Portugal no top dos 10 países que mais sofreram ataques ransomware no primeiro mês deste ano

forbespt.com/portugal-no-top-dos-10-paises-que-mais-sofreram-ataques-ransomware-no-primeiro-mes-deste-ano

Helena C. Peralta 5 de maio de 2023

Bruno Castro é CEO da VisionWare, empresa de cibersegurança por ele fundada em 2005. Licenciado em Engenharia Eletrotécnica e mestre em Engenharia Informática é especialista em temas como a segurança da informação, cibersegurança e investigação forense. Está credenciado em NATO-SECRET e EU-SECRET, e faz parte do grupo de auditores de segurança credenciado pelo Gabinete Nacional de Segurança, sendo ainda membro da European Society of Criminology.

Com cerca de 100 colaboradores e uma faturação a rondar os 4 milhões de euros, a empresa apostou o ano passado no lançamento de um centro pioneiro de operações e análise a ameaças cibernéticas à escala mundial,denominado VisionWare Threat Intelligence Center. Cerca de 34% dos seus colaboradores são mulheres e 26% dos cargos de liderança e gestão são também no feminino. Alerta que Portugal está no sétimo lugar dos países que mais sofrem ataques de *ransomware*.

Como e quando surgiu a VisionWare e qual era vossa principal missão quando arrancaram o negócio?

A VisionWare foi idealizada por mim, há muitos anos, ainda adolescente, com a ideia de poder vir a criar um projeto empresarial orientado unicamente à cibersegurança. Julgava eu, nos anos 90, que talvez fosse um projeto inovador, diria que "fora-da-caixa" e que, provavelmente, até poderia vir a dar para me pagar as contas no final do mês. Afinal até tinha razão. A VisionWare acaba por ser criada em 2005, no meio de uma crise, quando tudo indicaria que não seria o melhor momento para aventuras empresariais. Contudo, e essencialmente devido à coragem dos seus fundadores, à adoção de uma estratégia de especialização numa única disciplina e com alguma dose de loucura à mistura, adotámos o nosso *playground* à geografia internacional. É assim que a VisionWare, 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 nos exige.

Mais concretamente, em que áreas atua e qual a sua dimensão no mercado?

A VisionWare atua em toda a componente de segurança da informação. Podemos destacar a área de cibersegurança, *compliance* nos vários normativos e regulamentos, *privacy & legal*, incluindo os serviços de encarregado de proteção de dados pessoais, implementação de RGPC e respetivos canais de denúncia/*whistleblowing*, entre outros, SOC (Security Operations Center) & CSIRT (*Computer Security Incidente Response Team*), investigação forense, e ainda serviços de formação. Também 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 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*).

A VisionWare opera em todo o mundo. Detém mais de 200 clientes ativos, e em 2022, a empresa apresentou uma faturação a rondar os 4 milhões de euros, contando com perto de 100 colaboradores, nos escritórios de Porto e Lisboa, e em Cabo Verde, na cidade da Praia. Saliento que, desde 2020, aumentou o número de colaboradores do sexo feminino representando agora 36% do total dos seus recursos humanos, sendo que 26% dos cargos de liderança e gestão são ocupados por mulheres.

> A VisionWare opera em todo o mundo, detém mais de 200 clientes ativos, conta com perto de 100 colaboradores, nos escritórios de Porto e Lisboa, e na cidade da Praia, em Cabo Verde.

Como se deu o vosso crescimento a partir de 2005?

Em 2006 expandimos os nossos 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 nosso primeiro projeto em Cabo Verde, lançando a nossa presença nos PALOP, a qual se mantém sólida até hoje. Desde a sua génese, sempre foi evidente que, para promover a maturidade na segurança da informação, esta deveria ser abordada de uma forma holística. Neste sentido, a partir

de 2016, a VisionWare avançou para o desenvolvimento e implementação de áreas independentes e complementares. São exemplo 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. Com o aumento da cibercriminalidade, a VisionWare cresceu bastante.

Que projectos vos distinguem da concorrência?

No ano passado, a VisionWare lançou um centro pioneiro de operações e análise a ameaças cibernéticas à escala mundial**,** denominadoVisionWare Threat Intelligence Center. Este projeto surge em linha com a promulgação da Estratégia Nacional de Ciberdefesa, anunciado pelo Governo português, e conta com especialistas das áreas de *intelligence* e cibersegurança, de três continentes, onde a VisionWare detém operação comercial, e que efetuam a monitorização, análise e *repor*t urgente, em tempo real, para responder aos novos desafios e ciberameaças à segurança das instituições públicas e privadas. O objetivo desta 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 e combatê-las. 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. Produzirá relatórios geopolíticos relacionados com as ameaças em estudo, monitorização de atores 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, divididos por tempo e setor de risco. Como próximo passo, torna-se fundamental capacitar as autoridades de ferramentas e conhecimento para o constante controlo e monitorização da deepweb/darkweb, análise de riscos de cibersegurança das infraestruturas críticas, *profiling* de determinados indivíduos através de técnicas de *humint,* deteção e defesa de ciberataques e monitorização e supervisão contínua de determinados grupos cibercriminosos.

> A VisionWare assume-se como uma empresa de capital 100% português, referência internacional na área da segurança de informação.

Quais são os vossos objetivos a médio e longo prazo?

A VisionWare continua em franco crescimento, até pela própria conjuntura do mercado. Queremos manter o nosso nível de crescimento, apostando no desenvolvimento contínuo de serviços inovadores na disciplina de segurança, mas garantindo simultaneamente a sustentabilidade financeira da empresa. Este ano a VisionWare abriu o seu serviço de *Security Operation Center* (SOC) ao mercado internacional. Este serviço tem como objetivo implementar uma "guarda inteligente", com total abrangência, em modelo permanente, 24 horas dia, 7 dias por semana, à totalidade da infraestrutura digital da organização. Através do incremento contínuo do nosso volume de negócio internacional, conseguimos também formalizar uma operação fixa em África – através de Cabo Verde – e na Europa – junto da Comissão Europeia, em projetos essencialmente de Investigação e Desenvolvimento, na vertente de segurança e privacidade.

Como se posiciona o mercado nacional no tema da cibersegurança comparativamente com outros países da Europa?

Portugal está no top 10 dos países que mais sofreram ataques *ransomware* no primeiro mês de 2023, facto que não marca positivamente o início do ano na perspetiva da segurança de informação. Este alerta foi precisamente lançado pela VisionWare, de acordo com dados divulgados através do DarkFeed/DeepWeb Intelligence Feed, 2023 Top Targeted Countries, January 2023. Estes mostram que o país ficou em 7º lugar, numa altura em que assinalámos há relativamente pouco tempo, o grave ciberataque infligido à Vodafone.

> Vivemos tempos muito desafiantes no campo da inovação da segurança cibernética, quando a nossa aliada inteligência artificial acaba por se revelar a principal inimiga de quem nos protege.

Os ciberataques de *ransomware* continuam em ascensão, transformando-se numa força disruptiva no setor de segurança cibernética, afetando todas as áreas de atividade. Devido ao incremento do trabalho remoto, motivado e acelerado pela pandemia, estima-se que estes ataques tenham aumentado 148% em todo o mundo. O *ransomware* constitui por isso, uma ameaça visível para milhares de organizações e empresas, inclusive em Portugal, quando comparada com a tendência noutros países europeus. Os protagonistas deste tipo de ciberataques sabem que o seu modelo de negócio, altamente destrutivo, terá garantia de sucesso contínuo, desde que consigam inovar as suas técnicas de exploração e formatos de dispersão dentro da organização.

Parece-me cada vez mais evidente que a ameaça representada pelos cibercriminosos está a crescer e que é necessário fazer mais para prevenir acontecimentos futuros. Como tal, Portugal precisa de continuar a reforçar as suas infraestruturas de cibersegurança e a desenvolver estratégias eficazes para proteger os seus cidadãos, empresas e infraestruturas contra o número crescente de ciberataques, oriundos de redes criminosas diversas, cada vez mais bem organizadas e com uma maior capacidade disruptiva.

Onde estamos a falhar e no que poderíamos melhorar? O que pode o Estado fazer para melhorar situações como esta?

Temos assistido a uma intensificação e sofisticação de ciberataques na sociedade portuguesa. Estes ataques, transversais a quase todos os principais setores da nossa sociedade têm causado muita turbulência, visto que, em certos casos, também tem implicado um impacto direto para o *core* business das "vítimas'". 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. Face a isto as autoridades não dispõem de recursos necessários para responder a todas as solicitações. Para além de mais ataques, e com maior taxa de sucesso, estes são também cada vez mais complexos e sofisticados, e, portanto, obrigam a um esforço muito superior no processo de investigação. As autoridades competentes estão perante um enorme desafio, que, para além da capacidade de resposta, ainda se prende com o binómio técnico versus *know-how* especializado.

> A velocidade com que os hackers adotaram o programa ChatGPT foi alarmante: foi lançado em novembro de 2022 e as evidências de *scripts* de *malware* apareceram apenas um mês depois.

A aposta terá de ser sempre pela via da crescente literacia de todos os cidadãos, visto que, qualquer um poderá ser vítima de um ataque malicioso ou fraudulento. O fator 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 as instituições deverão ser os primeiros a preconizar e implementar medidas de segurança diárias com vista ao cumprimento de uma maior segurança cibernética. O 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 aproveitá-lo. Deve ser instituído 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 adotar, comunicação à CNPD e informação aos demais titulares dos dados.

Como estão as empresas portuguesas a lidar com o tema da cibersegurança? As lideranças estão mais preocupadas e atentas?

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 e com elevado grau de sucesso, estão tipicamente focados no roubo de dinheiro ou de dados "valiosos", resultando de múltiplos fatores 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. Após uma cobertura mediática e crescente consciencialização sobre este tema, acabam por ser visíveis alguns resultados e mudanças urgentes de mentalidade, ainda que, insuficientes. Na VisionWare, temos vindo a registar um número avultado de solicitações de empresas que começam agora 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.

Tecnologias como a Internet das Coisas, a Inteligência Artificial (IA), a Computação Quântica e o 5G trazem oportunidades, mas também riscos. O que é fundamental fazer para minimizá-los?

A Inteligência Artificial é um dos campos de desenvolvimento tecnológico mais importantes da atualidade. Pode ser aplicada para melhorar a qualidade de vida de todos os seres humanos e pode ser também utilizada para ajudar na redução da criminalidade, aumentando a segurança pública. Contudo, face ao desenvolvimento atual que temos assistido levanta-nos sérios dilemas. Não só éticos e morais, mas também securitários. Veja-se que, recentemente, mais de mil 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 Inteligência Artificial". Os signatários argumentam que é necessária esta pausa para que "os potenciais riscos à segurança sejam estudados e controlados".

Um relatório recente da Europol, a polícia da União Europeia, fez um alerta sobre os riscos representados por estas novas tecnologias. De acordo com este estudo, as redes de telecomunicações de quinta geração (5G), a criptografia quântica e a inteligência artificial, se forem parar "às mãos erradas", podem dificultar bastante o trabalho de investigação dos agentes das forças de segurança. Não basta ser reativo para enfrentar tão grande

evolução na tecnologia e na criminalidade; para continuar relevante, a polícia precisa prever quais, entre as tecnologias emergentes, serão as efetivas armas de escolha dos cibercriminosos.

O 5G será assim 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 os sistemas de ciberataques, como aqueles que distribuem vírus e *phishing*.

> Não existem fórmulas mágicas ou uma vacina milagrosa contra ciberataques.

Como vê os perigos associados ao desenvolvimento do ChatGPT?

A emergência da tecnologia da IA foi sempre recebida com um certo ceticismo e incerteza, e não é difícil perceber porquê. Embora tornando as nossas vidas muito mais fáceis em muitos aspetos, pode ter consequências terríveis para o futuro da cibersegurança – daí a existência do *malware* ChatGPT. Falo sobre os riscos da utilização do ChatGPT e sobre como 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. Muitas redes subterrâneas na *dark web* 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. Vários utilizadores do ChatGPT alertaram anteriormente para o facto do programa poder codificar um *malware* capaz de espionar as teclas digitadas pelo utilizador ou que poderia ser utilizado para criar *ransomware*. Os termos de serviço da OpenAI proíbem especificamente o uso do programa ChatGPT para criar qualquer tipo de *malware*, mas, embora o programa forneça todos esses avisos, muitas pessoas conseguiram contorná-los quando avançaram para a criação de *malware*. A velocidade com que os hackers adotaram o programa foi alarmante por si só – com o programa lançado em novembro de 2022 e evidências de *scripts* de *malware* aparecendo apenas um mês após este lançamento.

Por todos estes motivos, parece-me evidente que vivemos tempos muito desafiantes no campo da inovação da segurança cibernética, quando a nossa aliada inteligência artificial acaba por se revelar a principal inimiga de quem nos protege.

É possível ter organizações à prova de ciberataques ou isso é apenas uma utopia?

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. É necessário prevenir 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 ataques. Em simultâneo, e através de tecnologia, procedimentos, mas também através de testes de stress, deve testar-se vezes sem conta a nossa capacidade de recuperação a um incidente de segurança que possa implicar desastre global na organização.

Conhecer a nossa capacidade de recuperação a um ciberataque é fundamental para a gestão de uma organização nos dias de hoje.