que tínhamos em 2005, mas mais maduros e consistentes. Queremos crescer mais, ser a principal referência no sector da segurança de informação, e operar worldwide, com abordagens e soluções sempre na vanguarda inovadora deste desafiante mercado da cibersegurança.