O Estado da Nação

itsecurity.pt/news/analysis/o-estado-da-nacao-2022

A cibersegurança está em constante evolução e muito se tem alterado. As soluções estão a evoluir para proteger e prevenir as organizações, assim como ajudar as várias entidades a recuperarem no caso de um ciberataque.

A mesa-redonda Estado da Nação de Cibersegurança da IT Security procurou dar palco a empresas e CISO, CSO e diretores de informática com responsabilidades de cibersegurança para partilharem a sua visão sobre como é que a cibersegurança tem estado a evoluir, como vai evoluir e o que podem as organizações fazer para estarem mais protegidas.

Watch Video At: https://youtu.be/hGPppVcPzo8

Comparando Portugal com outros países europeus, como está o contexto da cibersegurança?

Sérgio Trindade, Diretor de Sistemas de Informação e Transformação Digital, EPAL: “A Agência de Tecnologias de Informação e Comunicação das Nações Unidas colocou Portugal no 14.º lugar do último Global Cybersecurity Index. Isto é uma boa notícia pelo trabalho que o país tem vindo a desenvolver e é coerente com aquilo que outros observatórios veem. Ainda assim, à primeira vista, não deixa de contrastar com o início de ano que tivemos. Mas isto não é algo que esteja a acontecer em Portugal; não é algo propriamente novo, mas algo que tem vindo a escalar ao longo do tempo”

"As empresas compram segurança num package porque [pensam que] assim fica tudo resolvido. Se acontecer alguma coisa foi de quem vendeu ou implementou o package"

Miguel Borges, Vishay Industries

Miguel Borges, Global IT Security, Vishay Industries: "Portugal está a fazer alguma evolução dado os ataques que foram noticiados. No entanto, creio que estamos ainda um bocado atrasados em relação à Europa, já para não falar em relação a alguns países, como os Estados Unidos, que estão mais avançados no tema, mas também são mais atacados. Ainda assim, aos poucos estamos a evoluir"

Roberto Trematerra, Head of Information Technology, Galp Gás Natural Distribuição (GGND): "Uma das preocupações é a sociedade e as pessoas. A tecnologia é um dos pilares que temos de assegurar; o outro será, com certeza, as pessoas terem a sensibilidade e a formação adequada, eventualmente, acrescentado por políticas que permitem que os vários procedimentos sejam respeitados e que não incutem um risco adicional nas organizações e na sociedade em geral"

Ricardo Madeira Simões, Chefe de Divisão de Sistemas e TIC, C.M. Amadora: "Os ciberataques do início do ano trouxeram para a ribalta estas questões da cibersegurança. Na Câmara da Amadora temos essa preocupação já há alguns anos, visto que somos certificados em [ISO] 27001 e temos todos os cuidados nesse âmbito, embora possamos sempre melhorar. Em relação aos nossos parceiros europeus – com base num projeto onde participámos que terminou em 2020 com municípios de Itália, Espanha e Alemanha – não notámos que tivéssemos menos cuidados ou menos evoluídos; ficámos agradavelmente surpreendidos"

"Comparando Portugal com as tendências europeias, acompanhamos as tendências do ponto de vista de sofisticação, dos vetores e até os próprios setores atacados"

Pedro Leite, S21sec

Pedro Leite, Chief Operating Officer, S21sec: "O que temos observado em termos de mercado europeu é que os Estados Unidos são o principal alvo dos ataques, com cerca de 50% de instituições que são atacadas. De seguida, vêm os países europeus – nomeadamente o Reino Unido, a Alemanha, a França. O contexto de Portugal – numa observação que fazemos – coloca-nos no 31.º lugar; comparando com o Global Cybersecurity Index, podemos deduzir que não somos um país fortemente atacado. É certo que, no primeiro semestre, tivemos muitos ataques, mas, do ponto de vista global, não somos um país muito visado pelos atacantes"

Paulo Pinto, Business Development Manager OT & Cloud, Fortinet: "Hoje, há dois grandes desafios que se colocam às organizações, quer em Portugal, quer noutros países europeus: internamente, temos a questão da lacuna dos recursos humanos e de conhecimento na área; este é o contexto mais difícil que as organizações enfrentam hoje; externamente, há um cenário de ameaças crescente, decorrente de ataques cada vez mais destrutivos e sofisticados. Do ponto de vista tecnológico, vemos que, em vez de os ataques serem dispersos, estão a ser cada vez mais dirigidos às organizações"

Orlando Campos, Cybersecurity Business Developer Manager, Ingecom: "É um pouco difícil comparar de forma direta Portugal com outros países europeus, talvez pelo simples facto de o país ter uma dimensão muito menor. Para me preparar para este debate, fiz uma busca por alguns fóruns na dark web para comparar quantas contas comprometidas de empresas portuguesas é que ontem existiam à venda e aquilo que constatei é que o número era muito menor e o valor para venda dessas contas também eram menores do que outros países de maior dimensão. No entanto, isso não significa – nem de perto nem de longe – que as empresas portuguesas não são atacadas"

O mais recente relatório de Riscos & Conflitos do CNCS indica que os níveis de incidentes continuam a aumentar. Qual foi a principal ameaça com que tiveram de lidar?

"Não tem só a ver com a indústria; é algo que inquina a segurança e a paz a que estávamos habituados para outro nível, o da academia"

Rogério Bravo, em representação da CIIWA

Rogério Bravo, Coordenador de Investigação Criminal da Polícia Judiciária, em representação da Competitive Intelligence & Information Warfare Association (CIIWA): "As fontes do relatório têm sempre a mesma conclusão: um aumento generalizado dos incidentes/cibercrimes. Diria cibercrimes porque a esmagadora maioria dos incidentes corresponde a cibercrime. O que interessa perceber é que os ataques cresceram imenso. Também existe um decréscimo no número de condenados, que pode ser visto com a possibilidade de não haver condenações 'à boca do tribunal', mas haver uma mudança de casos de condenados para uma figura de suspensão de processo que não corresponde a pessoas condenadas, mas a pessoas que tiveram ligação à repressão pela justiça e a quem lhes foi dada a oportunidade de se emendarem"

Paulo Moniz, Digital Global Unit Security & IT Risk, EDP: "A maior ameaça que tivemos nos últimos dois anos – e que já vinham de antes – são as coisas acabadas em 'ing', como smishing, phishing e vishing. Temos notado um grande nível de sofisticação e direcionamento, aquilo que se chama de spear phishing, incluindo 'CEO fraud'. Ainda não chegámos à fase de ter a simulação de imagem, mas acredito que dentro em breve as coisas vão acabar por ir para esse nível, de ter a imagem para enganar os colaboradores. Depois, também temos lidado com algumas campanhas de denial of service"

Bruno Castro, CEO, Visionware: "Cada vez mais, estamos numa realidade onde temos ferramentas que facilitam qualquer pessoa a lançar um ciberataque com alguma probabilidade de sucesso. Na Europa, o que temos sentido no cibercrime é ver grupos

operacionais totalmente especializados em verticais e direcionados para um setor. O que vemos mais é a usurpação de identidade, através do roubo de credenciais, e, depois, a exploração interna dos serviços associados a essas credenciais e, a partir daí, definir o landscape de ataque”

“O efeito dominó é uma realidade; a melhor forma de nos proteger é juntar forças e o decreto-lei vai-nos permitir isso: com a ajuda do CNCS”

Roberto Trematerra, GGND

Roberto Trematerra, GGND: “O evento que mais marcou a nossa organização – em termos de cibersegurança – foi o evento da Vodafone no início do ano. O interessante neste evento é que nem sequer atacou o nosso ecossistema tecnológico; foi um evento exterior ao nosso perímetro, mas que teve repercussões bastante sérias na operação. Ficámos parcialmente incapacitados de responder a algumas solicitações e comunicar com o exterior e uma boa parte dos parceiros também foram impossibilitados de contactar connosco. É uma mudança de paradigma que vai além da proteção do perímetro”

Josué Delgado, Chief Information Security Officer, Lusíadas Saúde: “Geralmente nas empresas – e a saúde não está fora desse perímetro – vemos o incremento de tentativas de ataque, seja phishing ou outras formas de ataque, estando constantemente a monitorizar e a responder. Temos estado muito atentos a ataques a empresas que gravitam à nossa volta, como outras empresas de saúde e empresas fornecedoras do nosso ecossistema. O que fazemos – assim como noutras empresas – é uma avaliação constante de quão bem estamos preparados para responder a cada um dos tipos de ataques”

"Os ataques do início do ano criaram um nível de alerta maior; as pessoas ficaram preocupadas com os seus dados e que os acessos possam ser comprometidos, mas continuam a apostar no facilitismo"

Mário Filipe, Universidade de Évora

Mário Filipe, Chief Information Security Officer, Universidade de Évora: "Não posso dizer que, durante este ano, tivemos grandes incidentes; tivemos o típico phishing, uma ou outra conta comprometida, mas observamos determinadas práticas de partilhas de passwords, de dados que são passados de forma absolutamente insegura sobre o qual é preciso fazer um trabalho de consciencialização dos utilizadores finais para a problemática da cibersegurança. Os ataques do início do ano criaram um nível de alerta maior; as pessoas ficaram preocupadas com os seus dados e que os acessos possam ser comprometidos, mas continuam a apostar no facilitismo"

Pedro Leite, S21sec: "Comparando Portugal com as tendências europeias, acompanhamos as tendências do ponto de vista de sofisticação, dos vetores e até os próprios setores atacados. Neste primeiro semestre, a S21sec verificou cerca de 20 incidentes críticos de cibersegurança em que houve um impacto forte na organização no mercado ibérico; desses, 25% foram a empresas portuguesas e o principal vetor de ataque foi roubo de credenciais ou credenciais que estão expostas"

"Os problemas aumentam não só porque o número de ameaças e ataques aumentam, mas também porque a base de incidência alargou, o que também é preocupante"

Paulo Pinto, Fortinet

Paulo Pinto, Fortinet: "Os problemas aumentam não só porque o número de ameaças e ataques aumentam, mas também porque a base de incidência alargou, o que também é preocupante. Numa fase inicial, até parece que se estava a atacar as empresas mais preparadas e, neste momento, quando a base de incidência alarga – como os sistemas industriais – estamos a ver fábricas e empresas que não estão tão preparadas a serem os alvos. A maioria das pessoas nem repara na sua existência até que começam a parar; quando começam a parar, começam a existir várias atividades a parar"

Rui Ribeiro, Cyber Security Engineer, Noesis: "Existem empresas que ainda não estão propriamente protegidas ou com os meios para endereçar este tipo de ataques. Tive um há uns tempos, de ransomware, em que o caso foi esse: não tínhamos propriamente ferramentas de frameworks de deteção, uma credencial 'leakada' e, a partir daí, foi despontado um ataque diretamente aos domain controllers que levou a uma encriptação total da empresa. Nos passos seguintes, tivemos o problema de que não existia registo de logs de entrada; tudo o que torna a recuperação e backup da infraestrutura acaba por ser complicada"

Qual é a maturidade das organizações e empresas portuguesas?

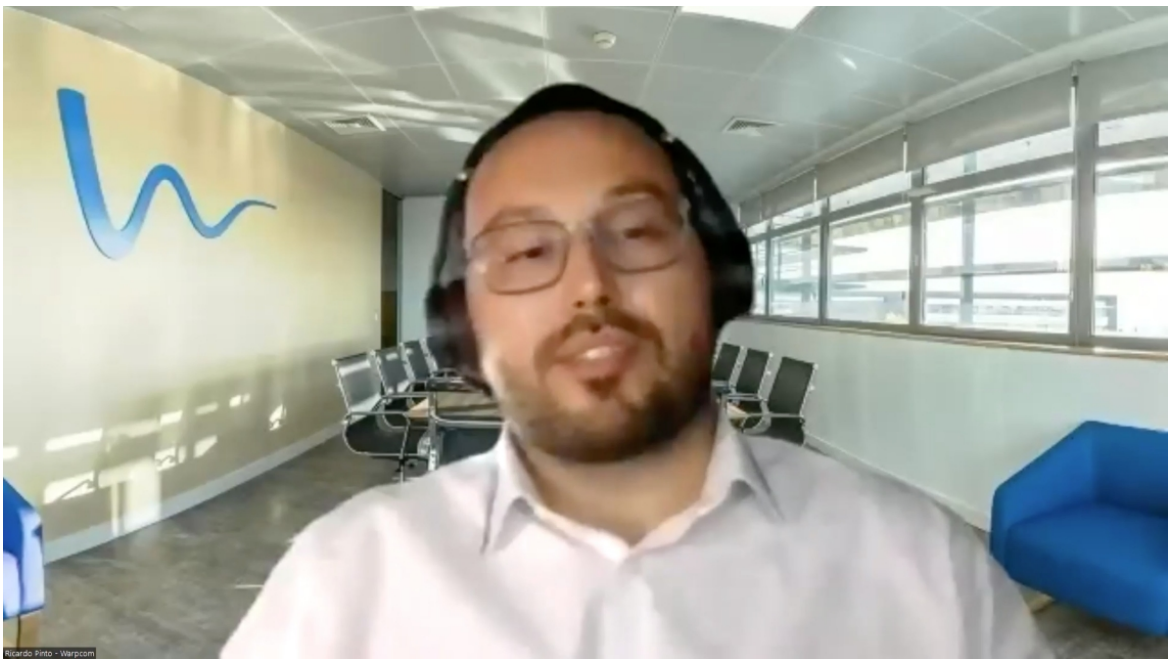
"Sinto da parte da administração um envolvimento direto em todas as salas de crise e deixei de ver uma procura por quem é o culpado"

Bruno Castro, Visionware

Bruno Castro, Visionware: "Houve uma grande evolução no que se refere à permeabilidade do top management face às questões de segurança. Ainda antes da pandemia, por questões regulatórias, a camada de gestão já estava orientada para gerir o risco de segurança num modelo bastante sólido. O pós-pandemia veio trazer uma mudança de paradigma drástico que foi sentir, de repente, que todo o tecido empresarial tem de saltar para a Internet de forma abrupta sem estar preparado para tal e o landscape passou a contar com muitos mais alvos e muito mais vulneráveis"

Adaíl Oliveira, Cybersecurity Architect & Pre Sales Manager, Cipher: "Portugal é constituído, na sua maioria, por PME onde as microempresas representam uma grande parte das existentes. Podemos caracterizar as PME como tendo poucos recursos humanos e os poucos que existem têm pouco conhecimento na área de segurança de informação. Se a tudo isto juntarmos a falta de orçamento e empresários que até consideram o risco cibernético é neste momento um dos principais riscos que enfrentam, a verdade é que a maioria olha para o investimento na segurança de informação como sendo um custo e não um investimento"

Rogério Bravo, CIIWA: "Existe diferença entre as grandes e as pequenas e médias empresas em termos de capacidade – geralmente financeira. Mas gostava de chamar à atenção para que todas as grandes empresas que foram atacadas no primeiro semestre tiveram como principal característica o grau de destruição e a queda em dominó, isto é, cada uma delas teve uma disrupção que levou à queda de falta de prestação de serviço a centenas de outras empresas. O ataque é a uma empresa, mas depois a disrupção é em dominó"



"Os planos de resposta destas organizações vão estar sempre dependentes destas equipas que muitas vezes nem sequer se conseguem preparar"

Ricardo Pinto, Warpcom

Ricardo Pinto, Technical Architect Consulting – Cybersecurity, Warpcom: "Noto que existem vários contextos em termos de maturidade. Um deles é a questão da maturidade operacional, o facto de as equipas serem muito curtas para a responsabilidade e o trabalho que executam dentro das organizações. Se juntarmos a isto o facto de terem poucas ferramentas ou formação para executarem as suas tarefas, isto pode resultar quase numa catástrofe. Os planos de resposta destas organizações vão estar sempre dependentes destas equipas que muitas vezes nem sequer se conseguem preparar"

Orlando Campos, Ingecom: "Existe uma consciencialização maior sobre segurança. Mas se compararmos a cibersegurança atual com a evolução que aconteceu no departamento de IT – em que o IT é visto como uma ajuda essencial ao desenvolvimento do negócio –, houve um salto muito grande do IT, mas a cibersegurança não acompanhou o que é o IT atual. É um facto que existe uma maior consciencialização, mas existe uma bipolaridade entre as empresas portuguesas, entre as PME com menos recursos e onde a segurança é um nice to have e as grandes empresas"

Pedro Leite, S21sec: "A maturidade das empresas portuguesas tem aumentado, mas tem aumentado de duas formas: de forma forçada porque alguém teve um incidente de segurança, onde o budget associado aumenta drasticamente ou por questões regulatórias; e de forma espontânea porque acontece aos outros, onde um setor é afetado e as empresas desse setor começam a olhar, também, para o seu ecossistema de cibersegurança e fazem o seu investimento. Depois, e como já foi referido, existe uma grande diferença de maturidade entre as PME e as grandes empresas"

Miguel Borges, Vishay Industries: “As empresas compram segurança num package porque assim fica tudo resolvido. Se acontecer alguma coisa foi de quem vendeu ou implementou o package. As empresas também dizem que faltam recursos em Portugal e não têm pessoas formadas. No nosso caso, somos uma empresa global; 60% da equipa de cibersegurança é portuguesa com um diretor e um gestor portugueses e parte das operações é controlada por portugueses numa empresa global. Contratamos pessoas localmente em Portugal que falam português. Há recursos em Portugal que são especialistas nestas áreas. O problema é mentalidade”

De que modo é que o decreto-lei 65/2021 está a impactar o modo como as organizações olham para a cibersegurança? Está a mudar alguma coisa?

Roberto Trematerra, GGND: “O decreto-lei apenas pode ser considerado como fulcral e essencial para o tecido económico português – públicas ou particulares. O efeito dominó é uma realidade; a melhor forma de nos proteger é juntar forças e o decreto-lei vai-nos permitir isso: com a ajuda do CNCS, ter uma compilação dos ativos que estão expostos e podem ser vulneráveis, como também ter uma capacidade de resposta mais adequada, juntando os eventos que poderão ocorrer nas várias organizações. O revés é o custo que isto poderá implicar para as organizações”

Sérgio Trindade, EPAL: “Este decreto-lei acaba por dirigir as ações das organizações para aquilo que, na verdade, umas já estavam a fazer e outras já deveriam estar há algum tempo. Aqui, o CNCS – como entidade reguladora – tem vindo a facilitar muito o conhecimento e a ajuda na sua aplicação. O decreto-lei assenta em três fatores principais: as pessoas e o conhecimento; a gestão dos processos; e a capacidade de recuperação. Aí, dirige-se muito para as pessoas, para assegurar a informação, a formação, a consciencialização que tem de ser feita”

“A maior ameaça que tivemos nos últimos dois anos – e que já vinham de antes – são as coisas acabadas em ‘ing’, como smishing, phishing e vishing”

Paulo Moniz, EDP

Paulo Moniz, EDP: “Há duas dimensões. As empresas que são alvo do decreto-lei acabam por já ter muito deste trabalho em tempos anteriores porque têm os recursos e meios dos riscos que se impõem à sua atividade – não só para os clientes, mas também para a sua atividade. Na segunda vertente, dá-nos um ordenamento do ciberespaço, uma linguagem comum e faz-nos alinhar na mesma coisa; isto é muito importante porque este ordenamento e linguagem vai sempre melhorando porque vamos reclamar que o decreto-lei não está a impor as coisas corretas, que tem coisas a mais. Esta dialética vai enriquecer a cibersegurança”

Mário Filipe, Universidade de Évora: “De facto, grande parte das empresas afetadas pelo decreto-lei já tinham trabalho feito nessa área e já se estavam a preparar. No caso concreto da Universidade de Évora, tornei-me CISO por causa do decreto-lei, porque era necessário nomear algum responsável da segurança da informação e o caminho seguiu assim; até aí, assumia-se que era um problema do IT. O decreto-lei veio trazer uma separação das águas e alguma linguagem comum que, de repente, faz com que as administrações tenham uma perspetiva diferente do que é a cibersegurança e as suas obrigações”

Ricardo Pinto, Warpcom: “Vejo uma maior movimentação na corrida atrás deste decreto-lei por parte do setor público. Este tema está diretamente ligado ao tema da maturidade; as equipas têm de estar preparadas para interagir com aquilo que são as interações que este decreto-lei implica. Do meu ponto de vista, muitas das organizações estão a pedir ajuda e parcerias para conseguir alcançar os objetivos e isto acontece em várias áreas do setor público, seja saúde, municípios ou educação”

“Este decreto-lei é uma oportunidade que permite olhar de outra forma para a cibersegurança nas organizações e, em alguns casos, para aproveitar para estruturar e arrumar a casa”

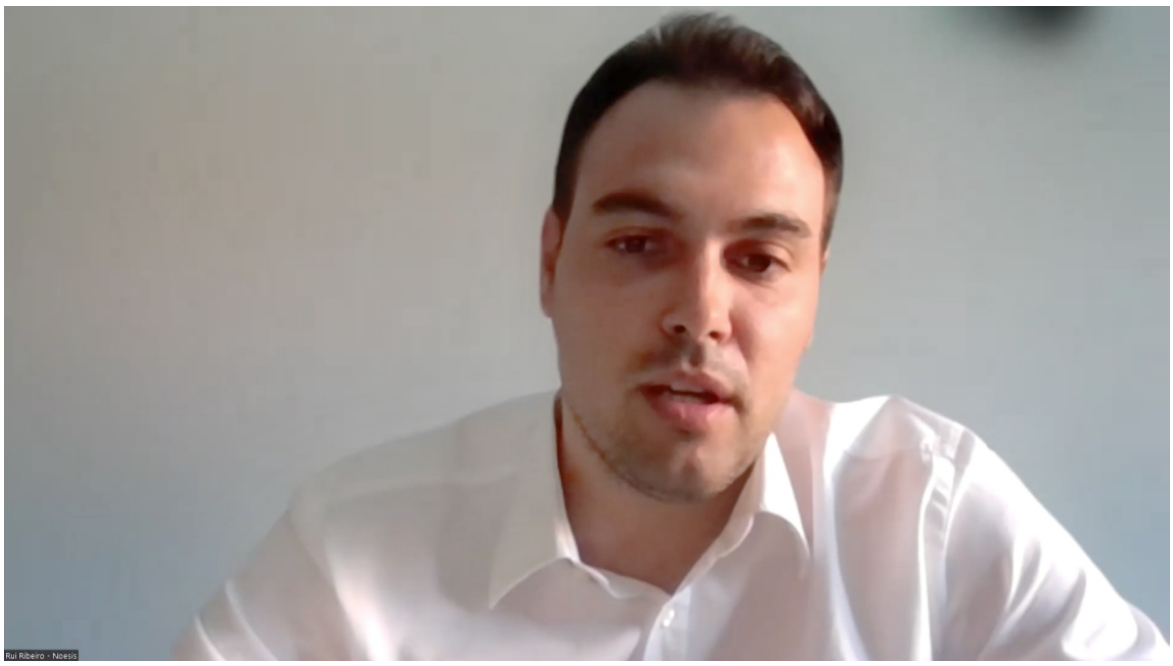
Adaíl Oliveira, Cipher

Adaíl Oliveira, Cipher: “Este decreto-lei é uma oportunidade que permite olhar de outra forma para a cibersegurança nas organizações e, em alguns casos, para aproveitar para estruturar e arrumar a casa. É uma oportunidade porque temos verificado que muitas organizações – não sei se por desconhecimento do decreto-lei ou falta de recursos – não têm dado seguimento ao decreto-lei, apesar de existir um regime sancionatório e do excelente trabalho de divulgação do CNCS. Em alguns casos, é uma oportunidade para a nomeação de um responsável de segurança, alguém que pensa segurança dentro da organização”

Josué Delgado, Lusíadas Saúde: “Algumas empresas, pelo facto de já se prepararem para responder a uma série de riscos da sua operação, estavam mais bem preparadas e já tinham um percurso feito; o decreto- lei vai ajudar a termos todos essa mesma linguagem. É uma questão de a organização rever e é mais um assessment, uma lei que tem de entrar no processo normal da organização de rever o quadro jurídico e regulatório e ver quão preparados estão, ver as diferenças e traçar o plano de atuação. Depois, permite a outras empresas porque vai trazer alguns instrumentos e a força necessários”

Como é que o atual contexto geopolítico está a afetar a segurança das organizações? Têm visto um maior número de ataques de atores estatais?

Paulo Moniz, EDP: “Em termos de atores estatais e ataques que vêm por essa via, o que temos observado – sendo que é sempre difícil de determinar a atribuição no ciberespaço – é muito mais atividade de países menos próximos dos nossos valores democráticos. Em termos globais, os atores estatais têm aumentado as suas atividades. É uma preocupação grande para as organizações porque o ciberespaço pode ser assimétrico em termos de poder, mas, na verdade, os atores estatais têm muito mais recursos, motivações e tempo. Esse ‘muito mais’ torna muito mais difícil para as organizações defenderem-se de advanced persistent threats”

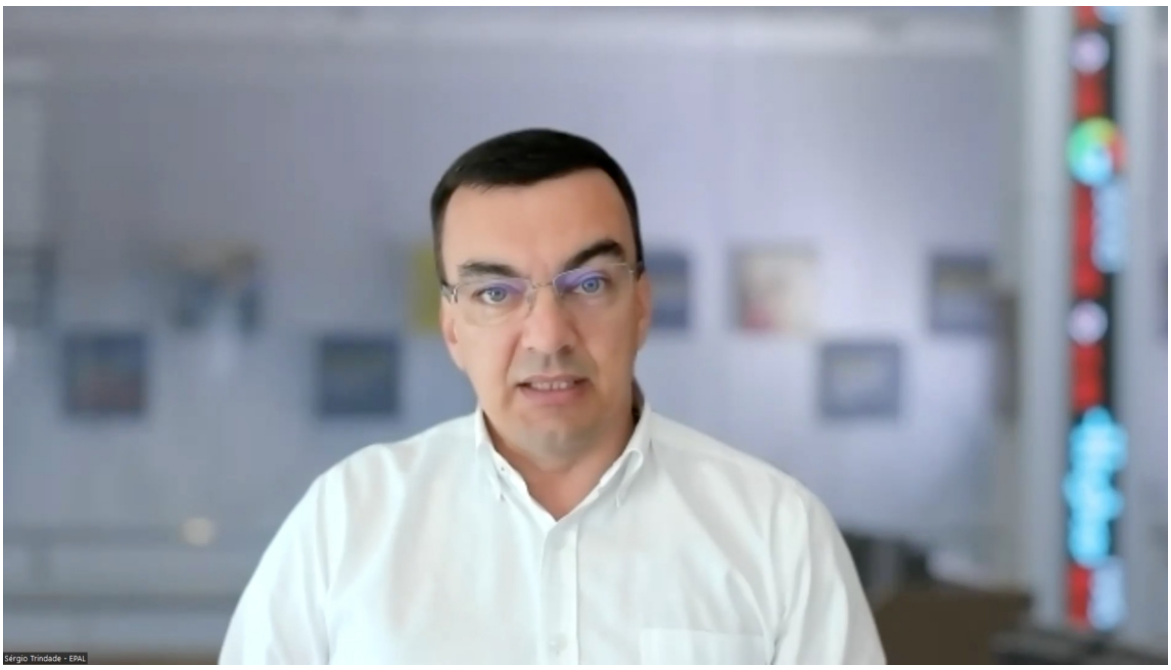


“ Em relação à administração, esta tem de ter um papel ativo no que é a gestão de segurança; na resposta a incidentes, o escalamento vai desde o analista de primeira linha até ao CEO ou administrador”

Rui Ribeiro, Noesis

Rui Ribeiro, Noesis: “No contexto geopolítico, podemos verificar uma coisa interessante nos últimos tempos que, no caso da guerra da Ucrânia, é a ciberguerra dos atores estatais. Foi possível verificar que tudo o que era infraestruturas russas, a quebra dos sites, inoperabilidade dos mesmos, acaba por demonstrar que os atores estatais e alguns cibercriminosos acabam por se aproveitar para provocar atos ilícitos. Existe um sentimento de impunidade de que estamos a fazer algo para o bem comum, mas não estamos”

Rogério Bravo, CIIWA: “É um problema transnacional, mas é muito mais do que isso. Não tem só a ver com a indústria; é algo que inquina a segurança e a paz a que estávamos habituados para outro nível, o da academia. Não estávamos muito habituados a olhar em termos de cibersegurança ou espionagem, que é olhar para os politécnicos portugueses e academia portuguesa e começar a falar e transmitir uma mensagem de preparação e de despiste de ações dessa natureza”



"A Agência de Tecnologias de Informação e Comunicação das Nações Unidas colocou Portugal no 14.º lugar do último Global Cybersecurity Index"

Sérgio Trindade, EPAL

Sérgio Trindade, EPAL: "Na observação que é feita, existe um aumento claro de incidentes e provenientes de países que demonstraram que são menos amigos da Europa, mas, sobretudo, a evolução drástica que houve. Por exemplo, estamos em contacto com várias entidades públicas porque estamos a perceber que recebemos constantemente emails já muito estruturados. Quando investigamos e contactamos as entidades é que existem algumas câmaras e empresas de água que foram atacadas – algumas há quase um ano – e, agora, estão a utilizar esses conteúdos para enviarem emails muito direcionados para pessoas concretas"

Miguel Borges, Vishay Industries: "Para nós é o habitual. Nós estamos no pior sítio; somos uma empresa norte-americana que trabalha para o departamento de defesa norte-americano, ou seja, o departamento de guerra. Somos atacados todos os dias. O que também notamos é que os ataques são cada vez mais sofisticados. Outra coisa que não falamos muito é o aproveitamento dos bugs zero days; neste momento, a nossa maior dor de cabeça são os zero days. Antes apareciam uma vez de seis em seis meses; depois passou para uma vez por mês e, agora, é quase todos os dias"

"Existe uma maior consciencialização, mas existe uma bipolaridade entre as empresas portuguesas, entre as PME com menos recursos e onde a segurança é um nice to have e as grandes empresas"

Orlando Campos, Ingecom

Orlando Campos, Ingecom: "Os grandes ataques de ransomware que temos visto também vêm de atores estatais, como a Coreia do Norte, que, de alguma forma, procuram fazer um bypass às sanções que lhes são impostas. No entanto, aquilo que vemos neste tipo de ataques é que são muito direcionados, altamente sofisticados, que, tipicamente, duram anos até serem descobertos. Aquilo que podemos ver é que estas tentativas de ataque por atores estatais é cada vez mais uma realidade e aumenta cada vez mais em número"

Ricardo Madeira Simões, C.M. Amadora: "O que notámos na Câmara Municipal da Amadora é que houve um incremento brutal dos ataques de phishing e ransomware com origem – não me arrisco a dizer que são atores estatais – na Rússia, na China e na Índia. Tivemos que tomar medidas restritivas relativamente ao tráfego que tinha origem nos países mencionados. O que tiramos daí é que, de facto, substituída a pandemia, é o conflito na Ucrânia que é o móbil das dinâmicas dos ciberataques ao nosso espaço nacional"

A cibersegurança é, hoje, um tema na mesa da administração? Como tem estado a evoluir o envolvimento da administração na cibersegurança?

"A cibersegurança deve ser vista como uma prática institucional de resposta ao risco e também a devemos ver como um tema do negócio"

Josué Delgado, Grupo Lusíadas Saúde

Josué Delgado, Lusíadas Saúde: "Temos visto que o aumento dos ataques e o impacto que temos tido em Portugal tem ajudado a que, cada vez mais, a cibersegurança tenha palco. A cibersegurança deve ser vista como uma prática institucional de resposta ao risco e também a devemos ver como um tema do negócio. O nosso desafio é como passar do tradicional discurso de proteção e resposta para um discurso para tornarmos a cibersegurança mais como um ativo estratégico, de business enabler. Para ter lugar na mesa da administração e no negócio, temos de mudar o discurso"

Bruno Castro, Visionware: "Diria que não há, hoje, nenhum administrador ou gestor que não saiba o que é cibersegurança. O tema está na ordem do dia e até no nosso setor isto acaba por ser um tema sexy. Após tudo o que aconteceu durante a pandemia, assim como os casos mais mediáticos, já não é um problema explicar o que é cibersegurança. Pelo contrário, até sinto da parte da administração um envolvimento direto em todas as salas de crise e deixei de ver uma procura por quem é o culpado e veem um conceito de que isto é um processo contínuo e é para sempre"

Rui Ribeiro, Noesis: "A cibersegurança é o tema do dia e todas as empresas estão a procurar reforçar-se nesta área. Em relação à administração, esta tem de ter um papel ativo no que é a gestão de segurança; na resposta a incidentes, o escalamento vai desde o analista de primeira linha até ao CEO ou administrador no caso de um incidente crítico que pode levar a uma disrupção do serviço que pode afetar a própria marca em questão. Também todo o processo de resposta a incidentes e planeamento, desde seguimento das frameworks que vão ser adotadas ou as ações de sensibilização dentro da empresa, toda a administração deve estar ciente disso"

Paulo Pinto, Fortinet: "Há uns meses, a SEC, a entidade reguladora norte-americana, apresentou uma série de propostas de regulação que visa obrigar cada empresa a ter no seu conselho de administração e o CISO. Tal como agora têm o responsável

financeiro que tem o peso que sabemos no conselho de administração, o que está a ser sugerido é que o CISO passe a estar presente na administração, trazendo a cibersegurança para a mesa da administração com todas as responsabilidades inerentes”

Adaíl Oliveira, Cipher: “Nas médias e grandes organizações, temos visto que o tema da cibersegurança é um tema de preocupação para as administrações. Temos verificado que tanto colaboramos com empresas que têm CISO que respondem diretamente à administração e participam na definição da estratégia da organização para o seu negócio, como temos recebido solicitações de CISO-as-a-Service nos mesmos moldes. Estas duas abordagens mostram a preocupação cada vez mais evidente da administração com a cibersegurança”

Ricardo Pinto, Warpcom: “Existe uma diferença de paradigma. Nota-se que já existem algumas organizações que já estão a reservar anualmente um budget dedicado para a área de cibersegurança; isto significa que as empresas já são proativas ao ponto de perceber que este investimento é mais um passo para a transformação digital. Era importante é ver isto replicada em mais organizações, porque muitas ainda são reativas aquilo que é o mundo da cibersegurança”

Sérgio Trindade, EPAL: “Temos que enfatizar uma situação que é a forma como passamos as coisas para a administração. Há sempre uma grande queixa de dizer que a administração não faz ou não permite, mas a verdade é que é uma responsabilidade nossa a forma como os envolvemos e a forma como lhes passamos essa informação. Não há nenhuma administração que responda bem quando vamos lá só pedir recursos ou dinheiro. É necessário envolvê-los no dia a dia e perceberem onde é que o negócio ou atividade de cada uma das empresas está envolvido para que, eles mesmos, vejam essa necessidade também com os inputs regulares que recebem”

"O que tiramos daí é que, de facto, substituída a pandemia, é o conflito na Ucrânia que é o móbil das dinâmicas dos ciberataques ao nosso espaço nacional"

Ricardo Madeira Simões, Câmara Municipal da Amadora

Ricardo Madeira Simões, C.M. Amadora: "Já há alguns que, felizmente, a administração percebeu – ou nós soubemos transmitir – a importância das matérias da segurança da informação e cibersegurança e tem- -nos apoiado – talvez não tanto quanto nós quiséssemos – para garantir que estamos seguros e certificados nesse âmbito. Os ataques do início do ano vieram fazer luz àquilo que vínhamos a dizer há alguns anos e de que podia ter impacto, de que mais vale prevenir do que remediar"

Mário Filipe, Universidade de Évora: "As universidades têm uma particularidade que é, normalmente, terem uma administração e uma reitoria; temos que justificar e explicar duas vezes as necessidades de investimento em cibersegurança. Já passei pela fase de 'somos uma pequena universidade do interior e ninguém quer saber de nós' e pela resposta histérica de 'toda a gente está a ser atacada e quando é que vamos ser nós e o que estamos a fazer contra isso'. É necessário procurar servir como âncora de equilíbrio junto da administração para mostrar que não somos tão insignificantes que não vamos ser atacados, mas que também não somos assim tão significativos de que não vamos ser a próxima vítima"


Security