“Nunca tivemos tantas solicitações de ajuda para responder e investigar ciberataques como agora”

linktoleaders.com/nunca-tivemos-tantas-solicitacoes-de-ajuda-para-responder-e-investigar-ciberataques-como-agora-visionware-bruno-castro

Link To Leaders 9 de dezembro de 2020

> “Algumas empresas, infelizmente, só investem depois de serem vítimas de um primeiro ciberataque. Mas já há algum tempo, a cibersegurança começa a ser vista como um investimento não só positivo como necessário”. A afirmação é de Bruno Castro, CEO da VisionWare, que em entrevista ao Link To Leaders alertou para o facto de o “ambiente de teletrabalho promover um certo descuido face às medidas de segurança”, e para a necessidade de haver “literacia em cibersegurança”.

Desde 2005, ano em que foi criada, que os temas da cibersegurança fazem parte do ADN da VisionWare. A empresa desenvolve projetos de elevada complexidade, e conta com uma base de clientes sólida no setor público e privado em áreas como a indústria, saúde, banca e finanças, telecomunicações, governo e defesa ou autoridade pública. Apesar de focada no mercado nacional, também tem vindo a atuar internacionalmente através de parcerias estratégicas.

Numa altura em que o ambiente digital ganhou protagonismo, e em que o contexto de teletrabalho, e não só, colocou a questão da segurança na ordem do dia, quer para empresas quer para os cidadãos, Bruno Castro, especialista em cibersegurança e CEO da VisionWare, aborda alguns dos cuidados ter na proteção da informação, bem como a importância de se apostar na prevenção, porque “os ataques informáticos não acontecem só às grandes empresas”. Mais do que “literacia digital”, há necessidade de haver “literacia em cibersegurança”, alertou o CEO da VisionWare.

Nos últimos meses, que alterações mais significativas sentiu no setor empresarial no que toca à proteção dos seus sistemas informáticos?
Apesar de o tecido empresarial português ser extremamente heterogéneo no que concerne à sua maturidade no tema da segurança, sentimos que todas as organizações, sem

exceção, tiveram de se adaptar ao desafio tecnológico que esta pandemia veio trazer, tal como aos novos riscos que o teletrabalho e a inerente ligação entre redes domésticas e corporativas implicam (mesmo as mais preparadas). Essa adaptação quase instantânea expôs as suas fragilidades e levou finalmente à gestão de topo o tema da cibersegurança, muitas vezes circunscrito ao departamento informático.

> (…) nunca tivemos tantas solicitações de ajuda para responder e investigar ciberataques bem-sucedidos como agora".

Sentiu que o número de ciberataques aumentou? Quais as maiores fragilidades das empresas neste domínio?
Nestes últimos quinze anos de VisionWare, nunca tivemos tantas solicitações de ajuda para responder e investigar ciberataques bem-sucedidos como agora. Estes ciberataques, desenvolvidos em vários formatos, mas tipicamente focados no roubo de dinheiro ou de dados "valiosos", resultam de vários fatores.
Por um lado, o cenário pandémico veio colocar mais pessoas, muitas sem formação, a viver no mundo cibernauta. Por outro, o ambiente de teletrabalho promove 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 fator humano é normalmente a maior fragilidade. As pessoas precisam de 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!

Quais são na sua opinião o tipo de ataques mais problemáticos? Phishing, vírus/malware, ransomware?
No decorrer dos últimos anos, os ataques tornaram-se altamente complexos e sofisticados. Recorre-se cada vez mais à engenharia social para aumentar a sua eficácia. Raramente estamos perante um caso isolado de ataque, como phishing, malware ou ransomware. Em vez disso, e cada vez mais, assistimos a uma conjugação de vários vetores de ataque que têm sempre em conta as fragilidades concretas de cada organização ou pessoas de relevo na organização e que são, por isso, adaptados individualmente pelos ciber criminosos no contexto da respetiva vítima. Os ataques, conjugados ou não, são cada vez mais desenvolvidos especificamente para a organização ou pessoa em específico.

Acho, no entanto, importante realçar o sucesso que os ataques através de phishing têm tido e que, como o nome sugere, assentam na ideia de "pescar" qualquer coisa, e que deliberadamente nos enganam, levando-nos a cair num engodo e a partilhar algo que não devíamos – o acesso à nossa organização, por exemplo.

> "(…) é preciso treinar a organização (…) para que esteja preparada para responder às ameaças cibernéticas, quando estas chegarem, porque mais tarde ou mais cedo vão chegar".

Como é que as empresas se podem preparar para combater ciberataques?
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.

E qual o tipo de soluções mais procuradas? Firewall, backup, cloud, gestor de passwords…?
Olhamos para a cibersegurança de uma forma holística, não nos circunscrevendo à aposta exclusiva em tecnologia. Os nossos consultores estão preparados, naturalmente, para apoiar na escolha, implementação e gestão desse tipo de soluções, mas para responder a uma ameaça que é tão complexa como a ameaça cibernética, é preciso ir mais longe. Quem procura apenas e só esse tipo de soluções não está, de maneira nenhuma, preparado para os desafios que este novo mundo cibernauta veio trazer.

> "(…) todos aqueles que prestem serviços básicos têm uma responsabilidade acrescida, pois um ciberataque (…), pode afetar de forma grave a vida de milhares de pessoas (…)".

Em que setores de atividade – indústria, saúde, banca e finanças, telecomunicações, governo e defesa ou autoridades públicas – considera ser mais prioritário ter uma estratégia de cibersegurança bem estruturada e implementada?
Todos os setores de atividade e empresas de todas as dimensões, desde que estejam presentes no mundo cibernauta, podem ser alvo de ciberataque. Claro está que todos aqueles que prestem serviços básicos têm uma responsabilidade acrescida, pois um ciberataque, além de afetar a atividade a que se dedicam, pode afetar de forma grave a vida de milhares de pessoas – inclusive interromper serviços essenciais de suporte à estabilidade de um país.

> "Algumas empresas, infelizmente, só investem depois de serem vítimas de um primeiro ciberataque".

O investimento em cibersegurança já é visto como tal ou ainda há muito a visão de ser apenas mais um custo para as empresas?
Isso depende apenas e só da perspetiva que as empresas queiram adotar. O investimento numa tranca na porta do estabelecimento, numa porta blindada, numa câmara para controlo do espaço ou num alarme é um investimento que as empresas fazem porque, apesar de poderem nunca vir a ser assaltadas, preferem estar preparadas para que tal nunca aconteça – afinal, se acontecer, o custo será sempre maior que o investimento na prevenção. Investir em cibersegurança segue a mesma lógica, mas a probabilidade de se ser "assaltado" é enorme.

Algumas empresas, infelizmente, só investem depois de serem vítimas de um primeiro ciberataque. Mas já há algum tempo, a cibersegurança começa a ser vista como um investimento não só positivo como necessário. Os mercados hoje são também mais exigentes e preferem empresas reputadas que protejam a sua informação e demonstrem maturidade de segurança – quer por certificações de relevo quer por metodologias ou procedimentos – no tratamento ou relacionamento cibernauta.

No atual contexto de teletrabalho, que medidas podem/devem as empresas adotar para diminuir os riscos de terem colaboradores informaticamente pouco experientes a aceder externamente às redes da empresa?
A formação é um passo essencial para colmatar as lacunas que os colaboradores possam ter. E reforço que mesmo os mais experientes podem ser alvo de ataque e, por isso, também devem ser continuamente formados. Até porque não se trata apenas de "literacia digital", mas "literacia em cibersegurança". Além disso, a formação não pode ser residual ou pontual. É fundamental formá-los continuamente e testar as suas capacidades, por exemplo, na avaliação da sua capacidade de deteção e resposta contra "ataques de phishing" simulados, para verificar se conseguem pôr em prática os novos conhecimentos adquiridos.

> "Muitas empresas portuguesas chegam mesmo a acreditar que este é o tipo de problema que só afeta os outros (…)"

Um estudo recente da PwC revelava que mais de 90% das empresas, a nível mundial, estavam a reforçar os investimentos na área da cibersegurança. Sente que as empresas portuguesas também já estão sensibilizadas para esta problemática e para os danos que um ataque informático pode causar no seu negócio?
Creio que muitas empresas estão sensibilizadas para a problemática e para os danos de um ciberataque e que a cibersegurança é sempre considerada em alguma medida. Mas os termos em que é considerada nem sempre são suficientes, e o conhecimento é mais "teórico do que prático", ficando muitas vezes circunscrito a um departamento de informática com pouco espaço de manobra para "assumir" a responsabilidade da segurança cibernética da empresa. Muitas empresas portuguesas chegam mesmo a acreditar que este é o tipo de problema que só afeta os outros, principalmente as empresas maiores e com mais capital que a sua, e têm alguma dificuldade em imaginar como e porque é que um ataque poderia ser feito à sua organização.

As soluções de cibersegurança que têm surgido no mercado, estão a ser suficientemente inovadoras para acompanhar própria transformação digital que muitas empresas se viram obrigadas a fazer?
O mundo está em constante mudança e é difícil para o tecido empresarial acompanhar esta velocidade. Mas no que toca às soluções, elas existem. O nosso setor, pela sua própria natureza, tem de acompanhar e antecipar as tendências, apostando muito na inovação e na constante formação dos seus profissionais. Por isso, se a empresa quiser, deve procurar ajuda especializada. Recomendo, no entanto, alguma ponderação na escolha das soluções. Uma solução de ponta só fará sentido se já houver maturidade para a sua implementação e, às vezes, as empresas são levadas a fazer investimentos pouco adequados ao seu nível de segurança.

> "As start-ups são excelentes polos de inovação. Têm uma grande capacidade de se reinventar e um espírito jovem, de superação, ousadia e criatividade (…)".

Qual o papel que as start-ups podem desempenhar nesse processo?
As start-ups são excelentes polos de inovação. Têm uma grande capacidade de se reinventar e um espírito jovem, de superação, ousadia e criatividade, que partilhamos, e que as leva a serem determinantes no processo de desenvolvimento de soluções inovadoras ao serviço da eficiência das empresas e da sociedade, no geral.

Como responsável de uma empresa de cibersegurança que dicas pode adiantar às empresas para protegerem os seus sistemas?
O processo de autoavaliação, através de auditoria é uma das fases mais reveladores e úteis para uma organização pois estabelece um ponto de partida para toda a definição da estratégia no que respeita o tema da cibersegurança. Permite ainda que a camada de gestão, como órgão máximo da organização, conheça e entenda o nível de segurança da empresa, identificando fragilidades e oportunidades de melhoria, o que permite, daí em diante, definir objetivos e metas de superação.

Que tendências prevê para o mercado de cibersegurança em termos de novas soluções?
Temos verificado junto do mercado que muitas vezes a gestão da informação, dos equipamentos e das pessoas, dispersas na organização, cada vez mais internacionais e assentes em diferentes plataformas, dificultam a sua capacidade de monitorização e resposta a ataques informáticos. Por isso, temos apostado bastante em promover soluções que permitam monitorizar de forma global a organização, apoiar a deteção e reduzir o tempo de resposta a eventuais ataques informáticos, quer se tratem de ameaças automatizadas, quer de comportamentos humanos de cariz suspeito ou erróneo.

> "O que falta, parece-nos, é colocar o tema da cibersegurança na ordem do dia (…)".

Que medidas legislativas devem os Governos, a União Europeia, assumir para que o controlo de ciberataques possa ser mais eficaz e não viole os direitos de privacidade de empresas/organizações e cidadãos?
Existem já vários mecanismos legais para apoiar as organizações e os cidadãos no que respeita ao tema da cibersegurança versus as condicionantes da privacidade e afins. O que falta, parece-nos, é colocar o tema da cibersegurança na ordem do dia, trabalhar mais com as empresas especializadas – provavelmente privados – que têm o know-how e podem apoiar no processo de *awareness* nacional que precisa de ser desenvolvido urgentemente para que a sociedade perceba quais os seus direitos e obrigações.

Qual tem sido a abordagem da VisionWare no sentido de reforçar a literacia informática das organizações, dos seus colaboradores e, porque não, também dos cidadãos?
No decorrer deste período da pandemia, e no âmbito das nossas iniciativas de responsabilidade social, temos vindo a colaborar com vários municípios na formação de professores na vertente da cibersegurança e as respetivas ameaças envolventes, até porque sentimos que foi um dos grupos profissionais que mais sofreu com a transição digital abrupta dos últimos meses. Temos ainda previstas outras iniciativas do género para um futuro próximo.
No plano privado, um dos nossos serviços que tem tido particular procura é a unidade de

Academy, cujas ações de formação, presencial e e-learning têm apoiado muito as empresas no processo de consciencialização dos colaboradores, em temas como a cibersegurança, privacidade e segurança da informação.

Quais os vossos objetivos de inovação e expansão enquanto empresa?
Apesar de, no início da VisionWare, em 2005, nos termos focado essencialmente no mercado nacional, o nosso objetivo sempre foi crescer e chegar a novas geografias num curto espaço de tempo. Assim sendo, e dois anos após o início da nossa aventura empresarial, conseguimos expandir a nossa atividade a nível internacional, nomeadamente na Europa e em África. Desde então, e com um 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 R&D, na vertente de segurança e privacidade. Além disso, e até pela exigência e dinâmicas do setor onde nos posicionamos, procuramos ser uma empresa que procura persistentemente as melhores soluções (tecnológicas ou não) para os clientes, respondendo às suas necessidades, mas também antecipando as tendências de mercado.

Em 15 anos de atividade, quais foram os momentos-chave da vossa atividade?
Pergunta difícil até porque 15 anos não são cinco anos... Destacaria três momentos que foram preponderantes para o nosso sucesso como empresa exclusivamente dedicada a um "nicho" de mercado, como é a segurança de informação.

Primeiro, a decisão arriscadíssima de avançar para um projeto empresarial numa área que ainda era desconhecida ou desvalorizada pelo mercado. Foi uma decisão que se baseou numa mistura explosiva de "acreditar", "visão" e "coragem" ou "loucura" dependendo da perspetiva de quem conta a história.

Segundo, foi a aposta estratégia, e também arriscada, de posicionamento internacional, nomeadamente em África, através de Cabo Verde, e na Europa, em plena crise económica a nível mundial. Foi precisamente esta abordagem que veio criar um suporte económico e financeiro para passarmos a crise de 2007/2009 em modo de crescimento. Daí termos um especial carinho por Cabo Verde, onde temos desde 2007 uma operação fixa com presença continua da nossa equipa.

Por fim, e como terceiro momento, apontaria para 2017 quando decidimos modificar o nosso modelo organizacional ao verticalizar as nossas competências – cibersegurança, privacidade, compliance, formação, forense, intelligence, etc. – em unidades de negócio e equipas diferenciadas. Deu-nos oportunidade de nos especializarmos ainda mais dentro de um setor que, por si, é já especializado. Passámos a estar mais organizados, com maior especialização por competência e com a capacidade de responder a qualquer solicitação na área da segurança num modelo de "one-stop-shop".

Quais as metas para 2021?
Face a este cenário de pandemia em que nada conseguimos prever, diria que os planos para 2021 passam essencialmente por solidificar a nossa base instalada de clientes e manter a abordagem comercial nos mercados internacionais definidos para 2020,

nomeadamente América Latina, Africa e Europa. Temos também a perspetiva de manter os nossos índices de crescimento, quer em volume de negócios quer em dimensão da nossa equipa de consultores. Por fim, e tal como previsto em 2020, iremos continuar a abordar novas linhas de serviço por especialização e competências no que respeita a disciplina de segurança. O principal objetivo será, cada vez mais, sermos a referência nacional no setor da segurança, onde a nossa oferta possa responder a qualquer solicitação de forma exclusiva e autónoma