SETEMBRO/OUTUBRO 2020
DISPONÍVEL POR ASSINATURA

NEWS

SECURITY MAGAZINE

WWW.SECURITYMAGAZINE.PT

REVISTA DOS PROFISSIONAIS DE SEGURANÇA

CIBERSEGUROS: MERCADO EM CRESCIMENTO

CYBER SECURITY

A OPINIÃO DE 16 ESPECIALISTAS

PANDA SECURITY

TALKDESK

CNCS

VIEIRA DE ALMEIDA

"SEGURANÇA É UMA DAS ÁREAS PRIORITÁRIAS"

RITA SOUSA
DIRECTORA
RITA.SOUSA@SECURITYMAGAZINE.PT

FAZER A DIFERENÇA

"Há um super-herói em todos nós. Só precisamos de coragem para colocar a capa", a frase ficou imortalizada pelo cinema e, em tempos como os que enfrentamos agora, faz todo o sentido recordá-la.

O dia-a-dia das empresas mudou radicalmente nos últimos meses. Muitas viram todas as suas estruturas transferirem-se, de um dia para o outro, para um ambiente completamente novo. Milhares de trabalhadores, em todo o mundo, mudaram-se de "armas e bagagens" para a sala lá de casa – mais bagagens do que propriamente armas, é verdade!

À pressa, departamentos inteiros, deslocalizam-se e dispersaram-se. Enquanto algumas empresas já tinham o conhecimento e ferramentas para assegurar, de forma mais ou menos eficaz, este processo, outras perceberam o salto que necessitam dar neste mundo, cada vez mais, digitalizado. Num caso ou noutro, as questões de segurança, associadas à componente cibernética, ganharam uma enorme dimensão.

A somar à falta de preparação, técnica e humana, evidenciada por esta dependência tecnológica, a pressão externa tem sido crescente. Chega escondida, por exemplo, num email pouco suspeito enviado a um colaborador, aproveita-se do momento, da situação, do desconhecimento, da fragilidade e ganha o seu espaço. O cibercrime cresceu a níveis sem precedentes nos últimos meses, deixando clara a necessidade de preparação e adaptação das organizações para esta questão. É por isso que decidimos fazer uma edição focada na cibersegurança.

No cenário actual, que provavelmente nem a melhor longa-metragem alguma vez idealizou, como é possível dar a resposta certa, sem comprometer a operacionalidade, prejudicar negócios, comprometer a informações? Como é possível lidar com a pressão a que estão sujeitas as pessoas dentro de uma organização – todas elas - de todos os departamentos?

Seguramente demoraremos anos a perceber e a medir os impactos do actual momento nas nossas vidas. Na vida das nossas organizações, nas dinâmicas familiares, na economia. Na forma como estamos no mundo, como somos e o que, de facto, queremos ser. Porém, cedo percebemos que todos podemos ser super-heróis e fazer a diferença.

FICHA TÉCNICA
DIRECÇÃO 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 **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. Gráfica: Print 24 - Alemanha. Email marketing EGOI

2 EDITORIAL

3 NESTA EDIÇÃO

4 SEGURANÇA 360
- CIBERSEGURANÇA
- PERCEPÇÃO DE RISCO

12 PRODUTOS & SERVIÇOS
- CIBER SEGUROS

22 ACTUALIDADE
- CNCS
- MOTIVAÇÕES DE COMPRA
- PANDA SECURITY
- SECURITYSCORECARD
- CANALYS
- IBM
- KASPERSKY
- PANDEMIA

40 EM FOCO
- VIEIRA E ALMEIDA
- TALKDESK
- EXPLOIT HUNTERS

65 PERFIL
- CISO

16 ESPECIALISTAS RESPONDEM A 3 QUESTÕES SOBRE CIBER RISCO, MOTIVAÇÕES DE COMPRA E IMPACTOS DA PANDEMIA

22 PANDA SECURITY

12 CIBERSEGUROS

40 VIEIRA E ALMEIDA

42 TALKDESK

TEMA DE CAPA

O CIBERCRIME ESTÁ A CRESCER EM TODO O MUNDO. EM PORTUGAL NÃO É EXCEPÇÃO. OS INDICADORES DO GABINETE DE CIBERCRIME DA PROCURADORIA GERAL DA REPÚBLICA REVELAM QUE A ECLOSÃO DO NOVO CORONAVIRUS REVELOU UM AUMENTO DO NÚMERO DE CIBERCRIMES, OS QUAIS SE MULTIPLICARAM DE FORMA EXPONENCIAL, NOS PRIMEIROS CINCO MESES DO ANO.

ALÉM DOS CRIMES INFORMÁTICOS CLÁSSICOS, CONTABILIZAM-SE CRIMES COMO BURLAS EM PLATAFORMAS DE VENDAS ONLINE, DIVULGAÇÃO ILÍCITA DE FOTOGRAFIAS, CRIMES CONTRA A HONRA, DIFUSÃO DE PORNOGRAFIA INFANTIL OU CRIMES CONTRA O DIREITO DE AUTOR. BOA PARTE DESTAS PRÁTICAS JÁ EXISTIA ANTERIORMENTE, PORÉM, GANHOU NOVO ESPAÇO NAS REDES DE COMUNICAÇÃO E INFORMAÇÃO. AS ESTATÍSTICAS DA JUSTIÇA, EM GERAL, AGLOMERAM OS CRIMES SEGUNDO OS TIPOS LEGAIS (POR EXEMPLO BURLAS, CRIMES CONTRA A HONRA, CRIMES CONTRA O DIREITO DE AUTOR), NÃO CONSIDERANDO AUTÓNOMA OU SEPARADAMENTE AQUELES QUE OCORREM ONLINE.

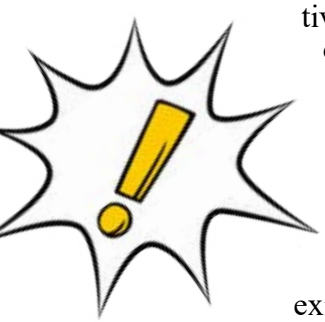
As queixas de crimes online recebidas pelo Gabinete Cibercrime de Portugal têm vindo consistentemente a aumentar, desde 2016. As denúncias recebidas no ano de 2020 (mesmo sabendo que apenas se contabilizaram até 31 de Maio) superaram "já em muito as dos anos anteriores". Por exemplo, tendo em conta os dados de 2018, a progressão para 2019 foi de 120% denúncias a mais. Quanto à evolução de 2019 para 2020 (e apenas considerando as denuncias entradas até 31 de Maio de 2020), a progressão é já de 139% denúncias a mais.
A Security Magazine, o Centro Nacional de Cibersegurança confirmou que (ver entrevistas completa) durante o período da pandemia se verificou um aumento do número de incidentes, registados por parte do CERT.PT. O CNCS salienta a actual situação vem "reforçar a ideia de que a cibersegurança é uma componente fundamental para a estabilidade das organizações".
Como aponta, este crescimento não foi uniforme. "**O sector da banca foi mais afectado do que outros**, nomeadamente através de campanhas de phishing, não só em termos absolutos como comparado com o no anterior". Já a distribuição e consumo de água "não viu o número de incidentes registados variar significativamente em relação ao ano anterior", salienta.
Este aumento, embora mais acentuado durante o período inicial da pandemia, não é de agora. As perdas cibernéticas entre as empresas atacadas por ciberataques em 2019 aumentaram quase seis vezes, de uma média de 10.000 dólares por empresa para 57.000, as conclusões são do estudo da Hiscox, que contou com a participação de mais de 5000 empresas.
Ainda assim, há sinais de que as empresas estão a responder com medidas de segurança mais rigorosas e investimentos mais altos em termos de segurança, que resultou num aumento de 39%.

COVID-19 INFLUENCIA INVESTIMENTOS

Fruto do aumento de ciberataques no mundo, o **mercado mundial de cibersegurança aumentou 9,7%** no primeiro trimestre de 2020. O investimento foi impulsionado no final do trimestre por organizações que apostam fortemente no teletrabalho nas fases iniciais de encerramento em resposta à COVID-19, indica estudo da Canalys.
Segundo os dados divulgados, o investimento total atingiu 10,4 mil milhões de dólares, o que inclui segurança de redes, segurança de endpoints, segurança da web e do correio electrónico, segurança de dados, e vulnerabilidade e análise de segurança.
De acordo com o estudo, a Cisco foi o principal fornecedor de cibersegurança durante o primeiro trimestre, sendo responsável por 9,1% do investimento total. A Palo Alto Networks continuou a ser o seu concorrente mais próximo, com uma quota de mercado de 7,8%. A Fortinet manteve a sua dinâmica e aumentou a sua quota para 5,9%. A Check Point foi o quarto maior fornecedor, representando 5,4%, enquanto que a Symantec completou os cinco maiores fornecedores com 4,7%.
O crescimento da cibersegurança estará sob pressão à medida que os orçamentos de TI forem sendo reavaliados tendo em conta o agravamento das condições económicas. Isto apesar da criticidade de proteger os dados, operações e empregados das organizações contra ameaças e vulnerabilidades crescentes. Consequentemente, **os aumentos planeados dos investimentos em cibersegurança ao longo dos próximos 12 meses serão ou reduzidos ou completamente interrompidos**, diz o estudo.
"A mudança sem precedentes para o trabalho remoto a partir de Março resultou numa forte procura de segurança dos enpoints para proteger os computadores da empresa, bem como os dispositivos dos funcionários utilizados (…)", disse Matthew Ball, Analista Chefe da Canalys. "A procura pela segurança dos endpoints aumentou 16,9%, o que representa 15,4% do mercado total de segurança cibernética. Este forte crescimento continuou no segundo trimestre, à medida que mais países implementaram medidas de bloqueio e confinamento. Mas a segurança da rede cresceu apenas 4%, uma vez que o negócio do hardware para alguns fornecedores foi afectado pelas restrições da cadeia de abastecimento. Além disso, muitas organizações puderam utilizar melhor o acesso à rede existente através de contratos de serviço ou do aumento da capacidade através de licenças adicionais em vez de construção de novas infra-estruturas de segurança de rede. A segurança da Web e do correio electrónico cresceu 13,8% à medida que as organizações continuaram a expandir a sua utilização de serviços baseados na nuvem e aplicações SAAS, incluindo o Office 365".
Os fornecedores de segurança informática responderam rapidamente à crise, permitindo às organizações proteger temporariamente trabalhadores em teletrabalho.
A Cisco estendeu licenças gratuitas para os seus produtos Umbrella, Duo Security e AnyConnect Secure Mobility Client, tanto aos clientes existentes como aos novos clientes. Também anunciou o seu Programa de Resiliência Empresarial de 2,5 mil milhões de dólares para manter o seu pipeline saudável.
A Palo Alto Networks lançou serviços financeiros para oferecer condições de pagamento alargadas, para além de testes gratuitos de 90 dias para as suas ofertas GlobalProtect. A Juniper Networks forneceu testes gratuitos do seu vSRX a clientes para expandir a capacidade de firewall, bem como testes gratuitos de AppSec, IPS e SecIntel.
A Bitdefender direccionou a sua oferta de acesso

gratuito de 12 meses para organizações de saúde, enquanto a Kaspersky também disponibilizou as suas ofertas de Endpoint Security e Hybrid Cloud Securi- ty gratuitamente para o sector.

A Trend Micro disponibilizou gratuitamente o seu produto de Segurança Máxima durante seis meses aos trabalhadores que tivessem de utilizar os seus próprios dispositivos.



A McAfee ofereceu licenças a curto prazo de três meses para os seus produtos Endpoint, DLP, Unified Cloud Edge e CASB.

"Os fornecedores que foram rápidos a apoiar os clientes existentes e os novos clientes durante o confinamento serão os que mais ganharão quando as organizações reavaliarem e redefinirem as suas estratégias de segurança cibernética", disse o analista de pesquisa Canalys Ketaki Borade.

"Os trabalhadores serão mais descentralizados e trabalharão a partir de múltiplos locais de trabalho pós-COVID-19. Isto tem implicações para o tipo de soluções de cibersegurança necessárias, com maior ênfase na segurança na nuvem, zero-trust e automatização de políticas. Mas é pouco provável que as despesas com cibersegurança sejam completamente protegidas de cortes orçamentais, à medida que as organizações se ajustam à deterioração das condições fiscais".

Espera-se que as taxas de crescimento abrandem durante o resto do ano, e até 2021, embora haja algum aumento em certos sectores à medida que os testes gratuitos expiram e os clientes mudam para ofertas pagas. Os grandes projectos já estão a ser analisados, causando atrasos, enquanto a procura das Pequenas e Médias Empresas caiu a partir de meados do segundo trimestre. Menos pagamentos adiantados para contratos plurianuais será outro factor ao longo dos próximos trimestres a enfrentar pelas empresas, embora muitos fornecedores já tenham mudado grande parte do seu negócio para modelos de subscrição mais previsíveis.

"A mudança de um crescimento elevado para um crescimento baixo irá afectar todos os fornecedores. Os fornecedores privados apoiados por capitais próprios procurarão reduzir ainda mais os custos, enquanto que as startups acelerarão os seus planos, dando aos fornecedores maiores oportunidades de adquirir tecnologia emergente e acelerar as suas estratégias. Os parceiros de canal e os clientes terão de avaliar cuidadosamente os fornecedores com quem trabalham, em termos de apoio e investimento para satisfazer as suas necessidades em evolução", diz Borade.

A resposta à crise continua a pressionar os orçamentos dos departamentos e a limitar recursos para outras funções menos essenciais. Segundo uma previsão da Mckinsey esta situação "direccionará os gastos no ano fiscal de 2021, que muitos departamentos estão já a planear".

Segundo a pesquisa, **os gastos gerais devem diminuir nos sectores mais atingidos pela pandemia**, mantendo-se estável nos sectores menos afectados. "Os desafios que as empresas de cibersegurança enfrentam contaminaram os fornecedores de tecnologia".

Muitos orçamentos dos CISOs (Chief Information Security Officer) para 2020 já tinham sido atribuídos antes da pandemia. Para cobrir o custo desta crise, "tiveram de suspender outros projectos", diz a Mckinsey. 250 CISOs indicam que "as medidas de segurança trazidas pela crise continuarão a ser as principais prioridades orçamentais no terceiro e quarto trimestre de 2020".

Mais de 70% dos executivos de segurança também acreditam que os seus orçamentos para o próximo ano irão diminuir. "Espera-se que o apoio a novas formas para salvaguardar as organizações limite os gastos em questões como conformidade, governance e ferramentas de risco".

Segundo o documento, o retalho, indústria avançada, energia e materiais, transportes, viagens e lazer deverão reduzir os seus investimentos em cibersegurança. Já o sector hospitalar, banca, serviços financeiros, tecnologia, media, telecomunicações e sector público deverão aumentar os seus investimentos em cibersegurança no próximo ano.

Os principais investimentos das empresas no próximo ano serão em network security, identity and access management e messaging security.

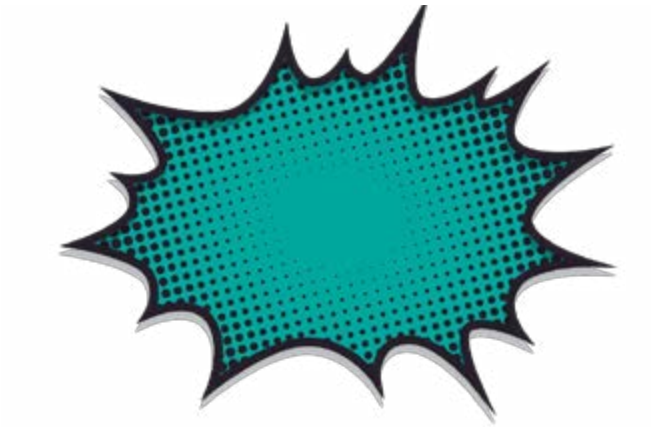
Destaque para as soluções de segurança do endpoint, protecção de dados, segurança web, gestão de segurança e vulnerabilidades e a aposta em managed security services (MSS). Existirá, segundo o documento, uma quebra da aposta no governance, risk, compliance/integrated risk management.

NOVAS PRIORIDADES

O cibercrime custa às empresas 24,7 dólares por minuto e o custo médio de um ataque de um malware é de 4,95 dólares por minuto, indica um estudo da empresa RiskIQ.

De acordo com a empresa, o cibercrime deverá custar globalmente 11,4 milhões de dólares por minuto em 2021, um aumento de 100% desde 2015.

Entre os dados divulgados, destaque para os ataques que têm surgido à volta do tema Covid-19. A cada minuto são detectados 35 emails de spam relacionados com a doença e um site é colocado online para



aplicar ataques sob o domínio Covid-19 a cada 15 minutos.
Além destes dados, destaque para o surgimento de 375 novas ameaças por minuto, assim como a divulgação de uma nova vulnerabilidade a cada 24 minutos e 16172 registos comprometidos por minuto.
Por minuto são investidos 235.540 dólares em infosec. Poucas funções corporativas mudaram de prioridades com tanta rapidez quando a crise do COVID-19 surgiu como as operações de cibersegurança e os fornecedores de tecnologia que as apoiam. De repente, milhares de funcionarios viram-se num modelo de trabalho a partir de casa. Os CISO ajustaram-se, passando do trabalho baseado em tarefas rotineiras e em direcção a metas a longo prazo, para passarem a estabelecer ligações seguras para a força de trabalho remota recém-criada. Tomaram medidas para evitar novas ameaças à rede que visam trabalhadores remotos e reforçaram operações voltadas para negócios e e-commerce após o aumento das compras online durante os bloqueios da pandemia. Estes profissionais responderam à pandemia instituindo rapidamente medidas para manter a continuidade do negócio e protegerem-se contra novas ameaças. Para gerir a continuidade do negócio, têm vindo a corrigir sistemas remotos através de redes privadas virtuais – VPN – que se têm deparado com sobrecargas crescentes. Têm vindo a monitorizar os níveis de ameaça, incluindo o crescimento acentuado de ataques de phishing desde o início da pandemia. Os trabalhadores remotos estão a ser bombardeados com ataques baseados no tema Covid-19. Estes estão a tirar partido de actualizações de filtros de correio electrónico e web e a utilizar engenharia social para se aproveitarem das preocupações dos trabalhadores.

FOCO NA RESILIÊNCIA

Até 2024, 75% dos CEOs serão responsabilizados pessoalmente pelas consequências dos incidentes de segurança ciber-físicos, indica estudo da Gartner. Segundo aponta, a responsabilidade por estes incidentes irá passar a barreira corporativa até chegar à responsabilidade pessoal.

"Devido à natureza dos sistemas ciber-físicos, os incidentes podem conduzir rapidamente a danos físicos a pessoas, destruição da propriedade ou desastres ambientais". Estes incidentes "irão aumentar rapidamente nos próximos anos, devido a uma falta de foco na segurança e aos investimentos actualmente alinhados a esses activos".
A Gartner define os sistemas ciberfísicos como sistemas concebidos para orquestrar a detecção, computação, controlo, ligação em rede e análise para interagir com o mundo físico (incluindo humanos). Estão subjacentes a todos os esforços de TI, tecnologia operacional (OT) e Internet das Coisas (IoT) ligados entre si, onde as considerações de segurança abrangem tanto o mundo cibernético como o físico, tais como infra-estruturas intensivas de bens, infra-estruturas críticas e ambientes clínicos de saúde.
"Os reguladores e governos reagirão prontamente a um aumento de incidentes graves resultantes da falta de segurança dos sistemas ciber-físicos, aumentando drasticamente as regras e regulamentos que os regem", aponta Katell Thielemann, vice-presidente de investigação da Gartner. "Nos EUA, o FBI, NSA e CISA já aumentaram a frequência e os detalhes fornecidos relativamente às ameaças aos sistemas relacionados com infra-estruturas críticas, a maioria dos quais são propriedade da indústria privada. Em breve, os CEO não poderão alegar ignorância ou recuar atrás de apólices de seguro". A Gartner preve que o impacto financeiro dos ataques a sistemas ciber-físicos, resultando em baixas fatais, atingirá mais de 50.000 milhões de dólares até 2023. Mesmo sem levar em conta o valor real de uma vida humana, os custos para as organizações em termos de indemnização, litígio, multas e perda de reputação serão significativos. "Os líderes tecnológicos precisam ajudar os CEOs a compreender os riscos que os sistemas ciber-físicos representam e a necessidade de dedicar mais atenção e investimento à sua segurança", sendo que "quanto mais ligados estiverem estes sistemas maior será a probabilidade de ocorrência de um incidente".
Edifícios inteligentes, cidades inteligentes, carros conectados, veículos autónomos, entre outros, colocam grande destaque a estes incidentes. "Os incidentes no mundo digital terão um efeito muito maior do que no mundo físico, uma vez que os riscos, ameaças e vulnerabilidades existem agora num espectro bidireccional, ciberfísico. Contudo, muitas empresas não estão conscientes dos sistemas já implementados na sua organização, quer devido a sistemas herdados ligados a redes empresariais por equipas fora das TI, quer devido a novos esforços de automatização e modernização impulsionados pelo próprio negócio". Como conclui, "é extremamente necessário um foco na gestão da resiliência operacional para além da cibersegurança centrada na informação".•

1. DE QUE FORMA TEM EVOLUÍDO A PERCEPÇÃO DO CIBER RISCO POR PARTE DAS EMPRESAS EM PORTUGAL?

(...) começam a aperceber-se de que o seu dia-a-dia está recheado de situações extremas, desconhecidas ou incertas que aparecem, se propagam e desaparecem de forma rapidamente desconcertante. E num ciclo que se repete e não parece querer voltar aos velhos dias pré-www! Apercebem-se que os riscos no ciberespaço podem ter origens desconhecidas, que não dominam ou que não foram considerados, e que se propagam mais rapidamente do que alguma vez pensaram. Começam a interessar-se, agora não ao nível técnico mas ao nível da gestão das empresas, em conhecer, ou tentar, as regras que governam esses riscos no ciberespaço. Esta é uma evolução interessante que pode trazer benefícios reais para as organizações,(...) nomeadamente porque passam a considerar a minimização dos riscos no ciberespaço como parte do investimento necessário para o seu negócio ou missão e não como um custo, assegurando a implementação dos controlos de segurança necessários (...)

PAULO PINTO, ESPECIALISTA EM CIBERSEGURANÇA, AXIANS PORTUGAL

(...) há uma evolução clara de uma realidade em que o ciber risco era percebido como um tema de TI, na esfera de responsabilidade dos gestores dessa área, para uma nova realidade em que é entendido como componente fundamental do risco corporativo. No seu todo da responsabilidade da gestão executiva da organização, que define um modelo de gestão mobilizando recursos em diferentes áreas, tais como tecnologias e sistemas de informação, cibersegurança, segurança corporativa, RH, auditoria, conformidade, entre outras. Esta evolução decorre da conjugação à escala global de diferentes factores, (...), onde se destacam: a crescente digitalização de processos de negócio, com fluxos de informação sensível estendidos a um universo cada vez mais alargado e heterogéneo de intervenientes (...), em localizações e com equipamentos não controlados; aumento do volume, frequência e sofisticação das ameaças cibernéticas; quadros legais (nacionais e internacionais) e regulatórios (sectoriais) cada vez mais exigentes.(...)

CARLOS VIDINHA, RESPONSÁVEL PELA PRÁTICA DE CLOUDINFRASTRUCTURESERVICES, CAPGEMINI PORTUGAL

A percepção do ciber risco tem vindo a aumentar junto de todo o tecido empresarial português, muito devido a um trabalho que os intervenientes de segurança têm vindo a fazer de evangelização sobre o tema, em conjunto com o acréscimo de casos de ataques críticos que têm sucedido nas empresas e que levam a que os gestores tenham que de uma vez por todas acordar para o problema. Porém, ainda nos encontramos longe de um nível aceitável de segurança. Continuamos a pensar somente no perímetro físico das empresas, esquecendo que os grandes vectores de ataques passam pelos dispositivos móveis e aplicações Cloud. É importante que passemos de uma visão meramente infraestrutural física, para uma visão endpoint.

RUI DURO, PORTUGAL COUNTRY MANAGER, CHECK POINT SOFTWARE

Estudos recentes, como o Global Cyber Risk Perception Survey de 2019, mostram que mais de 80% das empresas portuguesas indicam o ciber risco como uma das maiores preocupações. Esta percentagem tem vindo a crescer de ano para ano, ainda que em termos práticos possamos não assistir a um nível de investimento compatível com a percepção. Ciberameaças como o phishing, ransomware, social engineering, entre outros, têm ganhado cada vez mais expressão, sobretudo durante o actual período da pandemia, trazendo ainda mais urgência e awareness sobre a importância do tema

DAVID SANTOS, BUSINESS DEVELOPMENT MANAGER DE CYBER SEGURANÇA, CILNET A LOGICALIS COMPANY

A preocupação para o ciber risco tem estado cada vez mais presente no quotidiano das empresas em Portugal. Actualmente não existem gestores de TI que não tenham essa preocupação, pois cada vez mais a consciência de que o risco é iminente é uma realidade, existindo cada vez mais planos e estratégias integradas multilayer contra as potenciais ameaças que uma organização pode sofrer. Ainda não é uma realidade portuguesa a existência de um CISO, na maior parte das organizações, mesmo nas de grande dimensão, mas a médio prazo caminharemos nesse sentido

NUNO NOGUEIRA, DIRECTOR PRÉ-VENDA E GESTÃO DE PROJECTOS , DECUNIFY

O ciber risco já é um tema essencial nas agendas da gestão de topo das organizações, que efectivamente o consideram como sendo um risco operacional. Isto é, um risco com o potencial de gerar um impacto negativo, e profundo, seja ele reputacional, financeiro, regulamentar ou capaz de gerar uma quebra de produção. Apesar de se assistir a um aumento da sensibilização das organizações para o ciber risco, também se assiste a uma redução considerável no nível de confiança destas na sua capacidade de geri-lo. Esta perda de confiança está muitas vezes associada à dificuldade das empresas compreenderem o impacto dos riscos a que estão expostas, a probabilidade de ocorrência desses riscos e sobre quais agir. Esta dificuldade é acrescida pela progressiva adopção das políticas de BYOD, teletrabalho, aumento do número de fornecedores e clientes, que elevam consideravelmente a exposição a potenciais ataques.(...)

MAURO ALMEIDA, MANAGER PARA A ÁREA DE SEGURANÇA DE INFORMAÇÃO E CIBERSEGURANÇA, EVERIS PORTUGAL

Tem havido uma evolução positiva de maturidade, na maioria das organizações. Além das grandes empresas, onde há algum tempo existe esse cuidado, temos vindo a verificar um aumento de preocupação com o ciber risco em PMEs, e começamos a ver nestas algum esforço para avaliar e endereçar os riscos associados à pegada digital. A cibersegurança é uma dimensão da gestão de risco, e temos visto um maior envolvimento das administrações das empresas nos processos de decisão de cibersegurança, a reboque da crescente importância do negócio digital das empresas. As administações estão, como regra, habituadas a gerir risco, e o risco associado à protecção do digital não deveria ser estranho a isso.

RUI BARATA RIBEIRO, SECURITY SALES LEADER, IBM

A consciência deste risco é cada vez maior por parte das empresas em Portugal e a cibersegurança tem vindo a subir na sua lista de prioridades. Se no passado havia quem achasse que Portugal era um país demasiado pequeno e pacato, acontecimentos recentes têm mostrado que não é bem assim. As ameaças estão presentes, tanto nas grandes como nas pequenas empresas, e podem surgir de onde menos se espera. Os ataques são cada vez mais sofisticados e o tradicional perímetro de segurança já não funciona, tendo os hackers encontrado inúmeras formas de contorna-lo. Os mecanismos de segurança têm de actuar ao nível da identidade, do dispositivo e da própria informação. É a correlação de sinais captados nestas dimensões que permite a uma organização prevenir e detectar ameaças. Este é um tema que deve unir não só as empresas do sector privado, como os organismos do sector público, de ser visto de uma forma global, tirando partido dos dados e da inteligência a uma escala mundial.

SÓNIA FALCÃO, SALES MARKETING LEAD, MICROSOFT PORTUGAL

Tem existido nos últimos anos uma maior percepção dos ciber riscos nas empresas. Cada vez mais quem gere as empresas têm a noção que correm riscos financeiros e de imagem muito relevantes. Os factores que constituem para essa maior preocupação residem no incremento da transformação digital e na necessidade de cumprimento de regulamentos por parte das empresas. A pandemia Covid-19 acelerou este paradigma, uma vez que quer a forma de trabalho, quer o negócio teve de se adaptar.

CARLOS CALDEIRA, CYBERSECURITY DIVISION MANAGER, ORAMIX

Nem todos os sectores de actividade tiveram a mesma evolução, o mesmo ritmo ou timings, no entanto, felizmente esta cultura e consciência tornou-se incontornável e um factor diferenciador entre as organizações, na medida em que isso se traduz em confiança. Registamos um progresso bastante positivo na percepção desta natureza de risco por parte das empresas em Portugal, na medida em que já é uma preocupação constante e isso traduz-se nas decisões de gestão ao mais alto nível bem como na afectação de recursos materiais e humanos. Observamos com satisfação neste últimos anos o surgimento de vários centros de monitorização e operação de segurança, além de existirem inúmeras iniciativas a nível nacional, tais como a Rede Nacional de CSIRTs, o CNCS, o Quadro Nacional de Cibersegurança, o RGPD (em concreto o RCM 41/2018) e a legislação sobre cibersegurança (lei 46/2018). Todavia, esta é uma tarefa exigente e em constante evolução já que requer a adaptação aos novos desafios e uma reavaliação contínua das medidas e controlos de segurança.

PEDRO BOAVIDA, DIRECTOR TÉCNICO (SUL), SECURNET

Os últimos ataques perpetrados e que foram amplamente divulgados nos meios de comunicação fazem-nos perceber que este risco existe e é preocupante. No entanto, devido à situação económica actual, os investimentos em cibersegurança continuam a ser demasiado baixos. Embora a sua importância seja compreendida e a consciência cada vez maior, infelizmente o investimento ainda está aquém das necessidades reais. O que é que isto significa, na prática? Que embora as empresas possuam produtos de segurança, eles não são suficientes para cobrir as necessidades que actualmente consideramos básicas para ter uma proteção aceitável. Esperamos que com o tempo as empresas alcancem um nível de maturidade que lhes permita compreender verdadeiramente os riscos que correm e, sobretudo, actuem nesse sentido.

ALBERTO RODAS, SALES ENGINEER, SOPHOS IBÉRIA

Estamos diante de uma preocupante profissionalização do cibercrime. O modelo de ataque e invasor deixou de ser grupos profissionalizados que atacavam alvos para se tornar um modelo de serviço. Quando se trata de ransomware, o ransomware-as-a-service está na ordem do dia. Nesse tipo de ataque, descobrimos que os invasores se concentram exclusivamente na infecção e, posteriormente, leiloam a infecção no mercado negro. Assim que o leilão for concluído, o vencedor recebe os detalhes de acesso à infecção, mas também uma gama de ferramentas e serviços que permitem que conclua o sequestro de informações com o mínimo de conhecimento técnico. Também deve ser observado que o modelo de criptografia / resgate de informações evolui para extorsão cibernética: ou o resgate é pago ou as informações confidenciais da empresa afectada são tornadas públicas.

JOSE CAMPO, MARKETING MANAGER IBERIA, TREND MICRO

Infelizmente, ainda existe a ideia de que a aquisição de tecnologia de ponta, como antivírus, sistemas de firewall ou outras, são suficientes para garantir a segurança. Ao longo dos anos, temos procurado mudar essa mentalidade, procurando explicar que, a par da tecnologia, é crucial trabalhar as pessoas e processos ,para que a vertente cibersegurançaseja incorporada transversalmente,sempre com base nos três pilares que a definem: tecnologia, procedimentos e,cada vez mais, pessoas. (...) No entanto,é necessário ter em consideração que o tecido empresarial português é muito heterogéneo. Existem empresas extremamente conscientes, que não prescindem de cibersegurança, algumas que a desvalorizam e outras ainda que não têm qualquer percePção do risco. E é, infelizmente, só em virtude de um primeiro incidente de segurança que, muitas vezes, começam a mudar a forma como encaram a cibersegurança. Há ainda um longo caminho a percorrer.

BRUNO CASTRO, CEO, VISIONWARE

Os últimos dois anos tem revelado sinais encorajadores na forma como as empresas em Portugal percepcionam o ciber risco. Motivadas maioritariamente por grandes eventos mediáticos de ataques que ocorreram e causaram um impacto real e sério no negócio (...) As leis governamentais têm tido um papel importante nomeadamente através da imposição do GDPR e do NIS. (...) a percepção do risco cibernético está clara e firmemente no topo das agendas. Temos assistido a uma mudança positiva no que diz respeito à consciencialização e adopção de uma gestão de risco cibernético mais rigorosa e abrangente em muitas áreas. (...) a generalidade das organizações não tem ainda maturidade suficiente para entender que o ciber risco vai muito além das violações de dados e de segurança de perímetro, tendo evoluído para esquemas sofisticados que podem causar disrupção total de qualquer negócio, estes cada vez mais digitais. (...) as organizações continuam a lutar para definir a melhor forma de articular, abordar e agir de acordo com o ciber risco na sua estrutura, tendo uma geral falta de competências internas para o fazer e um grau de maturidade muito baixo face à sofisticação e abrangência dos ciber riscos existentes. (...)

BRUNO GONÇALVES , BU MANAGER DE CYBERSECURITY & PUBLIC SAFETY, WARPCOM

(...) as empresas não têm a noção do valor da informação que possuem, faltando sensibilidade para perceber o real impacto de um roubo ou perda dessa informação. E, muitas vezes, só quando os desastres acontecem é que se tomam as medidas necessárias. Isto porque, embora exista uma maior sensibilização para o tema, quando se trata de investimentos para aumentar a maturidade da segurança das empresas, estas muitas vezes retraem-se, até ao dia em que é tarde. Segundo um estudo do Gabinete de Estratégia e Estudos do Ministério da Economia, Portugal é dos países europeus com menor volume de investimento em cibersegurança. Este cenário é preocupante quando, de acordo com o mesmo estudo, somos um dos países europeus mais vulneráveis ao cibercrime. No entanto, estando no terreno, assistimos a uma progressiva consciencialização acerca dos riscos reais por parte das empresas, sendo que este despertar, embora tardio face ao avanço do cibercrime, é fundamental para "deitar mãos à obra" e preparar as empresas portuguesas para o combate à cibercriminalidade.

CARLOS VIEIRA, COUNTRY MANAGER PARA A IBÉRIA, WATCHGUARD

Os desafios de segurança têm aumentado com o célere processo de transformação digital. Com o decorrer dos anos os gestores nacionais têm procurado estar mais conscientes dos riscos de segurança que as suas empresas e negócio estão sujeitas, contudo é notório que ainda existe um longo caminho a percorrer, em especial no mercado das pequenas e médias empresas. A falta de visão por parte dos gestores, neste capítulo tão sensível, tem contribuído para o aumento do número de incidentes e em grande parte dos casos o prejuízo moral e financeiro é enorme. É crucial que as empresas procurem profissionais especializados e soluções tecnologias adequadas à actividade, de forma a protegerem o seu negócio e não comprometerem a sua competitividade.

NUNO MENDES, CEO, WHITEHAT

CIBERSEGUROS

MERCADO EM CRESCIMENTO

OS SEGUROS DE CIBERSEGURANÇA SURGIRAM NO MERCADO NACIONAL E ACOMPANHAM A EVOLUÇÃO CRESCENTE DAS PREOCUPAÇÕES DOS CEOS NO QUE À SEGURANÇA DA INFORMAÇÃO DIZ RESPEITO. COM O AUMENTO CRESCENTE DOS INCIDENTES NO CIBERESPAÇO, ASSOCIADA AOS DESAFIOS TECNOLÓGICOS TRAZIDOS PELA PANDEMIA, CADA VEZ MAIS EMPRESAS PROCURAM SALVAGUARDAR OS PREJUÍZOS FINANCEIROS CAUSADOS PELO SEU IMPACTO. A SECURITY MAGAZINE FOI PERCEBER COMO ESTE TIPO DE PRODUTO ESTÁ A EVOLUIR E POR ONDE PASSA O SEU FUTURO.

"Cada vez há mais empresas a interessar-se por este tipo de seguros e a adquiri-los", afirma **Ricardo Azevedo, director técnico da Innovarisk**. Nos últimos anos, diz, "as empresas e instituições mais directamente envolvidas no tema da cibersegurança têm feito um trabalho muito importante em termos da chamada de atenção para este tipo de riscos, ao mesmo tempo que o número crescente de incidentes e ataques que vêm a público acabam por despertar ainda mais a consciência de que **o risco é real e pode tocar a todos**", refere.

Ainda assim **Henrique Koenders, Risk Engineering & Prevention Director da Aon Portugal** esclarece que "apesar de cada vez mais as organizações se mostrarem sensíveis ao risco cyber, o grau de penetração é ainda relativamente baixo". Contudo, diz, "**existe um grande potencial de crescimento nos próximos anos**".

Como recorda, "os primeiros aderentes à compra de ciber seguros foram sectores como as instituições financeiras e as tecnologias da informação". Com o decorrer do tempo, outros sectores "têm vindo a ser alvo preferencial de ataques cibernéticos, nomeadamente sectores como a saúde, indústria transformadora, educação, construção, energia e serviços públicos". "A falta de experiência das organizações em lidar com eventos de cibersegurança, particu-

Henrique Koenders, Risk Engineering & Prevention Director Aon Portugal

larmente em Portugal, é um desafio para nós, enquanto conselheiros em risco para fazer perceber o impacto que estes temas podem representar para a sobrevivência das empresas quando estas se materializam", diz.
Ana Duarte, diretora geral Sul da F. REGO – Corretores de Seguros, refere que "a evolução da procura por seguros de cibersegurança em Portugal tem sido lenta". Este fenómeno assenta, por um lado, "no desconhecimento de uma significativa parte das organizações dos riscos que os ataques cibernéticos representam, não só em termos imediatos, mas também reputacionais, e, por outro, em **alguma resistência à mutualização dos riscos cibernéticos"**.

PANDEMIA ACELERA PERCEPÇÃO DO RISCO

Em tempo de pandemia, o interesse por parte das empresas para este tipo de produtos tem aumentado, assim apontam todos os responsáveis contactados pela Security Magazine. **Ricardo Azevedo** salienta que "estes tempos de pandemia, ao porem a nu uma série de fragilidades na forma como as empresas têm olhado para o risco tecnológico e ao tornarem-se um terreno fértil para acções de pessoas mal intencionadas, vieram **acelerar ainda mais essa consciencialização do risco**".
Henrique Koenders sublinha que "a pandemia tem tornado clara a necessidade de avaliar o tema de uma forma abrangente". Como aponta, a COVID-19 e a situação de estado de alarme "teve impacto, a curto prazo, no ciberrisco e na gestão do mesmo". O responsável salienta que desde o início da pandemia, "diferentes seguradoras verificaram e confirmaram um aumento de ataques cibernéticos, bem como tentativas de fraude e phishing por correio electrónico". Este aumento tem levado "a um **endurecimento do mercado, sendo exigido pelos seguradores um conjunto de informações das organizações que descrevam a maturidade da mesma face ao risco em causa**".
A pandemia "acelerou alguns processos em curso, uma vez que muitas organizações passaram a depender dos canais digitais para a continuidade da sua actividade, devido às restrições nos ajuntamentos e ao confinamento", sublinha **Manuel Coelho Dias, CyberRiskSpecialist da Marsh Portugal**. Para estas empresas, "**um evento cibernético pode significar o fim da única forma de que ainda dispõem para gerarem receita**".
Ana Duarte também não tem dúvidas que a actual situação "precipitou a digitalização dos modelos de negócio de muitas empresas, que transferiram para o online uma significativa parte dos seus processos internos e externos". Esta aposta acelerada por uma realidade inesperada "acarreta riscos, e assistimos a uma escalada inédita dos ciberataques, neste período". Como aponta, "**há uma crescente consciencialização de que o mundo digital acarreta um conjunto de riscos e que as consequências de um ataque poderão ser devastadoras** para uma organização". Neste sentido, a F.Rego tem notado "uma crescente procura de soluções que garantam às empresas um apoio fundamental na resposta a um eventual incidente cibernético".

"RECUPERAÇÃO DE UM INCIDENTE CIBERNÉTICO É EXTREMAMENTE DISPENDIOSA"

Mas, afinal, porque devem as empresas investir em ciberseguros? À Security Magazine, **Ana Duarte** explica que, hoje, "a esmagadora maioria das organizações tem toda a informação relativa à sua actividade informatizada, alojada em servidores". Esta, além de "ser basilar para as suas operações, representa também um compromisso com os seus clientes, nomeadamente o de proteger a sua privacidade e de apenas utilizar aqueles dados para o fim a que se comprometeram". Um ataque "que exponha (ou retenha, com pedido de resgate) estes dados resulta, em adição a uma hipotética interrupção da actividade, na perda de confiança dos stakeholders da empresa, que vêem as suas informações pessoais exploradas ilicitamente". Como refere, "**a recuperação de um incidente cibernético é extremamente dispendiosa para uma organização**".


Ana Duarte, diretora geral Sul,F. REGO – Corretores de Seguros

Dependendo da tipologia de ataque/evento, "os custos poderão incluir o pagamento de um resgate, a notificação de todos os afectados, a defesa perante o pagamento de multas, o investimento na identificação do problema, na resolução e na reconstituição da infra-estrutura informática, a que somam as perdas por interrupção do negócio (e eventuais apostas em estratégias de relações públicas para recuperação de reputação)".
É dentro deste cenário que surge esta tipologia de produtos. O ciberseguro "garante a cobertura de todas estas despesas por parte da empresa segurada, assegurando assim um apoio verdadeiramente fundamental num momento de particular desafio para a organização afectada", diz.
A lógica do seguro passa muito "por transferir para uma outra entidade - no caso, uma seguradora - o risco de ter que fazer face a uma factura demasiado pesada, que possa provocar problemas complicados de tesouraria ou, no limite, precipitar a empresa para um cenário de insolvência", comenta **Ricardo Azevedo**. No mundo ciber, "a história recente tem provado que **o risco é real, está crescer e há empresas em todas as geografias e sectores a passarem por problemas muito sérios e caros de solucionar**". O responsável faz o exercício de pensar no custo de 15 dias de paralização para uma empresa com os sistemas informáticos comprometidos devido a um ciberataque. "Além da questão do risco financeiro, a apólice ao garantir serviços de cariz tecnológico, legal e de gestão de imagem, faz com que o segurado possa também contar com um apoio importante em áreas para as quais não tem provavelmente conhecimentos e recursos próprios e em

Ricardo Azevedo, director técnico da Innovarisk

que não tem muitas vezes sequer os contactos de especialistas para agir de forma célere".

Manuel Coelho Dias aponta que a razão do investimento num produto de ciberisco "é a mesma de outro qualquer seguro", ou seja, "consciência da existência de riscos que impactam o negócio e a necessidade de gestão desses riscos". As coberturas mais valorizadas pelos clientes "dependem da situação concreta de cada empresa e das suas especificidades, mas **temos clientes muito preocupados com a paragem da actividade por um ciberevento, mesmo na indústria produtiva**".

Nos negócios B2C "há uma grande preocupação com os custos regulatórios e indemnizações, fruto do quadro legal da protecção de dados". Transversal a todos os sectores é "a preocupação com os custos de resposta e a gestão dos incidentes, que podem ser elevadíssimos".

DEPARTAMENTO DE TI VS CIBERSEGURO

Se as empresas já contam com o seu departamento de TI, fará sentido a aposta neste tipo de produtos?

Henrique Koenders diz que há "um mito infelizmente ainda muito comum no universo nacional", que assenta em pensar-se que "o departamento de TI é suficiente para evitar todo e qualquer tipo de ataque". "Nada mais errado", diz. Como acrescenta, "**existe uma grande diferença entre vulnerabilidade e risco**", ou seja, "podemos mitigar a vulnerabilidade, mas o risco existe sempre, pelo que a transferência do presente risco tem de ser obrigatoriamente um ponto a analisar pelos CEOs".

Como esclarece, existe um conjunto alargado de razões para uma empresa investir na subscrição de uma apólice ciber. Entre as razões destaca, o facto de os dados serem um dos bens mais importantes, mas não estão cobertos por apólices de seguro de Responsabilidade Civil Comercial Geral; os sistemas são fundamentais para o funcionamento das operações diárias, no entanto, o seu tempo de inatividade não está coberto pelo seguro de perdas de exploração; a contratação de uma apólice permite aceder a um conjunto de serviços e do apoio das principais empresas de cibersegurança que garantirá a mitigação dos danos decorrentes de um evento ciber; o cibercrime é o crime de crescimento mais rápido do mundo, no entanto, a maioria dos ataques não está coberta por apólices de seguro de Responsabilidade Civil ou de Crime; o cumprimento do RGPD, nomeadamente dos processos de comunicação a terceiros cujos dados foram expostos bem como ao regulador são morosos, complicados e de custo elevado.

"A contratação de uma apólice acaba por disciplinar e implementar procedimentos para estes eventos que as organizações enfrentam", diz.

A quase generalidade das apólices "prevê o que fazer assim que um cliente detecta que ocorreu um evento ciber, que seja enquadrável na apólice, e a intervenção de um especialista que possa, desde os primeiros momentos, conter os danos e evitar acções que possam prejudicar a detecção da origem e consequências do evento".

O QUE DISPONIBILIZAM NO MERCADO

Aon: "criou um conjunto de soluções de consultoria que permite às organizações avaliar o seu grau de maturidade ao nível da cibersegurança, identificando os pontos fortes e fracos, propondo medidas que mitiguem o risco e que na consulta ao mercado permita obter uma solução que vá ao encontro às reais necessidades da organização. Para organizações de maior dimensão disponibilizamos um serviço para quantificar os riscos, identificando os cenários mais relevantes, fazendo as organizações perceber quais as maiores perdas possíveis, quais as coberturas existentes nas apólices para os mesmos (ou a falta delas). Um seguro cyber vai muito além da mera protecção e compensação de danos próprios e/ou indemnização a terceiros lesados, ou mesmo dos custos de defesa e com comunicação de crise. É um produto integrado que oferece acesso a uma rede de peritos e de resposta permanente a incidentes que de outra forma não estaria ao alcance, pelos seus custos e especificidades. No mercado nacional temos soluções "chave na mão" cujo enfoque está na prestação de serviços pré-sinistro, que visam melhorar a forma como as organizações lidam com o risco e soluções taylor made mais adequadas a organizações cuja maturidade ao nível do presente risco já é significativa.Se a primeira solução tem como principal alvo as PME, a segunda tem como alvo empresas de maior dimensão".

F. Rego: "A aposta no desenvolvimento de soluções de seguro ciber surgiu com grande naturalidade, ancorada na percepção de que um número crescente de empresas está a realizar uma transição para o mundo digital. Infelizmente, constatamos que, em muitos casos, este investimento não tem sido sustentado, dado que diversas organizações não dispõem de mecanismos de protecção e segurança adequados, o que aumenta exponen-

ESPAÇO PARA CRESCER

Quanto ao futuro e à evolução deste tipo de produtos, o responsável da Marsh diz que "o mercado nacional está muito dirigido para as PME". Para as empresas de grande dimensão "o mercado português não tem grandes soluções". A **evolução deste tipo de produtos "passará essencialmente pela subscrição digital"**.

O mesmo responsável acredita que "o futuro trará o surgimento de mais produtos dirigidos a particulares, uma vez que hoje estão muito focados ainda nos segmentos empresariais". Há ainda, nota, "uma grande indefinição em relação aos danos materiais provocados por um cibereventto (o chamado SilentCyber), e o mercado vai evoluir no sentido de uma maior definição e clareza à medida que as perdas são conhecidas".

Já o responsável da AON, sublinha que "**o produto Cyber cada vez mais se tornará num produto integrado**, onde se incluirão um conjunto alargado de serviços pré-sinistro que permitam avaliar os pontos fortes e fracos da organização, bem como serviços de apoio pós-sinistro, que incluem investigação forense, apoio legal e apoio ao nível de imagem e reputação". Como acrescenta, "as perdas de exploração serão outro dos pontos fundamentais de uma apólice ciber, não esquecendo toda a vertente de responsabilidade civil que assumirá todas as despesas legais, assim como eventuais indemnizações a pagar a terceiros lesados".

Mais do que o aspecto básico do seguro, pagando os danos, "pensamos que o serviço associado às coberturas da apólice, trazendo competências críticas em momentos difíceis para os gestores das empresas, serão muito valorizadas no futuro", refere.

Para a responsável da F.Rego, a evolução deste tipo de produto "terá de acompanhar aquilo que será a própria evolução tecnológica e as tendências da actividade económica". A pandemia "veio acelerar muitos destes processos, criando novas oportunidades, mas também fomentando novos riscos, como pudemos constatar com as centenas de ataques realizados em plataformas de videoconferência, ao longo dos últimos meses". Para continuar competitivo, "o **sector segurador terá de adaptar a sua estratégia comercial e de marketing aos nichos de mercado** que pretende atingir, numa óptica permanente de especialização.

Por fim, o responsável da Innovarisk sublinha que "a penetração deste tipo de seguros continuará certamente a crescer. Prevê-se que a importância do risco imaterial e tecnológico possa tornar-se tão ou mais importante que o risco físico, pelo que é de esperar que no futuro as empresas encarem a compra de um seguro ciber da mesma forma natural com que há tantos anos se protegem contra os riscos de incêndio ou roubo. É aliás uma tendência a que se assiste em mercados seguradores mais maduros, pelo que cremos que Portugal siga, ainda que com algum desfasamento temporal, esse mesmo caminho." •

Manuel Coelho Dias, CyberRiskSpecialist, Marsh Portugal

cialmente a sua exposição a ataques, fraudes e demais riscos cibernéticos. O seguro Cyber garante a protecção contra perdas próprias, como a violação de dados, interrupção do negócio online, danos provocados por "hackers", e a extorsão cibernética, e perante perdas provocadas a terceiros, como são exemplo a responsabilidade por violação da privacidade e em matéria de segurança de rede".

Innovarisk: "Comercializamos o seguro de riscos cibernéticos, produto que desenvolvemos para dar resposta a um dos maiores e mais complexos riscos que actualmente pendem sobre as empresas. Este seguro garante à empresa que compra uma protecção financeira para o cenário de ocorrência de um incidente ciber ou de violação de dados, quer em relação a perdas próprias que sofra, quer em relação a questões de responsabilidade civil que possam surgir. Além da tradicional vertente indemnizatória de uma apólice de seguro, permite o acesso a serviços tecnológicos, jurídicos e de comunicação e relações públicas, prestados por parceiros nossos que através de um serviço especializado podem ajudar o segurado a ultrapassar um momento de crise."

Marsh: "oferece um leque amplo de serviços de gestão de risco, que começam na avaliação e quantificação de perdas por ciberventos e terminam na transferência do risco para o mercado segurador, sob a forma de uma apólice de seguro. Os nossos serviços vão assim da consultoria de risco, nos quais é avaliada a capacidade das organizações se protegerem de ataques, gerirem ameaças e recuperarem os seus sistemas, até à corretagem dos seguros propriamente dita. Tentamos manter e gerir uma oferta completa que permita aos nossos clientes conhecerem e compreenderem os riscos do seu negócio e, quando possível, colocar ao seu dispor as melhores soluções de cobertura para esses riscos".

CENTRO NACIONAL DE CIBERSEGURANÇA

"CIBERSEGURANÇA É UMA COMPONENTE FUNDAMENTAL"

A PANDEMIA TROUXE UM AUMENTO DO NÚMERO DE INCIDENTES DE CIBERSEGURANÇA. O CENTRO NACIONAL DE CIBERSEGURANÇA DESTACA O AUMENTO DOS CIBERATAQUES, "OS QUAIS APROVEITARAM O PERÍODO DE CONFINAMENTO PARA ESTRATÉGIAS OPORTUNISTAS, TORNANDO AS ORGANIZAÇÕES E OS INDIVÍDUOS ALVOS MAIS PROVÁVEIS" .

SECURITY MAGAZINE - O MUNDO ATRAVESSA UM MOMENTO DE GRANDE TRANSFORMAÇÃO, IMPOSTA PELA ACTUAL PANDEMIA. AO NÍVEL DA CIBERSEGURANÇA OS DADOS MAIS RECENTES DO CNCS APONTAM PARA UM CRESCIMENTO DE OCORRÊNCIAS EM PORTUGAL. QUE APRENDIZAGENS SE RETIRAM DO MOMENTO QUE ATRAVESSAMOS, AO NÍVEL DA PREPARAÇÃO DAS EMPRESAS E PROFISSIONAIS?

CNCS - Durante o período de pandemia verificou-se um aumento no número de incidentes registados por parte do CERT.PT. Esta ocorrência surge em linha com outros dados nacionais e internacionais que mostram o aumento dos ciberataques, os quais aproveitaram o período de confinamento para estratégias oportunistas, tornando as organizações e os indivíduos alvos mais prováveis. Tendo em conta a circunstância em causa, julgamos que as entidades estatais e as empresas souberam responder de forma adequada, sobretudo se considerarmos as necessidades de adaptação muito rápida ao teletrabalho e, por conseguinte, uma maior dependência do digital. Recorde-se que este período serviu também para reforçar a ideia de que a cibersegurança é uma componente fundamental para a estabilidade das organizações.

O LOCKDOWN NÃO PAROU CIBERCRIMINOSOS, OS QUAIS TÊM APROVEITADO ESTA SITUAÇÃO PARA CONCRETIZAR OS SEUS INTENTOS. COMO É QUE O CNCS AVALIA O GRAU DE COMPLEXIDADE DESTES ATAQUES, A SUA ABRANGÊNCIA E O NÚMERO DE OCORRÊNCIAS NOS ÚLTIMOS MESES?

Nos últimos meses sentiu-se um aumentou do número de ataques, bem como da janela de oportunidade que espontaneamente surgiu para que os ataques ocorram e com sucesso. Contudo, não se observou que o incremento dos ataques esteja directamente relacionado com um aumento na complexidade, ainda que denotemos que alguns incidentes possam ser, naturalmente, mais complexos do que outros. Salientar ainda que observamos uma maior abrangência no que respeita às vítimas destes ataques, podendo esta estar directamente relacionada com o lockdown, contudo, é importante reter que o factor complexidade não tem uma relação directa com o número de ataques.

FACE À SITUAÇÃO DA CRISE SANITÁRIA, DE QUE FORMA É QUE O CNCS SE ADAPTOU E QUE MEDIDAS TOMOU PARA RESPONDER E MONITORIZAR EFICAZMENTE ESTES DESAFIOS CRESCENTES E GARANTIR UMA RESPOSTA ATEMPADA ÀS EMPRESAS NACIONAIS?

Em termos práticos e de execução, o CNCS garantiu a resposta necessária para monitorizar de forma eficaz a resposta à comunidade servida, adaptando-se à prática de trabalho remoto, de forma a garantir a saúde e bem-estar de todos os colaboradores e garantindo todas as medidas de cibersegurança para o efeito. Por outro lado, sentimos a necessidade de apostar fortemente na área de sensibilização, e para isso, promovemos diversas campanhas de alertas, boas práticas, documentos, tendo em conta o contexto em que nos encontramos e a exploração desta oportunidade que houve por parte dos agentes maliciosos nesta fase. Estamos a falar de campanhas que podem ser encontradas nas nossas redes sociais ou no nosso site . Durante este período, e no âmbito do Observatório de Cibersegurança, também foram lançados três boletins que pretendem divulgar os dados, tendências que ajudam a conhecer o estado da cibersegurança em Portugal nos seus vários domínios. E ainda o Relatório Riscos & Conflitos, que apresenta os principais indicadores de riscos e conflitos no âmbito da cibersegurança, tendo em conta actores, incidentes, ameaças e prospectivas, com enfoque no ciberespaço de interesse nacional português, em relação ao ano de 2019, mas também considerando anos anteriores e possíveis desenvolvimentos futuros.

AS ENTIDADES DA ADMINISTRAÇÃO PÚBLICA, OPERADORES DE INFRA-ESTRUTURAS CRÍTICAS E OPERADORES DE SERVIÇOS ESSENCIAIS E PRESTADORES DE SERVIÇOS DIGITAIS TÊM REGISTADO UM AUMENTO DO NÚMERO DE INCIDENTES AO LONGO DOS ÚLTIMOS MESES?

O número de incidentes registados pelo CERT.PT aumentou com o início do período de confinamento devido à pandemia, em Março, atingindo o seu pico em Abril e diminuindo a partir de Maio, como é possível verificar no Boletim de Julho do Observatório de Cibersegurança do CNCS. Esta situação teve um efeito relativamente generalizado pelos diversos sectores e áreas governativas considerados pelo CERT.PT. Contudo, este efeito não foi sempre uniforme. Por exemplo, o sector da Banca foi mais afectado do que outros, nomeadamente através de

campanhas de phishing, não só em termos absolutos como comparando com o ano anterior. Já o sector da distribuição e consumo de água não viu o número de incidentes registados variar significativamente em relação ao ano anterior. Além disso, face aos meses homólogos do ano anterior, alguns sectores e áreas governativas viram em certos meses o número de incidentes registados pelo CERT.PT aumentar e, noutros, diminuir.

A NOTIFICAÇÃO DE INCIDENTES POR PARTE DESTAS ENTIDADES AO CNCS É OBRIGATÓRIA. EM PORTUGAL, JÁ FORAM DETECTADAS SITUAÇÕES EM QUE ESTA NOTIFICAÇÃO NÃO FOI REALIZADA?

As entidades do sector público e privado devem comunicar sempre que sejam alvos de acções maliciosas decorrentes do ciberespaço. Qualquer empresa/organização ou cidadão pode fazê-lo através do endereço cert@cert.pt . Recorde-se que as notificações de incidentes são obrigatórias nos casos previstos na Lei nº 46/2018, de 13 de Agosto, para entidades e sectores específicos, o que não invalida a notificação voluntária de incidentes por parte das entidades, o que tem acontecido.

DO TRABALHO DESENVOLVIDO PELO CNCS, EM PORTUGAL PERCENTUALMENTE QUAIS SÃO OS PRINCIPAIS ALVOS DE ATAQUE, EM TERMOS DE SECTORES DE ACTIVIDADE E TIPOLOGIA DE EMPRESAS? QUAIS OS PRINCIPAIS MÉTODOS UTILIZADOS POR CIBERCRIMINOSOS?

No que diz respeito às tipologias de incidentes que o CNCS teve conhecimento, realçam-se as campanhas de phishing (que aproveitaram a oportunidade da pandemia como contexto). Neste sentido, denota-se um predomínio destas campanhas a entidades bancárias, mas também a empresas de serviços de streaming, ao sector dos transportes de entregas, entre outros. Ainda neste âmbito, destacam-se as campanhas de smishing, onde se percepcionou um incremento de incidentes neste contexto. Também assistimos à divulgação de plataformas digitais ou de aplicações para dispositivos móveis que aparentam divulgar informação em real time sobre a pandemia (e.g. mapas dinâmicos de contágio) mas que procuravam, na realidade, a infecção de equipamentos com malware, inclusive da tipologia ransomware. Ocorreu também um acréscimo de incidentes de compromisso de conta de utilizador que poderão estar associados, por um lado, a esquemas de phishing não percepcionados, e à divulgação pública ou em fóruns privados/especializados de leaks de informação de contas de utilizadores que resultam de exfiltração dessa informação, a partir de sistemas vulneráveis. E por último, salientar ainda os esquemas de fraude digital partilhados por email ou através de redes sociais, que divulgam iniciativas de crowdsourcing para a recolha de donativos para falsas campanhas de compra de material médico ou de protecção pessoal.

AS PESSOAS/COLABORADORES SÃO FREQUENTEMENTE APONTADAS COMO O "ELO MAIS FRACO" NUMA ESTRATÉGIA DE CIBERSEGURANÇA DE UMA EMPRESA. QUAL O PAPEL QUE OS CISOS DEVERÃO DESEMPENHAR NESTA MATÉRIA?

As pessoas e o seu comportamento enquanto utilizadores de tecnologia são efectivamentemais fáceis de explorar que os sistemas informáticos. Por isso, os CISOs têm um papel fundamental, para compreender e melhorar a cultura da organização (nível de conhecimento e preparação) em termos de cibersegurança;para desenvolver programas de sensibilização em cibersegurança adequados à organização e actuais;para ministrar essa sensibilização e/ou treino e convidar especialistas em determinadas áreas (referências para passar melhor a mensagem). Mas também têm uma forte componente de monitorização dos resultados do programa de sensibilização (através de realização de campanhas internas de phishing, análisedos incidentes de segurança, inquéritos etc.), numa lógica de melhoria contínua, (actualizar os programas para fazer face às novas ameaças, bem como melhorar nas áreas com piores resultados). Um dos principais objectivos desta posição dentro das organizações e empresas passa por que sejam elementos ativos, dinamizadores e de referência na organização no âmbito da segurança da informação.

UM ANO DEPOIS DO LANÇAMENTO DO QUADRO NACIONAL DE REFERÊNCIA PARA A CIBERSEGURANÇA E DO WEBCHECK, QUE AVALIAÇÃO E BALANÇO É POSSÍVEL FAZER DA UTILIZAÇÃO DESTAS FERRAMENTAS?

Decorrido um ano desde o seu lançamento, o WEBCHECK.PT foi utilizado na validação de mais de 18.000 domínios. Neste período, através do feedback recolhido bem como da avaliação periódica de alguns domínios, constatámos uma melhoria efetiva dos parâmetros de segurança associados às componentes de correio eletrónico e de acesso a páginas de internet de variados domínios nacionais, muitos deles no âmbito da Administração Pública e resultantes de um trabalho de divulgação e acompanhamento da utilização da ferramenta junto de diversas entidades. Ainda no decorrer deste ano, e de modo a acompanhar a constante evolução dos standards e boas práticas de segurança a aplicar, serão disponibilizadas validações adicionais bem como novas recomendações técnicas que permitam orientar os elementos responsáveis pela sua implementação.

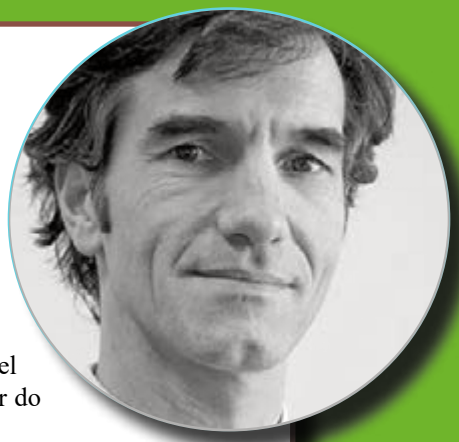
QUANTO À CONFERÊNCIA ANUAL CDAYS, QUAIS AS NOVIDADES RELATIVAMENTE À EDIÇÃO DESTE ANO?

Haverá efectivamente a C-DAYS 2020 no final do ano, num formato diferente adaptado à realidade que vivemos devido à pandemia... que muito em breve lançaremos um comunicado com os detalhes da mesma. •

2. QUAIS SÃO AS PRINCIPAIS MOTIVAÇÕES DE COMPRA POR PARTE DOS CLIENTES AO NÍVEL DE PRODUTOS/SOLUÇÕES DE CIBERSEGURANÇA?

De um ponto macro observamos que as motivações de compra advém da necessidade: de melhorar e manter o controlo sobre as operações, assegurando a manutenção das operações - esta será a necessidade mais difícil de justificar pois o seu sucesso traduz-se na ausência de incidentes; cumprir com obrigações legais, assegurando o cumprimento de legislação sectorial e interna à organização; de manter a reputação da organização, assegurando a capacidade de resposta e gestão de incidentes; suportar as iniciativas de transformação digital, estrategicamente planeadas ou fruto de uma situação de excepção, como é o caso corrente do crescendo de acessos remotos e presenças remotas decorrentes da pandemia.

PAULO PINTO, ESPECIALISTA EM CIBERSEGURANÇA, AXIANS PORTUGAL



(...)assistimos à adopção de abordagens estruturadas e sistematizadas para este tipo de tomada de decisão a nível corporativo. O elemento fundacional destas abordagens é a avaliação de risco, do nível de ciber risco incorrido pela organização, e do seu impacto no nível de risco corporativo. As organizações têm de inventariar os seus activos, identificar as ameaças a que estão sujeitas e vulnerabilidades a que estão expostas em função dos controlos de segurança existentes, determinando desta forma o impacto no negócio e a probabilidade de ocorrência de incidentes de segurança de informação e privacidade de dados. Feita esta avaliação de risco, há que decidir se o nível de risco incorrido por cada activo é compatível com o perfil de risco da organização e, caso não o seja, tomar as decisões de investimento necessárias à adopção de medidas de mitigação que concorram para essa compatibilização.Este exercício tem de ser projectado no tempo de forma evolutiva (nenhuma organização tem recursos para operar uma mudança radical no seu nível de ciber risco de forma imediata) e recorrente (porque a realidade, quer do lado dos activos quer do lado das ameaças e vulnerabilidades, é dinâmica e obriga a ciclos de reavaliação frequentes).

CARLOS VIDINHA, RESPONSÁVEL PELA PRÁTICA DE CLOUDINFRASTRUCTURESERVICES, CAPGEMINI PORTUGAL

A principal motivação é o receio de perda e violação de dados. É comum dizer-se que o petróleo da era da informação são os dados, pois se estes são um bem precioso é necessário cuidar e proteger. As empresas têm tomado consciência que a sua informação e dados está cada vez mais fora do perímetro físico das suas instalações e que isso exige maiores cuidados e atenção, não só para adoptar soluções clássicas de segurança de infraestruturas, como também de alargar essas soluções até aos dispositivos de uso profissional e pessoal dos seus colaboradores, como é o caso do telemóvel.

RUI DURO, PORTUGAL COUNTRY MANAGER CHECK POINT SOFTWARE

Durante algum tempo sentimos que havia uma "distância" entre a cibersegurança e o "negócio" propriamente dito, por parte do mercado. Com grande parte dos boards e executivos C-level a não entenderem verdadeiramente o impacto que esta área tinha no resultado do negócio como um todo. Nessa altura as principais motivações de compra estavam alinhadas sobretudo com desafios técnicos e com regulamentação. A cibersegurança era encarada como um custo, e não como um investimento. (...)com o aumento exponencial de ciberataques e estando os clientes, mais consciencializados dos custos operacionais resultantes desse tipo de problemas, muitos líderes organizacionais e as suas equipas de IT começam a repensar a forma como abordam a cibersegurança; e cada vez mais transitam de abordagens de "controlo e recuperação de danos", para uma iniciativa mais proativa e estruturada.

DAVID SANTOS BUSINESS DEVELOPMENT MANAGER DE CYBER SEGURANÇA NA CILNET A LOGICALIS COMPANY

A motivação é simples. Criar estratégias de defesa e minimização de impacto a um ataque de cibersegurança. Tem existido um investimento nestas áreas, nem sempre com um carácter holístico, mas de um modo geral vamos evoluindo na capacidade de defesa das organizações. Algo que trouxe benefícios significativos, foi o desenvolvimento de soluções de AI e ML por parte da esmagadora maioria dos fabricantes de soluções de segurança, que revolucionaram o método e a agilidade na defesa contra potenciais ataques.

NUNO NOGUEIRA, DIRECTOR PRÉ-VENDA E GESTÃO DE PROJECTOS , DECUNIFY

Grande parte das organizações adquire soluções de cibersegurança com o objectivo de aumentar o nível de maturidade de segurança de informação e cibersegurança. (...) No entanto, a aquisição de soluções de segurança motivada pelo aumento do nível de maturidade não é aquela que garante o melhor ROI para as organizações. A abordagem que defendo é a aquisição de soluções sob a perspectiva do ciber risco, tendo a avaliação de risco como pedra basilar de uma estratégia de segurança robusta e holística. Esta abordagem permite a selecção adequada das soluções a adquirir, ou implementar, e garante uma aplicação eficiente do orçamento disponível e correcta priorização do investimento com a consequente redução do ciber risco. Existirão sempre mais vulnerabilidades a mitigar e mais controlos de segurança a implementar do que aqueles que, mesmo organizações sem restrições orçamentais, serão capazes de endereçar. É por isso premente que as organizações sejam capazes de tomar decisões rigorosas e factuais sobre os principais ciber riscos aos quais estão expostas e com base nessa análise decidir, de forma eficiente, quais os investimentos a realizar em ciber segurança.

MAURO ALMEIDA, MANAGER PARA A ÁREA DE SEGURANÇA DE INFORMAÇÃO E CIBERSEGURANÇA, EVERIS PORTUGAL

(...) as equipas de IT e segurança das organizações estão já muito subdimensionadas, e coloca-se muito a questão da execução e consumo das capacidades de segurança. Nesse sentido, uma outra dimensão de interesse é a de permitir que as capacidades de segurança sejam mais consumíveis pelas organizações, por via de abordagens como "As a Service", Serviços Geridos, ou de aquisição de soluções chave na mão. Por outro lado, na área de cibersegurança era comum o fenómeno de aquisição de "point products", i.e., soluções tecnológicas que buscam endereçar uma necessidade específica; esta abordagem conduz facilmente a um aumento de custos e a maiores dificuldades de gestão, conforme vão aparecendo novas ameaças. Uma das motivações que temos encontrado é também a procura por soluções integradas, interoperáveis, de forma a proteger os investimentos feitos e a fazer.

RUI BARATA RIBEIRO, SECURITY SALES LEADER IBM

Podemos olhar para as motivações a dois níveis. Por um lado, a Transformação Digital, que está (ou devia estar) presente na estratégia de todas as organizações, veio desencadear um conjunto de mudanças ao nível da forma como as organizações se relacionam com os seus clientes, produtos que vendem, eficiência dos processos internos, como trabalham e como desenvolvem o seu capital humano. Estas mudanças, sendo essenciais à inovação e sucesso das empresas, trazem novos cenários que podem levar a uma maior exposição ao risco. Os Sistemas de Informação e as equipas de IT em geral não podem ser bloqueadores desta inovação. Têm por isso que encontrar formas de suportar e facilitar todas estas mudanças. Por outro lado, as tradicionais abordagens de segurança já não são suficientes. Não só o perímetro de segurança mudou, como para além de se proteger, as empresas têm de estar preparadas para monitorizar, detectar e conter ataques, pois eles vão acontecer. Isto implica ter a capacidade de recolher quantidades massivas de informação sobre o que se está a passar em cada momento ao nível das identidades (colaboradores), dispositivos e informação propriamente dita, assim como, analisar e correlacionar toda esta informação para identificar situações suspeitas e descobrir a sua causa. Tudo isto requer ferramentas diferentes das tradicionais ferramentas de segurança.

SÓNIA FALCÃO, SALES MARKETING LEAD, MICROSOFT PORTUGAL

As motivações dos clientes para a compra de soluções de cibersegurança, passa essencialmente por garantir que o seu negócio esteja seguro mas também que cumpra os regulamentos legais a que este está sujeito tais como o RGPD, ISO27001, PCDSS, COBIT, etc. A cibersegurança deixou de ser um "commodity" e passou a ser um pilar para o desenvolvimento de negócio digital. Não faz sentido pensarmos apenas em soluções tecnológicas, se não existem processos (que servem de alicerces para a sua continuidade consolidando-as no negócio) e pessoas (que as usam e as mantêm).

CARLOS CALDEIRA CYBERSECURITY DIVISION MANAGER, ORAMIX

Existem várias motivações, desde a vertente de vantagem competitividade/produtividade, passando pela imposição de regulamentações específicas do sector e, na realidade nacional, o recente despertar para as obrigações legais adicionais. As organizações procuram sempre renovar-se, adaptar-se e procurar formas inovadoras de expandir a sua actividade ou transpô-la para outros canais. Com efeito, há que dar estes passos com a devida prudência e com todos os mecanismos (materiais e humanos) para que esses passos ocorram com sucesso. A confiança que uma organização possui, está intrinsecamente ligada ao risco, que inclui a vertente ciber. Existe cada vez mais um certo mediatismo com os incidentes de cibersegurança e nenhuma organização quer ser notícia pelos motivos errados nem tão pouco ver a sua reputação afectada por causa de um incidente desta natureza. É também por este motivo que é necessário fazer os investimentos ajustados para assegurar que as organizações disponibilizam uma relação fiável com os seus utilizadores/clientes/utentes.

PEDRO BOAVIDA, DIRECTOR TÉCNICO (SUL), SECURNET

Como diz o ditado, "o medo guarda a vinha" e é isso que vemos com os grandes ataques que sofreram empresas de renome. Se algo assim pode ocorrer a empresas com essa dimensão, o que não poderá acontecer a qualquer uma? É este pensamento que faz com que as empresas vão deixando, aos poucos, os seus antiquados sistemas de protecção e façam a transição para sistemas de nova geração, com as protecções que actualmente permitem detectar novos ataques e investir cada vez mais – embora, como disse no ponto anterior, de forma ainda lente e insuficiente – em sistemas EDR e até MDR (serviços geridos, como o Sophos MTR). Estes sistemas actualizados tornam possível a detecção proativa de ataques nas suas fases iniciais, quando ainda não representam um verdadeiro problema, mas que, se não forem detectados, decerto passarão a ser. As empresas ainda se pautam pelo que vêem acontecer aos "vizinhos", quando o seu pensamento estratégico deveria ser a protecção imediata e acima de várias outras prioridades.

ALBERTO RODAS, SALES ENGINEER, SOPHOS IBÉRIA

A primeira motivação é óbvia: proteja-se contra ataques cibernéticos. No entanto, algumas empresas, como a Trend Micro, oferecem benefícios adicionais aos clientes. Por exemplo: as nossas soluções de patching virtual não apenas protegem nossos clientes, mas também fornecem um retorno sobre o investimento em termos de economia de custos, reduzindo os seus tempos de ciclo. Além disso, não devemos esquecer a grande quantidade de informações que essas soluções podem fornecer. Essas soluções são usadas pelos clientes não apenas para identificar riscos de segurança cibernética, mas também para identificar problemas de configuração em redes e sistemas corporativos.

JOSE CAMPO, MARKETING MANAGER IBERIA, TREND MICRO

As motivações estão, normalmente, alinhadas com a percepção do risco de cibersegurança que as organizações têm e, muitas vezes, as escolhas e investimentos feitos assentam no marketing e capacidade de venda dos fabricantes e não na análise das necessidades. O foco tem de estar na melhor relação necessidade/qualidade/preço para cada organização, porque, obviamente, as necessidades de segurança de cada organização são especificas dela própria. Na VisionWare,temos uma visão holística da segurança e, por isso, consideramos que a aquisição de produtos e soluções de cibersegurança é, apenas, uma pequena parte da solução para mitigar o risco. A capacidade de conhecer as próprias vulnerabilidades, através de processos de auditoria, assim como a formação da estrutura humana, desempenham um papel determinante. É preciso colocar este tema na ordem do dia e alertar o cliente para as várias dimensões da segurança, em que a aquisição de soluções tecnológicas nem sempre é prioritária face a outras vertentes do modelo de segurança a implementar.

BRUNO CASTRO, CEO, VISIONWARE

Se algumas organizações ainda procuram uma simples solução de protecção de um ou outro elemento dentro da sua arquitetura de segurança core, outras vão ao mercado movidas pelo medo impulsionado pelos grandes eventos mediáticos e imposições regulamentais, não sabendo muitas vezes qual o produto/solução que realmente necessitam. Existe um terceiro grupo que, por ter uma maior consciencialização do tema, e conhecendo a priori as diversas ameaças a que está exposto, foca-se não só em proteger a sua infraestrutura on-prem ou na cloud, mas também os endpoints utilizados pelos seus colaboradores dentro e fora da rede, em definir processos internos, adquirir mecanismos de detecção, de resposta e recuperação a eventos e incidentes de segurança e garantir a correcta gestão de vulnerabilidades e compliance de todos os seus sistemas. Analisando as motivações presentes nos primeiros dois grupos constata-se que existe uma dissonância entre o risco real a que estão expostas e as açções que acabam por tomar, não existindo uma abordagem ao tema de uma forma holística, levando por vezes a resultados catastróficos. Existe uma mentalidade muito agarrada à ideia de que tomando o comprimido certo – leia-se, adquirindo determinado produto ou solução –, qualquer que seja a situação que surja no futuro irá de imediato ser ultrapassada. Contudo, a verdade é que na área da cibersegurança tal não corresponde à realidade. (...) Acredito que estamos num ponto de viragem (...). que, cada vez mais, as organizações entendem a necessidade de uma abordagem holística à cibersegurança, com o desenho e arquitetura de soluções completas, adopção de serviços de segurança que apoiam as organizações a ganhar competências na gestão de todas as plataformas e garantem a existência – e execução – de processos reactivos de detecção e resposta a incidentes e processos proativos de gestão de todos as camadas de segurança que incluem a gestão de vulnerabilidades e compliance.

BRUNO GONÇALVES , BU MANAGER DE CYBERSECURITY & PUBLIC SAFETY, WARPCOM

O aumento de incidentes de segurança conhecidos, o custo e impacto financeiro, político e reputacional por estes causados tem vindo a aumentar velozmente, o que veio a intensificar as preocupações com a segurança por parte dos consumidores particulares e das empresas. Há, por isso, um aumento da procura e da sensibilidade para a temática, sobretudo no que diz respeito à protecção do endpoint, dispositivos móveis e ligações de rede, complementado pela necessidade de uma maior consciencialização dos utilizadores, muitas vezes considerados o elo mais fraco e o principal ponto de entrada dos cibercriminosos nas redes das empresas.

CARLOS VIEIRA, COUNTRY MANAGER PARA A IBÉRIA, WATCHGUARD

As principais motivações de compra de soluções de cibersegurança estão relacionadas com a protecção dos sistemas, contra ransomware, malware ou ataques de rede. Ainda assim, existem múltiplas camadas de segurança para as quais as empresas não estão sensibilizadas ou têm dificuldade em valorizar o retorno, nomeadamente em tecnologias como: UTM (Unified Threat Management), DLP (Data Loss Prevention), Backup e Disaster Recovery, Two-Factor Authentication ou Encriptação.

NUNO MENDES, CEO, WHITEHAT

PANDA SECURITY

"TODAS AS EMPRESAS SÃO SUSCEPTÍVEIS DE SER ATACADAS"

ATRAVESSAMOS UM MOMENTO DE GRANDE TRANSFORMAÇÃO A NÍVEL MUNDIAL, O QUAL TEM COLOCADO GRANDE FOCO E PRESSÃO NA CIBERSEGURANÇA. NA SUA PERSPETIVA, QUE ENSINAMENTOS PODERÃO RETIRAR OS EMPRESÁRIOS E PROFISSIONAIS NACIONAIS NO QUE DIZ RESPEITO À CIBERSEGURANÇA?

MARIA PINTO - Esta pandemia conduziu a políticas agressivas de trabalho em casa, com as empresas a fechar escritórios e enviar a maior parte - senão a totalidade - dos seus colaboradores para trabalhar em casa em período integral, quase da noite para o dia. Embora muitas empresas se tenham preparado, algumas cederam portáteis configurados à pressa ou desktops que não foram inicialmente desenhados para sair da segurança da rede local.

É importante garantir que estes dispositivos, que agora estão a regressar ao escritório, não introduzem malware e outras ameaças quando se ligam à rede da organização..

Mesmo após o término do surto do COVID-19, iremos perceber que este fenómeno provavelmente elevou o perfil do planeamento da continuidade de negócio para todas as organizações e que é extremamente importante consciencializar as forças de trabalho das empresas para as principais ameaças de segurança que podem afectar organizações de todos os tamanhos, mesmo quando estão fora do perímetro da rede da empresa, preservando ao mesmo tempo a sua produtividade.

QUAIS AS GRANDES AMEAÇAS QUE SE COLOCAM ÀS EMPRESAS PORTUGUESAS AO NÍVEL DA CIBERSEGURANÇA?

As empresas são um dos alvos dos cibercriminosos e muitas delas acabam mesmo por sofrer sérios danos na sua reputação depois de um ataque, sendo que esta consequência é muitas vezes mais difícil e morosa de reparar do que uma perda económica directa.

Entre os riscos mais frequentes e danosos estão ataques de dia zero, campanhas de phishing e ransomware. Para minimizar os efeitos, o obviamente recomendável em qualquer situação é ter em conta a segurança desde o início de qualquer desenvolvimento e implementação. As empresas tendem a investir mais na prevenção de falhas e menos em estratégias desenhadas para detectar e antever futuros ataques. É, por isso, essencial prevenir, detetar e responder a qualquer tipo de ciberameaças. A segurança deve estar presente como elemento fundamental desde o início e deve ser entendida como um processo – não um estado imóvel.

É FREQUENTE A AFIRMAÇÃO SOBRE O PAPEL E RESPONSABILIDADE DAS PESSOAS NA CIBERSEGURANÇA, SENDO OS COLABORADORES DAS EMPRESAS MUITAS VEZES APONTADOS COMO O "ELO MAIS FRACO" AO NÍVEL DA SUA SEGURANÇA. CONCORDA COM ESSA VISÃO?

Gostaria de não concordar, mas a verdade é que o maior activo das empresas é também o seu elo mais fraco e o principal vector de ataque. Muitos dos seus funcionários nunca ouviram falar de phishing nem de um ataque de ransomware, e os hackers sabem disso.

É essencial, por isso, que as empresas eduquem os seus colaboradores sobre os métodos de ataque mais comuns e como evitá-los. Coisas que a nós, que vivemos neste mundo da cibersegurança, parecem básicas, podem não o ser para os recursos humanos de muitas organizações. Alguns exemplos de conselhos básicos que lhes podemos dar: nunca clicar em links fornecidos num e-mail; ter cuidado ao abrir anexos de e-mail, ao aceder um site; prestar atenção ao URL, que deve começar por HTTPS; evitar enviar informações pessoais via e-mail e nunca dar a sua password a alguém via e-mail, entre outras medidas.

E porque sabemos que uma grande parte das violações de dados envolve credenciais perdidas, a autenticação multi-factor (MFA) é agora um pré-requisito para todas as empresas e a WatchGuard conta com um forte aliado nesta matéria, o Authpoint, fácil de implementar, de utilizar e de gerir, tudo através da cloud.

QUAL A IMPORTÂNCIA E PAPEL QUE UM CISO DEVERÁ ASSUMIR DENTRO DE UMA EMPRESA NO QUE TOCA À CIBERSEGURANÇA?

O papel do CISO é hoje mais importante do que nunca dentro de uma organização.

As empresas estão actualmente muito mais preocupadas com a segurança e privacidade dos seus dados e com conformidade regulamentar, e por boas razões. O custo médio de uma violação de dados é incomportável, quer do ponto de vista financeiro, quer reputacional.

Há uma década, era aos CIO que cabia gerir todos os aspectos de segurança e privacidade dos dados com base nos conselhos de um especialista em segurança externo ou subcontratado.

A PANDA SECURITY FOI RECENTEMENTE ADQUIRIDA PELO GRUPO WATCHGUARD. HOJE A EMPRESA É UMA SUBSIDIÁRIA INTEGRAL DO GRUPO GLOBAL SEDIADO NOS EUA, E A EMPRESA COMBINADA "PERMITIRÁ QUE OS SEUS CLIENTES E PARCEIROS ACTUAIS E FUTUROS CONSOLIDEM OS SEUS SERVIÇOS DE SEGURANÇA FUNDAMENTAIS, DA PROTECÇÃO DE REDES ATÉ AO ENDPOINT, NUMA ÚNICA EMPRESA", AVANÇA À SECURITY MAGAZINE, MARIA PINTO, DIRECTOR FIELD MARKETING DA WATCHGUARD PARA A EMEA

Mas o que passou a estar em jogo mudou essas responsabilidades para os directores de segurança da informação (CISO).
Hoje consultores líderes do conselho de administração, os CISO são responsáveis por mitigar os riscos de segurança e privacidade, manter a conformidade, educar toda a empresa acerca do panorama das ameaças e como combate-las, e ainda impedir que quaisquer incidentes afectem o negócio e manchem a rentabilidade e a reputação da empresa.

AO ANALISAR O MERCADO NACIONAL, COMPOSTO MAIORITARIAMENTE POR PMES, COMO CLASSIFICA O GRAU DE MATURIDADE EM TERMOS DE CIBERSEGURANÇA? COMO ENCARA A EVOLUÇÃO DESTA MATURIDADE NOS PRÓXIMOS ANOS?

Nesta matéria dizemos sempre a mesma coisa: todas as empresas, seja qual for o tamanho ou a tipologia do negócio, são susceptíveis de ser atacadas; a única interrogação é quando.
Não obstante, as PME portuguesas ainda têm, na sua maioria, a convicção que o cibercrime é algo que só acontece aos outros e acreditam que a sua informação é de pouco interesse ou valor para os cibercriminosos.
Este é um modo de pensar perigoso, porque os hackers utilizam frequentemente as pequenas empresas como trampolins para aceder às maiores. Aliás, os hackers não necessitam de uma razão para ter como alvo as PME – fazem-no simplesmente porque podem fazê-lo e, em muitos casos, porque são um alvo fácil.
A maioria dos ataques bem-sucedidos – sobretudo os que têm nas empresas de menor dimensão o seu alvo – ainda recorrem a técnicas básicas.
Embora algumas ameaças usem técnicas sofisticadas, a maioria das falhas de segurança em PME têm a ver com regras básicas que não são cumpridas.
A verdade é que se as organizações dedicarem esforços - e não necessariamente grandes orçamentos ou recursos - a cumprir as mais básicas práticas de segurança, conseguirão evitar a maioria dos ataques.

RECENTEMENTE, ALGUMAS EMPRESAS QUE PRESTAM SERVIÇOS CRÍTICOS E ESSENCIAIS EM PORTUGAL DEPARARAM-SE COM CIBERATAQUES COM ALGUMA ABRANGÊNCIA E IMPACTO. O QUE PODEMOS APRENDER E QUE CONCLUSÕES PODEMOS RETIRAR DESSAS SITUAÇÕES?

É um facto que o cenário de pandemia fez disparar os casos de ransomware e outros ciberataques a empresas e a infra-estruturas críticas. Temos visto inclusivamente isso a acontecer no nosso país e a organizações que, pela sua dimensão, não julgaríamos ser possível que se tornassem vítimas destes ataques.
Mas a verdade é que, com Covid-19 ou sem ele, só a simples natureza destas organizações as torna num alvo muito apetecível para os cibercriminosos.
É por isso mais importante do que nunca que os operadores de infra-estruturas críticas invistam em segurança avançada. Só assim se podem proteger das novas tendências do cibercrime, muito sofisticadas, como o ransomware, ataques de dia zero ou ataques a dispositivos móveis de empregados e membros da direcção.

> **"A SEGURANÇA DEVE ESTAR PRESENTE COMO ELEMENTO FUNDAMENTAL DESDE O INÍCIO"**

PANDA FOI RECENTEMENTE ADQUIRIDA PELA WATCHGUARD. O PROCESSO ESTÁ CONCLUÍDO?

A Panda é já hoje uma subsidiária integral da WatchGuard, uma companhia global sediada nos EUA, e a empresa combinada permitirá que os seus clientes e parceiros actuais e futuros consolidem os seus serviços de segurança fundamentais, da protecção de redes até ao endpoint, numa única empresa.

QUE IMPLICAÇÕES TERÁ ESTA AQUISIÇÃO PARA O MERCADO PORTUGUÊS? O QUE MUDOU OU ESTÁ PREVISTO MUDAR?

Destacaria como principal consequência desta aquisição o potencial de crescimento do nosso negócio.
A expansão do portfólio WatchGuard para abordar mais profundamente a segurança baseada no endpoint tem sido uma das principais solicitações da nossa comunidade de clientes e parceiros ao longo dos últimos anos e agora, com a junção das duas companhias, podemos dar resposta a essas necessidades.
A aquisição da Panda Security por parte da WatchGuard permitirá oferecer, a curto prazo, a melhor detecção e resposta de endpoints, mitigação de ameaças, antivírus para endpoints, segurança de email, patches, conformidade e encriptação de dados da sua categoria, acessíveis a toda a nossa base de clientes.
Por último, mas não menos importante, de destacar o facto de agora contarmos a nível local com uma equipa alargada, por força da junção de ambas as empresas, composta por profissionais altamente qualificados e conhecedores do mercado da cibersegurança.

E QUAIS SERÃO AS PRINCIPAIS VANTAGENS DESTA AQUISIÇÃO PARA CLIENTES E PARCEIROS?

A aquisição agora concluída da Panda Security e a subsequente integração do seu portfólio na WatchGuard Cloud representam um marco significativo e resultarão em benefícios imediatos e de longo prazo para os nossos clientes e parceiros, que terão a possibilidade de responder aos desafios comuns de complexidade da segurança, alterando rapidamente as topologias de rede, os modelos de compra e muito mais.
O foco imediato da organização resultante desta aquisição é fornecer aos parceiros e clientes de ambas as empresas acesso ao portfólio recém-expandido de soluções de segurança. Assim que os portfólios estiverem totalmente integrados, os clientes e parceiros beneficiarão de funcionalidades de detecção avançada e resposta a ameaças, alimentada por recursos modernos de IA, técnicas de perfil de comportamento e correlação de eventos de segurança de ponta, além de vantagens operacionais adicionais, como uma gestão centralizada da rede e dos endpoints.•

Panda Adaptive Defense 360

Fortaleça as suas capacidades de prevenção, deteção e remediação

Prevenção, Detecção e Resposta:

para ataques de malware e malwareless, num único agente.

Visibilidade em Tempo Real e em Retrospectiva:

informação detalhada detoda a actividade dos endpoints.

Classificação de 100% dos Processos:

99,98% através de Machine Learning, e 0.02% por especialistas da Panda.

Threat Hunting e Análise Forense:

realizados pelos analistas da Panda Security e dos nossos MSSPs.

TELEFONE: 21 041 44 00

www.watchguard.com | pandasecurity.com

SECURITYSCORECARD

ENTENDER O RISCO DO ECO-SISTEMA

FUNDADA EM 2013, A SECURITYSCORECARD, SEDIADA EM NOVA IORQUE, DEDICA-SE AO RATING EM CIBERSEGURANÇA. A TECNOLOGIA É UTILIZADA PARA AUTO-MONITORIZAÇÃO, GESTÃO DE RISCOS DE TERCEIROS, RELATÓRIOS DE DIRECÇÃO E SUBSCRIÇÃO DE SEGUROS CIBERNÉTICOS. EM PORTUGAL, EMPRESAS COMO A EDP E A TRUPHONE UTILIZAM-NA. A EMPRESA CONTA COM ESCRITÓRIOS EM PORTUGAL, BRASIL, REINO UNIDO, ALEMANHA, FRANÇA E SINGAPURA, ENTRE OUTROS, AVANÇOU À SECURITY MAGAZINE JOSÉ FERREIRA DA COSTA, REGIONAL DIRECTOR, LATAM & IBERIA DA SECURITYSCORECARD.

SECURITY MAGAZINE – O QUE É A SECURITYSCORECARD E DE QUE FORMA PODE AJUDAR AS EMPRESAS A GANHAREM VISIBILIDADE DO SEU RISCO DE CIBERSEGURANÇA?

JOSÉ FERREIRA DA COSTA - Pensem na SecurtiyScorecard como ratings (classificações) financeiros para a área de segurança cibernética. As organizações hoje são particularmente desafiadas por novos regulamentos e normas para fornecedores. Estas precisam de ter uma compreensão, não apenas do seu próprio risco, mas também dos riscos na cadeia de abastecimento e dos fornecedores com quem trabalham.

A SecurityScorecard desenvolveu um mecanismo de classificação simples - com notas de A a F. Na verdade, na SecurityScorecard estamos a analisar mais de 90 vulnerabilidades externas para mais de 1,5 milhões de empresas / entidades mapeadas em todo o mundo, adiccionado todos os dias novas empresas a este já grande número. Para cada empresa, a pontuação é actualizada diariamente, de forma instantânea e com uma tecnologia não intrusiva. Os clientes do SecurityScorecard podem rever a maturidade cibernética de qualquer um dos seus fornecedores essenciais e também acompanhar a sua própria postura cibernética.

QUANDO FALAMOS DE RISCO DE CIBERSEGURANÇA REFERIMO-NOS A QUE TIPOLOGIA DE AMEAÇAS E DESAFIOS?

Onde a SecurityScorecard entra em jogo é em dar às organizações uma visão de como o mundo as vê de fora - não apenas como é a sua segurança, mas como estão a expor-se e como todo o seu eco-sistema de fornecedores está exposto à Internet. Permite que vejam como é sua a reputação para o mundo exterior.

O maior desafio para uma empresa é entender completamente o risco do eco-sistema inteiro. Se uma empresa tem fornecedores que foram expostos ao mundo externo com vulnerabilidades críticas, podem expor potencialmente a empresa a uma violação de dados. Na realidade, 70% das violações de dados em 2019 aconteceram por meio de fornecedores.

COMO É QUE A SECURITYSCORECARD CHEGOU A PORTUGAL E POR ONDE PASSA O SEU CRESCIMENTO?

Com mais de 1.500 clientes a utilizar SecurityScorecard em todo o mundo, incluindo grandes marcas em Portugal, como EDP e Truphone, a SecurityScorecard tem duplicado a receita todos os anos desde a sua fundação.

Em 2018, SecurityScorecard expandiu a sua presença em territórios como APAC, EMEA e América Latina.

No início de 2019 fui integrado como um orgulhoso 'Scorecarder' para gerir e expandir as operações na Península Ibérica e na América Latina. Como líder global em classificações de risco de segurança cibernética, o nosso crescimento ano a ano baseia-se num produto exemplar e na satisfação do cliente.

A SecurityScorecard preocupa-se intensamente com a experiência do cliente e o valor que os seus clientes obtêm da plataforma. A SecurityScorecard tem crescido rapidamente desde que foi fundada em 2013, com sede em Nova York - EUA, com escritórios na Alemanha, França, países nórdicos, Singapura, Reino Unido, Portugal e Brasil, a empresa acabada de concluir uma rodada de financiamento da Série D no verão passado, e já arrecadou cerca de 112 milhões de dólares em financiamento até o momento.

A PANDEMIA TROUXE DESAFIOS ACRESCIDOS ÀS EMPRESAS AO NÍVEL DA CIBERSEGURANÇA. QUE APRENDIZAGENS PODEM RETIRAR AS EMPRESAS E PROFISSIONAIS DESTA CRISE SANITÁRIA?

As empresas devem compreender e estar atentas ao real risco de exposição a que estão sujeitas, seja directa ou indirectamente através de terceiros, monitorizando e colaborando com eles no dia-a-dia para serem o mais seguras possível. •

OPERADOR DE SERVIÇO ESSENCIAL

ÁGUAS DO NORTE VAI TER CENTRO DE OPERAÇÕES DE SEGURANÇA

A Águas do Norte foi identificada pelo Centro Nacional de Cibersegurança (CNCS) como um operador de serviço essencial no sector do fornecimento e distribuição de água potável, de acordo com a legislação em vigor. Para atingir o nível de segurança compatível com o serviço que presta, a Águas do Norte candidatou-se ao programa Connecting Europe Facility – Telecom, para apoio ao desenvolvimento de capacidades operacionais na área da cibersegurança e implementação da Directiva SRI. Concluído este processo, "foi aprovada a atribuição de um incentivo não reembolsável de 75% das despesas elegíveis, num projecto que se prevê ter um custo global de cerca de 300 mil euros", aponta a Águas do Norte.
O plano de cibersegurança em água (WCSP), "visa proteger toda a rede e infra-estrutura de Águas do Norte, a fim de garantir a continuidade dos serviços de abastecimento de água e de saneamento de águas residuais".
Como resultado desta acção, a Águas do Norte "poderá contar com ferramentas inteligentes para lidar com a maior parte da monitorização de eventos e resposta a incidentes".
Segundo avança, "a próxima geração sistemas de segurança terá tecnologia de auto aprendizagem incorporada, com capacidade de reconhecer padrões de eventos e bloqueios automáticos de ameaças". Através deste plano de cibersegurança, pretende-se assim "criar um Centro de Operações de Segurança (SOC) com base nas plataformas SIEM (Security Information and Event Management) e inteligência cibernética artificial (AI)".
Esse sistema "deverá monitorizar todo o ecossistema, identificando e adaptando-se continuamente às ameaças cibernéticas mais evoluídas, melhorando as capacidades técnicas e operacionais da Águas do Norte".
Essa solução deverá também "ter a capacidade de fornecer informações relevantes para as partes interessadas em segurança cibernética, nacionais e internacionais". Consequentemente "espera-se que a maturidade da segurança tecnológica da Águas do Norte aumente em coerência com a aposta estratégia que esta Concessionária do sistema multimunicipal de abastecimento de água e de saneamento do Norte de Portugal tem vindo a implementar no âmbito da digitalização dos serviços".

7 A 9 DE OUTUBRO

CYBER & CLOUD EXPO DECORRE ONLINE EM OUTUBRO

Ciber riscos, cibercrime, segurança da cloud, blockchain, ciberdefesa, RGPD e privacidade são alguns dos principais temas abordados na 1ª edição do Cyber & Cloud Expo . o evento decorre online de 7 a 9 de Outubro. A Security Magazine é media partner da iniciativa.
Ao longo de três dias mais de duas dezenas de profissionais analisam os principais temas à volta da segurança no ciberespaço. O programa do evento já está disponível no site do evento em http://www.cybercloudexpo.com/
O evento tem como sponsors a Microsoft e a APCER e como parceiros a B10Sec, Check Point, Claranet, Cloudfense, Deloitte, Eurotux, Fidelidade, Fortinet, GFI, Palo Alto, Panda, Rolling Space e Watch Guard, assim como o apoio do CNCS. A Security Magazine é media partner.
De acordo com a organização, "este evento vem preencher uma lacuna e responde a uma necessidade por parte do mercado empresarial carente de soluções e respostas para os novos desafios, riscos e oportunidades decorrentes da cibersegurança, da privacidade e do respectivo impacto nos seus negócios".
A cibersegurança "é um dos maiores desafios globais e um tema que está na ordem do dia" e que o confinamento, resultante do COVID-19, "veio expor com um inusitado números de ataques cibernéticos revelador da fragilidade das organizações".
O Cyber Cloud Expo – WebConference cuja participação é gratuita mas sujeita a registo contará com mais de três dezenas de conferências da responsabilidade de oradores e especialistas na temática.

MERCADO

CANALYS AVALIA FORNECEDORES

SETE FORNECEDORES DE CIBERSEGURANÇA ALCANÇARAM A DISTINÇÃO DE CAMPEÕES NA MATRIZ DE LIDERANÇA DE SEGURANÇA CIBERNÉTICA DA CANALYS 2020. CISCO, ESET, FORTINET E PALO ALTO NETWORKS REAFIRMARAM SUAS POSIÇÕES COMO CAMPEÕES NA EDIÇÃO 2020 E JUNTARAM-SE À JUNIPER NETWORKS, KASPERSKY E TREND MICRO.

O mercado total de cibersegurança cresceu fortemente em 2019, um aumento de 12% de acordo com as estimativas da Canalys.

"O rápido aumento do trabalho remoto devido à pandemia COVID-19 aumentou significativamente os gastos com segurança no primeiro trimestre de 2020, especialmente em endpoint e segurança em nuvem, acesso VPN e gestão de acesso de identidade, à medida que as empresas corriam para proteger os funcionários", disse o Canalys Chief Analyst, Matthew Ball.

"Novos desafios de segurança continuarão a surgir, pois, embora as organizações estejam a regressar aos escritórios em todo o mundo, um número significativo de pessoas continuará a trabalhar remotamente."

A Cisco possui uma posição de destaque no mercado de segurança e foco estratégico contínuo em serviços geridos. A empresa alocou recursos dedicados para ajudar os parceiros a construir os seus próprios serviços de segurança e o lançamento do SecureX ajudará a impulsionar os negócios MSP, fornecendo uma visão unificada do seu portfólio.

A ESET alcançou a mais elevada pontuação em benchmarks nas categorias de disponibilidade de produto, distribuição e facilidade de comunicação ao nível dos negócios.

"A posição melhorada da ESET na matriz reflecte o lançamento de um módulo de activação de MSP para impulsionamento do crescimento através de 7.000 MSPs, além de contemplar o feedback de Conselhos de Parceiros locais em roadmaps de produto, tecnologias e necessidades de clientes", justifica a empresa.

Esta abordagem colaborativa "garante que regiões em todo o mundo sejam operadas de forma inovadora e eficiente e que estejam sintonizadas com o pulsar da cibersegurança global", refere a ESET.

A Fortinet ofereceu especializações de parceiros em áreas-chave para incentivar a receita liderada por parceiros em clientes novos e existentes. A recente aquisição da enSilo e da CyberSponse será integrada à arquitectura do Security Fabric, gerando ainda mais oportunidades de parceria.

A Juniper Networks fez um grande investimento em segurança em 2019, com o lançamento da sua estratégia de Segurança Conectada.

O seu programa de nuvem MSP dedicado continuará a sua expansão em 2020.

A Kaspersky continuou a investir em seu programa de parceria e portais de parceiros, oferecendo novos modelos e equipas de suporte dedicadas para MSPs.

Tinha como alvo o recrutamento MSP e as integrações com as principais plataformas RMM e PSA.

A Palo Alto Networks foi um dos cinco principais fornecedores de segurança cibernética de crescimento mais rápido em 2019 e obteve classificações de parceiro consistentemente altas. A sua estratégia de diversificar o foco de negócios repercutiu entre os parceiros. Continuou a investir em MSPs e CSSPs.

A Trend Micro aumentou o seu investimento na sua estratégia de canal em 2019 e em 2020 e ajudou o crescimento do MSP por meio de serviços co-gerenciados e SOCaaS.

O lançamento da plataforma Cloud One este ano impulsionará os negócios SaaS em todo o seu portfólio.

A Canalys é uma empresa global de análise de mercado com um foco especial no canal que procura guiar os clientes pelo futuro da tecnologia da indústria e olhar para lá dos modelos de negócio do passado.

O Cybersecurity Leadership Matrix 2020 avaliou 17 fornecedores de cibersegurança de acordo com o seu desempenho global no canal e mercado ao longo dos últimos 12 meses.

O Matrix combina feedback recebido de parceiros através da ferramenta Vendor Benchmark da Canalys "com uma análise independente do momento de cada vendedor no canal em função do seu investimento, estratégia, desempenho no mercado e execução".

ENSINO

SPINUP DÁ ESPAÇO A FINALISTAS DE MESTRADOS DE CIBERSEGURANÇA E SEGURANÇA DA INFORMAÇÃO

SPINUP É A INICIATIVA LANÇADA PELA SECURITY MAGAZINE TENDO EM VISTA RECONHECER OS MELHORES ALUNOS FINALISTAS DE MESTRADOS DE ENGENHARIA INFORMÁTICA, CIBERSEGURANÇA, SEGURANÇA INFORMÁTICA E SEGURANÇA DA INFORMAÇÃO OU SEMELHANTES DO ANO LECTIVO 2019/2020.

Através desta iniciativa, a Security Magazine convida todos os finalistas daqueles cursos a partilhar com os seus leitores sinopses de teses ou de projectos desenvolvidos no final do mestrado.
A Security Magazine, como publicação dos profissionais de segurança, procura desta forma dar espaço e destaque aos novos e futuros profissionais, contribuindo para a sua aproximação ao sector e mercado empresarial.
Ao mesmo tempo, procura identificar e captar novos talentos em áreas que se assumem cada vez mais cruciais para as organizações e sociedades.
O Spin Up by Security Magazine é uma iniciativa que visa reconhecer os/as alunos/as que mais se destacaram no ano lectivo 2019/2020.
A Security Magazine está a aceitar sinopses de teses ou de projectos de finalistas com melhor média final de Mestrados de Engenharia Informática, Cibersegurança, Segurança Informática e Segurança da Informação ou semelhantes.

CONDIÇÕES DE PARTICIPAÇÃO

1. Ser finalista do mestrado (integrado ou 2º ciclo) em Engenharia Informática, Cibersegurança, Segurança Informática e Segurança da Informação ou semelhantes no ano lectivo 2019/2020 de um estabelecimento de ensino superior nacional - Universitário e Politécnico (público e privado)

2. Ter a melhor média final no ano lectivo 2019/2020 naquele estabelecimento de ensino e naquele mestrado

3. Será publicado um artigo único por turma, sendo a selecção em caso de médias equivalentes da responsabilidade do coordenador do curso

CARACTERÍSTICAS DO ARTIGO

Textos até 5000 caracteres com espaços, acompanhados por título, nome, cargo e fotografia do autor

COMO PARTICIPAR

Os artigos deverão ser enviados para a Security Magazine pelos coordenadores ou equivalentes do curso para o email geral@securitymagazine.pt
O envio poderá ser realizado até 30 de Março de 2021 ou data posterior mediante indicação do motivo.

ONDE SERÁ PUBLICADO

Os artigos enviados serão divulgados nas plataformas da Security Magazine online - website, newsletter e redes sociais. •

**DAR DESTAQUE AOS NOVOS E FUTUROS PROFISSIONAIS, CONTRIBUINDO PARA A SUA APROXIMAÇÃO AO MERCADO EMPRESARIAL.
IDENTIFICAR E CAPTAR NOVOS TALENTOS EM ÁREAS QUE SE ASSUMEM CADA VEZ MAIS CRUCIAIS PARA AS ORGANIZAÇÕES E SOCIEDADES**

SPINUP
Powered by Security Magazine

ESTUDO

IBM ANALISA IMPACTO FINANCEIRO DE VIOLAÇÕES DE DADOS

A IBM SECURITY ANUCIOU OS RESULTADOS DE UM ESTUDO GLOBAL QUE ANALISOU O IMPACTO FINANCEIRO DAS VIOLAÇÕES DE DADOS, REVELANDO QUE ESSES INCIDENTES CUSTAM ÀS EMPRESAS, EM MÉDIA, 3,86 MILHÕES DE DÓLARES POR VIOLAÇÃO E QUE CONTAS DE EMAIL COMPROMETIDAS SÃO O FACTOR DE MAIOR PESO.

Com base numa análise das violações de dados sofridas por mais de 500 organizações em todo o mundo, "constatou-se que 80% desses incidentes resultaram na exposição de informações de identificação pessoal (PII) dos clientes". De todos os tipos de dados expostos nestas violações, "as PII dos clientes foram também as que tiveram maior custo para as empresas".

À medida que as empresas acedem cada vez mais de forma remota a dados confidenciais, o relatório evidencia as perdas financeiras que as organizações podem sofrer, caso esses dados venham a ser comprometidos. Um outro estudo da IBM constatou que mais de metade dos colaboradores que só começaram a trabalhar a partir de casa devido à pandemia, não recebeu novas directrizes sobre como lidar com informações pessoais de clientes, apesar das alterações nos modelos de risco associados a esta mudança.

Patrocinado pela IBM Security e conduzido pelo Ponemon Institute, o "2020 Cost of a Data Breach Report" é baseado em entrevistas detalhadas a mais de 3.200 profissionais de segurança em organizações que sofreram uma violação de dados durante o ano passado.

ALGUMAS DAS PRINCIPAIS CONCLUSÕES DO RELATÓRIO DESTE ANO INCLUEM:

•**Tecnologia inteligente reduz os custos em metade:** as empresas que implementaram tecnologias de automação de segurança (que utilizam IA, analítica e orquestração automatizada para identificar e responder a eventos de segurança) tiveram menos de metade dos custos com violação de dados em comparação com as que não possuíam essas ferramentas – em média, 2,45 milhões de dólares contra 6,03 milhões de dólares

•**Pagar um resgate por credenciais comprometidas**: nos incidentes em que os cibercriminosos acederam a redes corporativas utilizando credenciais roubadas ou comprometidas, as empresas apresentaram custos com violações de dados mais elevados em quase 1 milhão de dólares quando comparados com a média global – alcançando os 4,77 milhões de dólares por violação de dados. A exploração de vulnerabilidades de terceiros foi a segunda causa com custos mais elevados para violações maliciosas (4,5 milhões de dólares) para este grupo.

• **Custos de mega-violações de dados aumentam em milhões:** nos casos em que as violações de dados comprometeram mais de 50 milhões de registos, os custos aumentaram para 392 milhões de dólares em contrapartida aos 388 milhões registados no ano anterior. Violações de dados em que 40 a 50 milhões de registos foram expostos, custaram às empresas, em média, 364 milhões de dólares, um aumento de 19 milhões de dólares em comparação com o relatório de 2019

Credenciais de colaboradores e Clouds mal configuradas – ponto de entrada preferido dos cibercriminosos Credenciais roubadas ou comprometidas e configurações incorretas da cloud foram as causas mais comuns de uma violação maliciosa para as empresas, representando quase 40% destes incidentes.

Com mais de 8,5 mil milhões de registos expostos em 2019 e cibercriminosos que utilizam e-mails e passwords anteriormente expostos numa das cinco violações de dados estudadas, as empresas "devem repensar a sua estratégia de segurança através da adopção de uma abordagem de zero-trust (confiança zero) – reavaliando a forma como os utilizadores são autenticados e o nível de acesso atribuído aos mesmos".

Da mesma forma, a dificuldade sentida pelas empresas perante a complexidade da segurança – um dos principais factores de custo das violações de dados – "está provavelmente a contribuir para que as configurações incorrectas da cloud se tornem num crescente desafio de segurança".

O relatório de 2020 revelou que os cibercriminosos utilizaram configurações incorrectas da cloud para violar redes em quase 20% das vezes, aumentando os custos com violações de dados em mais de meio milhão de dólares, para 4,41 milhões em média – tornando-o no terceiro vector inicial de ataque com mais custos analisado no relatório.

ATAQUES PATROCINADOS PELOS ESTADOS SÃO OS QUE MAIS AFECTAM

Apesar de representarem apenas 13% das violações maliciosas analisadas, os agentes de ameaças patrocinados pelos Estados foram o tipo de adversário mais prejudicial, de acordo com o relatório de 2020. A natureza altamente táctica, a longevidade e as manobras furtivas dos ataques apoiados por Estados, bem como o elevado valor dos dados alvo de ataque, geralmente resultam num maior comprometimento dos ambientes das vítimas, aumentando os custos de recuperação de violações de dados para uma média de 4,43 milhões de dólares.

Tecnologias avançadas de segurança provam ser inteligentes para o negócio. O relatório destaca a crescente divisão dos custos de violação de dados entre as empresas que implementaram tecnologias avançadas de segurança e as que estão atrasadas, revelando uma diferença na redução de custos de 3,58 milhões de dólares para as empresas com automação de segurança totalmente implementada em comparação com as que ainda não implementaram este tipo de tecnologia. A diferença nos custos cresceu 2 milhões de dólares, face a uma diferença de 1,55 milhões de dólares em 2018.

As empresas participantes neste estudo com sistemas de automação de segurança totalmente implementados, reportaram ainda um tempo de resposta a violações de dados significativamente menor, outro factor chave indicado na análise para reduzir custos com violações de dados.

O relatório constatou que IA, machine learning, analítica e outras formas de automação de segurança permitiram às empresas responder a violações de dados 27% mais rapidamente do que as empresas que ainda não implementaram automação de segurança – a última das quais exige, em média, 74 dias adicionais para identificar e conter uma violação.

A preparação para resposta a incidentes (RI) também continua a influenciar fortemente as consequências financeiras de uma violação.

De acordo com o relatório, as empresas que não possuem uma equipa de RI nem testam planos de RI, têm, em média, 5,28 milhões de dólares em custos com violações de dados, enquanto as empresas que possuem uma equipa de RI e usam exercícios teóricos ou simulações de mesa para testar planos de RI, apresentam uma redução de custos com violações de dados de 2 milhões de dólares – reafirmando que a preparação e a capacidade de resposta gera um ROI significativo em cibersegurança.

ALGUMAS CONCLUSÕES ADICIONAIS DO RELATÓRIO DESTE ANO INCLUEM:

• **Os riscos do trabalho remoto terão um custo** – com modelos de trabalho híbridos que criam ambientes menos controlados, o relatório constatou que 70% das empresas analisadas e que adoptaram o teletrabalho devido à pandemia, esperam que isso agrave os custos com violação de dados.

• **Chief Information Security Officer's responsabilizados por violações de dados, apesar do seu limitado poder de tomada de decisão**: 46% dos entrevistados referiram que o seu Chief Information Security Officer (CISO)/Chief Security Officer (CSO) foi, em última análise, responsável pela violação, apesar de apenas 27% afirmarem que o CISO/CSO é o responsável pela tomada de decisões em matéria de tecnologia e de política de segurança. O relatório constatou que a nomeação de um CISO estava associada a uma redução de custos de 145.000 dólares em comparação com o custo médio de uma violação de dados.

• **Maioria das empresas com seguro cibernético faz reclamações devido a custos de terceiros:** o relatório constatou que as violações de dados em organizações com seguro cibernético têm, em média, um custo de menos cerca de 200.000 dólares que a média global de 3,86 milhões.

De facto, das organizações que utilizaram o seu seguro cibernético, 51% aplicaram-no para cobrir despesas com honorários de consultoria e serviços jurídicos prestados por terceiros, enquanto 36% das organizações o utilizaram para restituir custos às vítimas. Apenas 10% utilizaram o valor recebido para cobrir o custo com ransomware ou extorsão.

• **Insights Regionais e do Sector:** enquanto os EUA continuam a ter os custos mais elevados do mundo com violação de dados, em média 8,64 milhões de dólares, o relatório constatou que a Escandinávia teve o maior aumento homólogo nos custos com violação de dados, com um aumento de quase 13%. O sector da saúde continua a incorrer nos custos médios mais elevados com violação de dados em 7,13 milhões de dólares – um aumento de mais de 10% em relação ao estudo de 2019. •

KASPERSKY

"FUTURO SERÁ MAIS DIGITAL"

BORJA ROBLEDO ASSUMIU RECENTEMENTE O CARGO DE ENTERPRISE ACCOUNT MANAGER DA KASPERSKY PARA PORTUGAL. À SECURITY MAGAZINE ESCLARECE QUE A EMPRESA CONTINUARÁ ATENTA "AOS DESAFIOS E EXIGÊNCIAS DO PRESENTE". COMO APONTA, "ESTE FOI UM ANO PARTICULARMENTE DESAFIANTE PARA TODOS", SENDO QUE AS "EMPRESAS DEVEM ESTAR PREPARADAS PARA UM FUTURO MAIS DIGITAL".

SECURITY MAGAZINE – O QUE IRÁ MUDAR COM A SUA ENTRADA, EM TERMOS DE POSICIONAMENTO E ESTRATÉGIA?

BORJA ROBLEDO - Na Kaspersky, continuamos empenhados em ampliar os nossos serviços de protecção, seja para uso doméstico, para empresas de pequena, média e grande dimensão, instituições políticas ou infra-estruturas críticas. Por isso, como sempre temos feito, vamos continuar a estar atentos aos desafios e exigências do presente e a adaptar a oferta em função das mesmas.

Pretendemos continuar a trabalhar com rigor e qualidade para conseguirmos garantir a melhor protecção tanto às pessoas, como às organizações, especialmente numa altura em que os cibercriminososse aproveitam da vulnerabilidade dos utilizadores e em que passamos mais tempo online. Temos reforçado a actuação com soluções de protecção e recomendações para os utilizadores – particularmente para os que estão pouco familiarizados com o online – e para as empresas, de forma a que saibam actuar e sensibilizar colaboradores em caso de um ciberataque.

QUAL A IMPORTÂNCIA QUE O MERCADO PORTUGUÊS ASSUME NO GRUPO KASPERSKY?

Portugal assume-se uma grande oportunidade para a Kaspersky e, por isso, incorporámos recentemente duas pessoas na equipa, dedicadas exclusivamente ao negócio português. Já estamos a trabalhar neste mercado há mais de dez anos e temos tido resultados excepcionais, tanto en clientes SMB, como em grandes contas de todos os sectores, como o Governo, indústria, telecomunicações, serviços públicos, entre outros.

AO NÍVEL DO SEGMENTO B2B, QUAIS SÃO AS GRANDES APOSTAS DA KASPERSKY PARA O MERCADO PORTUGUÊS?

Estamos a fortalecer o portefólio de soluções, tanto on-premise como em cloud, e a incorporar tecnologias disruptivas como ThreatAtributtionEngine, Research Sandbox, Managed EDR e outras soluções, que permitem a empresas portuguesas adoptar serviços e produtos para incrementar os níveis de segurança. A plataforma de soluções da Kaspersky pode ajudar os clientes a facilitar a gestão e operação da segurança corporativa, algo que é cada vez mais complexo.

QUANDO SE FALA DE SEGURANÇA DA INFORMAÇÃO, QUAIS SÃO OS PRINCIPAIS DESAFIOS QUE AS EMPRESAS ENFRENTAM ATUALMENTE?

Quando olhamos para o panorama geral de cibersegurança, percebemos que os cibercriminosos continuam focados em atacar empresas e pessoas. Aliás, este foi um ano particularmente desafiante para todos, onde empresas e colaboradores tiveram de reaprender a trabalhar à distância e os próprios cibercriminosos tiraram partido de todas as vulnerabilidades que estas mudanças exigiram. Portugal não foi excepção e, como mostraram alguns dos nossos relatórios, está em segundo lugar na lista dos países mais atacados por phishing, o que nos relembra da importância de sensibilizar e alertar os utilizadores, a nível individual, e também empresas, de um ponto de vista de equipas e protocolos, sobre as principais ameaças que podem encontrar quando estão online e como se devem proteger.

Com o quadro geral de ameaças a tornar-se cada vez mais diversificado, as empresas deparam-se com desafios maiores, entre os quais garantir a segurança e harmonia dos seus processos remotos, que poderão vir a tornar-se a regra e não a excepção. Desta forma, precisam de encontrar ferramentas certas para estarem cada vez mais protegidas contra incidentes relacionados com a segurança da sua informação, como ataques dirigidos e fugas de dados, por exemplo. Para algumas, a estratégia poderá passar por um maior investimento na área de IT que, tal como os últimos meses nos revelaram, é uma área que não deve ser menosprezada.

Tanto as pequenas, como as médias e grandes empresas são potenciais alvos para os ataques de hackers e é fundamental que tenham ao seu dispor os recursos certos para enfrentar qualquer tipo de cibercrime. Por outro lado, as maiores ameaças que as organizações e colaboradores podem enfrentar estão relacionadas com spam e phishing de recursos online específicos, esquemas falsos de ajuda e suporte para problemas de IT, ataques a serviços de cloud, contas desprotegidas e a utilização de uma rede WI-FI pública. Todas estas "portas de entrada" permitem a criação de uma maior superfície para ataques.

ESTAMOS A ATRAVESSAR UM MOMENTO ATÍPICO, QUAL A ANÁLISE QUE FAZ DOS IMPACTOS DESTA PANDEMIA NA ESTRATÉGIA DE SEGURANÇA DAS EMPRESAS?

A pandemia trouxe instabilidade e insegurança a todo mundo e desvendou até que ponto as empresas apostam na segurança. Assistimos – e ainda continuamos a assistir - a empresas que precisaram de redefinir as estratégias para que pudessem proteger tanto os colaboradores, como o negócio, quer com a passagem de equipas e processos para teletrabalho, quer com a implementação de planos de segurança e novos protocolos nos escritórios ou ainda com a reinvenção ou exploração de novas áreas de negócio. Além desta instabilidade, também permitiu acelerar a transformação tecnológica nas empresas, mais ainda para aquelas que não dispunham de grandes ferramentas digitais ou que não apostavam em IT. Em poucos meses, escritórios ficaram vazios e indústrias que estavam longe de se tornar "digitais" deram um grande salto ao adaptarem-se, reinventaram-se e aprenderem em conjunto a testar novos modelos (testandlearn) para que tudo continuasse a funcionar da melhor forma. E assim chegámos a um novo paradigma no mundo do trabalho. Por outro lado, devido à falta de recursos que já podia existir em muitas empresas, principalmente nas que não estavam tão familiarizadas com o digital, e aos cortes orçamentais a que a pandemia forçou, muitos gestores de IT de pequenas e médias empresas foram obrigados a procurar as melhores alternativas para garantirem a segurança de todos os processos com orçamentos muito limitados. Inclusive, de acordo com uma recente investigação que fizemos na Kaspersky, cerca de um terço dos trabalhadores envolvidos nas consequências de uma ameaça ou ataque à sua empresa, como a violação de dados, viram as vidas pessoais comprometidas, pois tiveram que falhar eventos importantes, trabalhar durante a noite e, ainda, sofreram de stress adicional. Alguns chegaram mesmo a cancelar as férias para poder dar apoio a situações de crise nas empresas. E isto é algo que tem de ser gerido melhor pelas empresas para que no futuro tenham sempre sob controlo a segurança dos seus dados, sem afectar negativamente a vida e conduta dos seus trabalhadores, nem a sua reputação.

Com uma maior dependência agora do online, deve-se, mais do que nunca, olhar de forma crítica para cibersegurança, para as áreas de IT e investir em recursos, formação e soluções especializadas que permitam evitar riscos e manter o negócio e os colaboradores em segurança. Acima de tudo, as empresas devem estar preparadas para um futuro mais digital, tendo ao seu dispor aquilo que precisam para evoluir e não ficar pelo caminho. E o futuro será, certamente, mais digital.

QUE ENSINAMENTOS PODERÃO RETIRAR AS EMPRESAS DESTA ATUAL SITUAÇÃO DE SAÚDE PÚBLICA?

Acredito que as empresas devem estar abertas a novas formas de gerir o negócio, especialmente se isso simplificar o trabalho e não colocar em causa o bem-estar dos colaboradores e o compromisso para com a empresa.

Devido à súbita mudança de paradigma, desencadeada por esta pandemia, muitas empresas estão a atravessar um período crítico.

Para subsistirem e fazerem face aos novos desafios, têm de se conseguir transformar, reinventar e, caso se justifique, alterar em grande parte a estratégia e o modo de trabalho. Para estarem adaptadas à nova realidade, as empresas devem introduzir novas ferramentas digitais ou reforçar as existentes, com o intuito de garantir um trabalho remoto eficaz e maximizar a produtividade. Refiro-me à utilização de tecnologias que facilitem as operações, tais como serviços cloud ou outros semelhantes.

Outro dos grandes leanings que podemos retirar deste novo contexto, é que deve existir uma comunicação ainda mais aberta entre as empresas e os funcionários, de forma a que todos fiquem alinhados com as transformações e saibam como agir perante diferentes cenários.

As empresas devem comunicar de forma clara, alertar os colaboradores para os potenciais riscos e garantir que todos os que estão em confinamento ou em teletrabalho têm acesso remoto em segurança. Sempre que um equipamento é utilizado fora da infraestrutura da rede e é conectado a novas redes, os riscos aumentam. E é importante que todos saibam como minimizar estes riscos. No entanto, embora o período actual levante uma série de desafios, acredito que também vai dar espaço para que novas oportunidades surjam no futuro. Com esta nova realidade, mais empresas serão capazes de conectar os seus negócios às pessoas, como nunca antes tinham experimentado, e quem sabe, redefinir o seu negócio para tirar mais partido do digital e construir relações ainda mais fortes com os clientes. Muitas vão "renascer", enquanto outras vão simplesmente ficar para trás e dar lugar a novos projectos de empreendedorismo.

QUE NOVOS DESENVOLVIMENTOS ESTÃO PREVISTOS PARA O MERCADO NACIONAL DURANTE O PRÓXIMO ANO, EM TERMOS DE NOVOS PRODUTOS, APOSTAS E INVESTIMENTOS?

Este ano, tão complicado devido à pandemia, permitiu-nos oferecer ao mercado a nossa ajuda desinteressada, sob a forma de soluções gratuitas para ambientes de saúde, públicos e privados, assim como em diferentes casos de clientes que sofreram graves ataques e que temos sido capazes de ajudar. Em 2021, continuaremos a trabalhar em iniciativas de sensibilização, introduzindo no mercado novas soluções que foram lançadas recentemente e procurando evoluir nas restantes, com o ambicioso objectivo de conseguir que Portugal desça no ranking dos países mais atacados e suba no dos países mais protegidos. •

3. A PANDEMIA TROUXE IMPACTOS À ESTRATÉGIA DE GESTÃO DE RISCO DAS EMPRESAS? QUE APRENDIZAGENS PODEM RETIRAR EMPRESÁRIOS E PROFISSIONAIS DESTA SITUAÇÃO?

Não à estratégia mas antes à sua implementação que por força das circunstâncias vê alargado o perímetro de actuação, passando a contemplar grupos de trabalhadores remotos (...). Verificamos um crescimento nas preocupações relactivas à privacidade; aumento dos ataques aos utilizadores que não estando acostumados, passaram a trabalhar de forma remota; aumento dos ataques a organizações que disponibilizam conteúdos ou serviços na internet. (...) as organizações que actuam neste contexto e cujas missões dele dependem não vão deixar de prosseguir os seus objectivos porque as adversidades aumentam, vão antes proteger as linhas de operação que as ligam aos seus clientes ou colaboradores. (...) as organizações não mudaram a estratégia de gestão do risco mas, decorrente da mesma, passaram a implementar controlos adicionais ou complementares por forma a mitigar esses riscos. Destacamos o reforço de controlos tecnológicos ao nível da segurança dos acessos remotos e da sua capacidade, assim como o reforço de controlos de gestão, por exemplo, ao nível da formação de utilizadores que, por força das circunstâncias, se encontram agora em novas situações (trabalho remoto).

PAULO PINTO, ESPECIALISTA EM CIBERSEGURANÇA, AXIANS PORTUGAL

O principal impacto (...) foi o ter acelerado de forma dramática o processo de evolução de variáveis com impacto significativo neste domínio: deslocalização de colaboradores, redefinição e digitalização de processos de negócio; desmaterialização de suportes de comunicação com clientes e parceiros; utilização de equipamentos heterogéneos e não controlados; multiplicação do volume e sofisticação de ameaças; deslocalização dos pontos de acesso à informação, entre outras. Esta evolução obrigou a uma adaptação à nova realidade num prazo de tempo inimaginável noutras circunstâncias, com impactos significativos nos níveis de investimento e esforço incorridos, bem como, por vezes, na aceitação de níveis de risco não toleráveis noutros cenários. Demonstrou a necessidade estratégica da concepção e adopção de modelos ágeis, ao nível organizacional e tecnológicos, que permitam responder de forma efectiva e eficiente a mudanças radicais de conjuntura; quer as impostas por variáveis endógenas (...), quer as que resultem de alterações de estratégia de negócio (...).

CARLOS VIDINHA, RESPONSÁVEL PELA PRÁTICA DE CLOUDINFRASTRUCTURESERVICES, CAPGEMINI PORTUGAL

Trouxe sim, levou a que os gestores não tivessem tempo para parar e pensar se valeria a pena arriscar não estar seguro. A cibersegurança, tal como o teletrabalho entrou não só no léxico como também nos hábitos de gestão. Há que relembrar que até ao momento pré-pandémico as empresas portuguesas encontravam-se num estágio muito imberbe no que toca à sofisticação de adopção de soluções de segurança informática. Com a pandemia e com o forçar de mudança de paradigma de trabalho e de atitudes por partes dos colaboradores, foi necessário reforçar e estruturar toda a infraestrutura das empresas para continuarem a ser produtivos sem colocar em causa a segurança dos mesmos. Vemos os empresários e profissionais a olharem para a cibersegurança como um ponto estratégico para a continuidade da sua actividade, juntamente com processos híbridos e flexíveis de trabalho.

RUI DURO, PORTUGAL COUNTRY MANAGER, CHECK POINT SOFTWARE

A pandemia ajudou a acentuar os desafios/impactos que a gestão de risco e consequentemente a cibersegurança têm nas organizações. E que. em certos casos, o que anteriormente era considerado como uma opção quem sabe até "evitável", presentemente e no futuro será indispensável para a continuidade do negócio. Uma das maiores aprendizagens, ou evolução de mindset para os líderes empresariais prende-se com a consideração da cibersegurança enquanto parte estratégica e integrante do negócio, e menos como "último recurso" após terem sofrido um ataque; ou seja, tem a ver com a estruturação e planificação do investimento feito nesta área. Sabemos também que para potenciar ao máximo os investimentos em cibersegurança é necessário ter os recursos certos, e que muitas vezes esse não é o cenário junto das equipas de IT dos clientes, por isso é que cada vez menos faz sentido vender produtos, e sim serviços e soluções que aportem valor real e ajudem os clientes nesta transição (daí também termos vindo a evoluir a nossa oferta e serviços).

DAVID SANTOS, BUSINESS DEVELOPMENT MANAGER DE CYBER SEGURANÇA, CILNET A LOGICALIS COMPANY

A actual pandemia trouxe impactos inesperados, tendo sido realçadas e aperfeiçoadas as soluções de acesso remoto, e protecção de dispositivos, algumas que eram inexistentes em algumas empresas. A gestão de risco com assets e informação distribuídos não era uma realidade para muitas empresas e a aprendizagem e mudança aconteceram com falta de tempo de adaptação, o que fez com que a pandemia trouxesse uma evolução e celeridade na adopção de algumas tecnologias sem ímpar. Seguramente após esta situação, estaremos ainda mais preparados para uma transformação digital mais integrada na sociedade.

NUNO NOGUEIRA, DIRECTOR PRÉ-VENDA E GESTÃO DE PROJECTOS , DECUNIFY

A pandemia teve dois impactos muito curiosos na estratégia de gestão de risco. Um negativo e outro positivo. Por um lado, (...) as empresas sofreram quebras na procura e enorme incerteza no que respeita os cenários económicos. No imediato, houve duas preocupações principais por parte das organizações: 1. Assegurar a continuidade de negócio e o teletrabalho e 2. Garantir a liquidez necessária para cumprir com os compromissos, como por exemplo o pagamento de salários. Isto fez com que as organizações acelerassem alguns programas de transformação digital e desmaterialização que, pressionadas pela necessidade de garantir a continuidade de negócio, foram implementados sem uma componente de segurança e representam, por isso, um risco elevado para as empresas, os seus fornecedores e clientes. Por outro lado, veio expor as organizações a novos riscos que não haviam ainda sido identificados ou estariam, eventualmente, mal classificados.Obrigadas a alargar o perímetro de segurança, literalmente, à casa dos colaboradores e fornecedores, as organizações viram a superfície de ataque aumentar consideravelmente. Esta situação veio influenciar positivamente as organizações, no sentido em que as sensibilizou para a importância de adotarem uma abordagem à SI que englobe processos, pessoas e tecnologia. (...) Em SI não existe uma receita one-size--fits-all e por isso há que compreender a estrutura da organização, (...). Existirão sempre mais vulnerabilidades a mitigar e controlos de segurança a implementar do que aqueles que, mesmo organizações sem restrições orçamentais, serão capazes de endereçar. É por isso premente que as organizações sejam capazes de tomar decisões rigorosas e factuais sobre os principais ciber riscos aos quais estão expostas(...).

MAURO ALMEIDA, MANAGER PARA A ÁREA DE SEGURANÇA DE INFORMAÇÃO E CIBERSEGURANÇA, EVERIS PORTUGAL

(...) Um dos impactos da presente pandemia foi o aumento expressivo do volume de negócio digital das organizações, pelo que a cibersegurança foi sem dúvida afectada. Noutra perspetiva, a segurança tornou-se também num componente de competividade, uma vez que permite às organizações alargar os serviços que presta em plataformas digitais. Outro fenónemo, foi a necessidade de lidar com os colaboradores a trabalhar de forma atomizada, e fora do "perímetro de segurança". Esta necessidade obrigou várias organizações a expor serviços, de forma a permitir a manutenção da operação – e a assumir riscos. Um conjunto de ataques de alta visibilidade ocorridos em Março e Abril demonstraram a necessidade de um pensamento mais estratégico na forma como se desenvolvem as capacidades de cibersegurança nas organizações, para poder lidar de forma rápida e eficaz com as ameaças – e, parece-nos a ter de pensar a Ciber Resiliência de uma forma integrada e proactiva, uma vez que pode ser um elemento diferenciador e importante num processo de Transformação Digital.

RUI BARATA RIBEIRO, SECURITY SALES LEADER, IBM

A actual pandemia veio acelerar um conjunto de transformações tecnológicas que há muito estavam a ser estudadas pela maioria das organizações. Os temas da mobilidade, inclusão digital, colaboração intra/inter equipas que podiam estar dispersas geograficamente já estavam nas agendas de muitas empresas, mas talvez não de forma tão abrangente como a pandemia veio a obrigar. O que a pandemia fez foi extremar estes cenários e exigir uma resposta com uma velocidade para a qual a maioria das organizações não estava preparada. Essa talvez seja a grande aprendizagem. Nos tempos que correm, com ou sem pandemia, as empresas têm de se dotar de níveis de flexibilidade e capacidade de resposta a imprevistos muito superiores aos do passado. Nesse contexto, paradigmas como a Cloud e a Inteligência Artificial são essenciais para se atingir esses objectivos.

SÓNIA FALCÃO, SALES MARKETING LEAD, MICROSOFT PORTUGAL

A estratégia de gestão de risco foi revista tornando-se mais proactiva, uma vez que o negócio não pode parar e quem gere as empresas teve de tomar decisões mais rápidas, para garantir a sua continuidade, mas sem que o seu coeficiente de risco seja alterado. Consideramos que se fez mais em 5 meses, do que em 2 anos, no que concerne á transformação digital e cibersegurança. Durante este periodo, foi observado um incremento dos ataques devido à dilatação do perímetro das organizações, uma vez que passou a ser a casa e o endpoint de cada colaborador. (...) Demonstrou-se que faz muito sentido a aposta em transformação digital e na adopção de cloud, garantindo que a sua força de trabalho esteja em qualquer lugar, a qualquer hora, online e segura. A automatização de processos constituem também uma importante vantagem competitiva, permitindo agilidade e ao mesmo tempo segurança.

CARLOS CALDEIRA CYBERSECURITY DIVISION MANAGER, ORAMIX

Veio acelerar o processo de transformação digital e de mobilidade do tecido empresarial (...) O paradigma da descentralização dos recursos e acessos revelou enormes desafios e novos riscos. Na prática esta conjuntura traduziu-se numa oportunidade de rever e apurar a estratégia de gestão de risco, especialmente para organizações em que o trabalho remoto ainda não era uma realidade, ainda que numa escala diferente, dado que também eles passaram a estar expostos a novos riscos Esta nova realidade veio demonstrar de forma inusitada que muitos sectores de actividade se podem adaptar, até com algumas vantagens, a este formato de trabalho remoto, total ou parcial.

PEDRO BOAVIDA, DIRECTOR TÉCNICO (SUL), SECURNET

Definitivamente. Há vários anos que os fabricantes de segurança falam do "perímetro evanescente" – ou seja, o fenómeno de que na verdade já não há perímetro – e a pandemia fez com que isto se tornasse numa realidade completa, uma vez que alargou o espectro do teletrabalho a praticamente todos os tipos de empresas e qualquer perfil de colaborador. Vemos empresas com sistemas tradicionais que não protegem os seus utilizadores, nem possuem informações sobre eles, apesar de estarem em casa há semanas... e por algo tão simples quanto a falta de contacto com a consola de controlo, e isto é algo que não acontece na Cloud. Assim, felizmente, possuíamos clientes absolutamente relutantes em usar sistemas Cloud que, devido à pandemia, adoptaram esses modelos e ultrapassaram todos os problemas do passado, e apesar de migrarem em marcha forçada agora reconhecem a grande vantagem que estas soluções oferecem. Também vimos como as empresas expandiram a sua capacidade de utilizadores VPN em mais de 500% (...). com esta nova realidade podemos constatar que os serviços em Cloud vieram para ficar, tal como o teletrabalho e a necessidade de sistemas com o "zero trust" como filosofia de abordagem à arquitetura segurança (...)

ALBERTO RODAS, SALES ENGINEER, SOPHOS IBÉRIA

A pandemia forçou o teletrabalho em massa. Isso teve consequências indiscutíveis do ponto de vista da cibersegurança, já que muitas empresas tiveram que adoptar esse modelo do zero, arriscando-se ao expor sistemas que não possuíam as medidas de segurança correspondentes. Diante dessa situação, as empresas derivaram rubricas orçamentárias para alcançar a segurança adequada no modelo de teletrabalho e a procura por serviços de segurança tem claramente aumentado. A lição aprendida é que o modelo de "segurança ou design padrão" está correcto. Ou seja, a segurança cibernética deve ser considerada durante a concepção de um projecto ou de qualquer serviço como mais um pilar fundamental

JOSE CAMPO, MARKETING MANAGER IBERIA, TREND MICRO

A pandemia teve um impacto tremendo no que respeita o cibercrime e os dados disponíveis comprovam-no. A necessidade de colocar o negócio e a operacionalidade – recursos humanos – disponíveis via internet veioacelerar, de forma brusca, o processo de digitalização de muitas empresas, expondo-as, de repente, ao mundo digital e de uma forma para a qual não estariam ainda preparadas. As empresas reagiram ao contexto, mas ficaram expostas a novos riscos, sem que tivessem as ferramentas e capacidade para os gerir. Isto explica o aumento significativo do número de casos de ciberataque detectados. A pandemia veio colocar o tema do teletrabalho em cima da mesa. Uma grande maioria das empresas não estava preparada para gerir os cibe riscos que vieram com esta nova realidade. Felizmente, tivemos empresas que investiram, atempadamente, em cibersegurança e estavam mais preparadas, e outras que procuraram, reactivamente, corrigir a sua estratégia, à medida que passavam por este novo enquadramento social, o que, não sendo o ideal (na óptica da prevenção), é um ponto de partida. Infelizmente, deparámos-nos com muitos casos em que a falta de investimento e maturidade no tema da cibersegurança, essencialmente por desconhecerem o seu nível de segurança, provocaram graves dissabores e perdas efectivas, com efeitos directos no negócio.

BRUNO CASTRO, CEO, VISIONWARE

Obrigou quase todas – se não todas – as empresas a adaptarem-se rapidamente a este novo normal, forçando-as a ter de transformar em tempo record a sua organização, a gestão interna, os processos e os meios tecnológicos. Durante esta transformação foi evidente que a generalidade das organizações não estava preparada, ou pensada, para fazer face aos riscos inerentes a um cenário de pandemia como o actual. (...) este momento único deixou claro que as organizações que melhor estavam preparadas (...) mais facilmente se adaptaram e em pouco ou nada viram a operação do seu negócio ser afectada.

Desta forma, as principais aprendizagens deverão ser:

1. **Um plano elementar é melhor do que um "não-plano"**
2. **A segurança e resiliência cibernéticas vão muito para além do IT**
3. **A identificação, acção e comunicação são pilares essenciais**
4. **Nenhuma organização é um super-herói**

BRUNO GONÇALVES , BU MANAGER DE CYBERSECURITY & PUBLIC SAFETY, WARPCOM

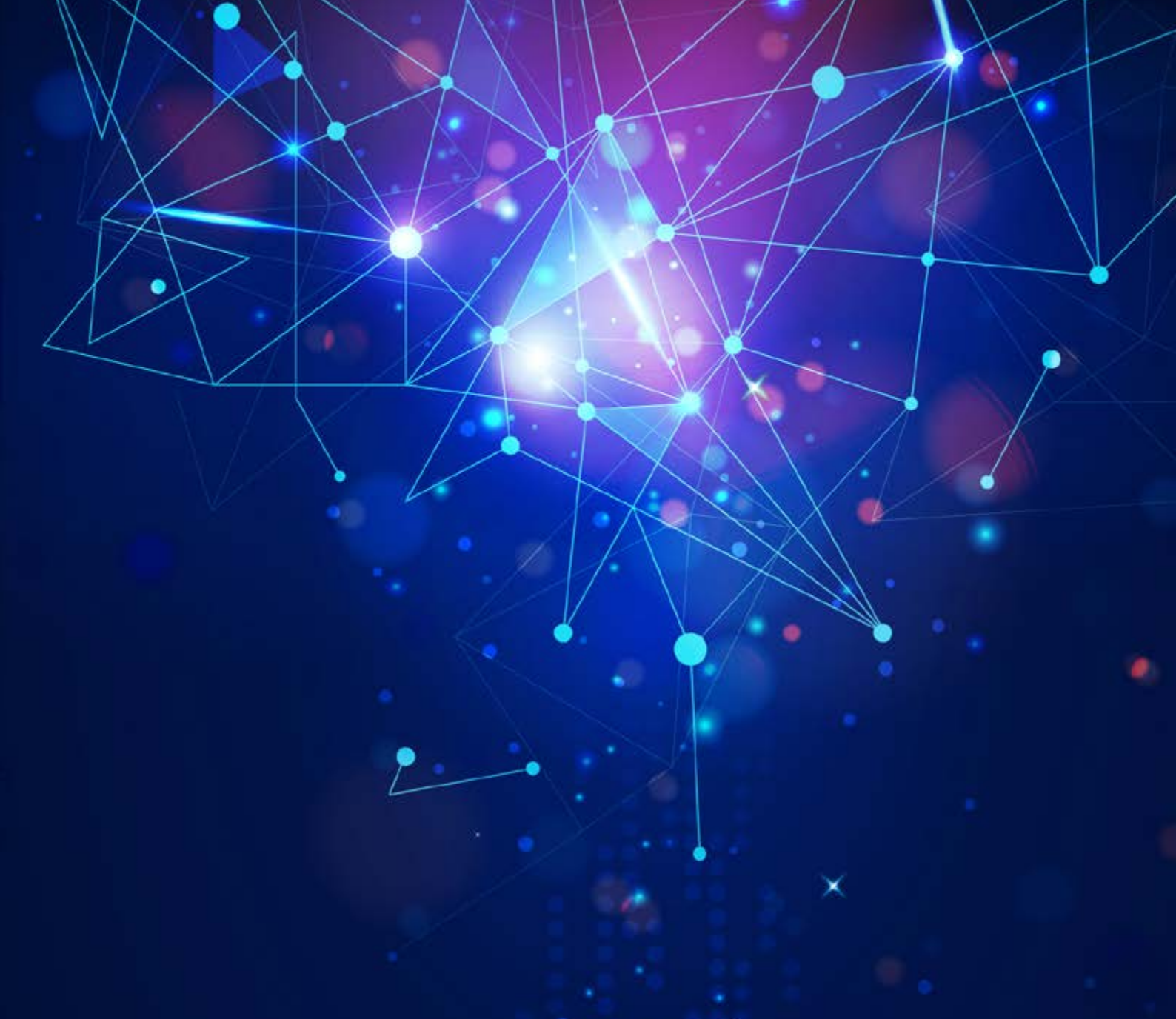
Sem dúvida. De repente, o local de trabalho das empresas passou a ser composto por dezenas de funcionários espalhados pelas suas casas, em regime de teletrabalho, com a pandemia a forçar milhares de organizações portuguesas e no mundo a tornar o trabalho remoto o seu modus operandi, no espaço de algumas semanas. O normal passou a ser trabalhar na mesa da cozinha ou no sofá da sala, mas para os profissionais mais acostumados a trabalhar no escritório, este era um jogo totalmente novo sobre cujas regras ainda havia muito desconhecimento. Embora muitas empresas se tenham preparado, algumas cederam portáteis configurados à pressa ou desktops que não foram inicialmente desenhados para sair da segurança da rede local, o que elevou exponencialmente a sua exposição a ciberameaças. Mesmo quando esta crise terminar, iremos perceber que este fenómeno provavelmente elevou o perfil do planeamento da continuidade de negócio para todas as organizações e que é extremamente importante consciencializar as forças de trabalho das empresas para as principais ameaças de segurança que podem afetar organizações de todos os tamanhos, mesmo quando estão fora do perímetro da rede da empresa, preservando ao mesmo tempo a sua produtividade.

CARLOS VIEIRA, COUNTRY MANAGER PARA A IBÉRIA, WATCHGUARD

Sim, creio que a pandemia trouxe impactos notórios à estratégia de gestão de risco das organizações. A urgência em adoptar processos de trabalho exclusivamente digitais e remotos levou a um aumento do ciber-risco global, mesmo nas organizações que já tinham uma estratégia de risco definida. A maior aprendizagem é que os negócios podem, em certa medida, ser realizados remotamente, mas que existem novos vetores de risco que devem ser considerados na estratégia de segurança de cada organização.

Neste novo paradigma, é fundamental que os decisores sejam devidamente aconselhados e ajam rapidamente no sentido de identificarem os novos vectores de risco, encarando a tecnologia de segurança necessária como um investimento.

NUNO MENDES, CEO, WHITEHAT



SECURITY MEETUP

CICLO DE CONFERÊNCIAS

PANDEMIA & SEGURANÇA

DEZEMBRO.2020

+INFO: GERAL@SECURITYMAGAZINE.PT

SECURITY MAGAZINE
REVISTA DOS PROFISSIONAIS DE SEGURANÇA

VIEIRA DE ALMEIDA

"A PALAVRA CHAVE É PREPARAÇÃO

QUAIS OS PRINCIPAIS DESAFIOS QUE A ACTUAL PANDEMIA TROUXE AO NÍVEL DA CIBERSEGURANÇA?

TIAGO BERNARDO - A Vieira de Almeida (VdA) é uma firma internacional de referência, destacando-se por um track-record impar na assessoria jurídica empresarial e pelo seu carácter inovador. Com cerca de 450 colaboradores, a maior do mercado português, assegurou a implementação de teletrabalho de toda a equipa, a nível nacional e internacional.

Este projecto de transformação digital, com inicio em 2019, para além das questões operacionais, teve um enorme foco em soluções que protegessem o nosso eco sistema, garantindo aos nossos colaboradores um ambiente flexível, mas garantindo também a segurança do mesmo.

Durante a pandemia todos esses sistemas foram postos à prova, demonstrando a resiliência dos mesmos.

Na sua maioria, para além dos ataques que diariamente sofríamos, houve um aumento exponencial de ataques de phishing sob a temática "Covid 19".

Muitos destes ataques foram bloqueados pelas ferramentas implementadas que nos garantiram bastante protecção e, os que por algum motivo não eram detetados pelos nossos sistemas devido à sua sofisticação, foram parados graças à consciencialização dos nossos utilizadores que nos reportaram situações suspeitas de imediato. Esta consciencialização advém de inúmeras iniciativas internas levadas a cabo pela Direcção de Tecnologias (DTEC) nos últimos três anos, que, sob a forma de eventos internos sobre diversas temáticas de cibersegurança, reforçou o alerta para este tipo de ataques de engenharia social.

> "DURANTE A PANDEMIA TODOS ESSES SISTEMAS FORAM POSTOS À PROVA, DEMONSTRANDO A RESILIÊNCIA DOS MESMOS"

QUE MEDIDAS FORAM DESENVOLVIDAS PELA SUA EMPRESA/ORGANIZAÇÃO AO NÍVEL DA CIBERSEGURANÇA?

A maior parte das medidas já tinham sido implementadas previamente, fruto das necessidades típicas de trabalho remoto para colaboradores que viajam bastante.

Contudo, a massificação do teletrabalho, sobretudo no período de confinamento obrigatório, obrigou a um esforço adicional por parte de toda a DTEC e das equipas que a compõem.

Desde a nossa primeira linha de ServiceDesk, até à área de Enterprise Solutions, todos contribuíram para que os nossos utilizadores se sentissem seguros e aptos para desempenhar as suas funções.

QUE LIÇÕES PODEM AS EMPRESAS E OS PROFISSIONAIS RETIRAR DESTA CRISE SANITÁRIA NO QUE SE REFERE À CIBERSEGURANÇA?

A palavra chave é preparação. Esta pandemia ensinou-nos que não existem cenários impossíveis, e que a preparação de todas as equipas, sistemas e colaboradores é um factor de sucesso para se conseguir ultrapassar uma situação tão grave como aquela que o mundo estava e está a sofrer.

Graças à visão dos membros dos órgãos de gestão da VdA, a cibersegurança passou a fazer parte do dia-a-dia de todos, e todos colaboramos para garantir a resiliência dos nossos sistemas e dos nossos processos.

A consciencialização e o forte investimento em sistemas trouxe uma adaptação rápida e eficaz de todos os envolvidos.

COMO ESTÁ ORGANIZADA A CIBERSEGURANÇA DENTRO DA VOSSA EMPRESA (QUANDO FOI CONSTITUÍDO, QUANTOS ELEMENTOS TEM, A QUEM REPORTA, PROJECTOS DESENVOLVIDOS)?

A área de Systems & Cybersecurity foi criada em 2017 como forte aposta da Direcção de Tecnologia materializando a visão estratégica da VdA.

A coordenação desta área ficou a meu cargo, contando neste momento já com quatro colaboradores dedicados 100% à mesma.

Um dos grandes projectos em desenvolvimento este ano é a certificação ISO 27001 que neste momento já está muito avançada. Com esta certificação a VdA quer continuar a ser uma referência também na área da cibersegurança. •

TIAGO BERNARDO É COORDENADOR DE SYSTEMS & CYBERSECURITY DA VIEIRA E ALMEIDA. A ÁREA QUE LIDERA FOI CRIADA HÁ TRÊS ANOS E NESTE MOMENTO CONTA COM QUATRO ELEMENTOS. A EMPRESA ESTÁ EMPENHADA NO PROCESSO DE CERTIFICAÇÃO DA ISO 27001. "COM ESTA CERTIFICAÇÃO A VDA QUER CONTINUAR A SER UMA REFERÊNCIA TAMBÉM NA ÁREA DA CIBERSEGURANÇA", AVANÇA O RESPONSÁVEL À SECURITY MAGAZINE.

TALKDESK

"A SEGURANÇA É UMA DAS ÁREAS PRIORITÁRIAS"

TALKDESK É UMA EMPRESA QUE "AJUDA OUTRAS EMPRESAS A CRIAR O SEU PRÓPRIO CENTRO DE CONTACTO", APOIADO NUM SERVIÇO TOTALMENTE NA CLOUD. EDGAR PIMENTA, INFORMATION SECURITY DIRECTOR DA EMPRESA, ADIANTOU À SECURITY MAGAZINE QUE "A SEGURANÇA DA INFORMAÇÃO DOS SEUS CLIENTES E DA SUA PRÓPRIA INFORMAÇÃO É PRIORIDADE".

COMO NASCEU A TALKDESK E QUAL É ACTUALMENTE A SUA OFERTA NO MERCADO NACIONAL E INTERNACIONAL?

EDGAR PIMENTA – A Talkdesk nasceu a partir de um hackathon, no qual os fundadores da Talkdesk participaram e ganharam. Rapidamente perceberam que a ideia podia ir mais além e criaram a Talkdesk.

Somos uma empresa que ajuda outras a criar o seu próprio centro de contacto e relação com a sua base de clientes. Tendo o cliente em mente como primeira referência de gestão, a nossa plataforma é totalmente personalizável para permitir que, de um ponto de vista operacional, cada empresa possa adaptá-la de forma a melhor atender às suas necessidades. Oferecemos soluções de contexto, roteamento, relatórios e análise de dados suportadas em Inteligência Artificial, que, entre outras funcionalidades, permitem recolher informação sobre o histórico do cliente que está a efectuar o contacto, disponibilizando-a, em tempo real, ao agente previamente seleccionado para que este melhor possa endereçar as suas solicitações.

Como resultado, as interacções tornam-se mais eficazes e personalizadas: os tempos de resposta diminuem, os recursos existentes são rentabilizados e a agilidade dos centros

de contacto como um todo aumenta.
É esta abordagem que nos permite assegurar a satisfação dos clientes e que se traduz em ganhos de produtividade para as empresas. Sendo uma empresa que fornece um serviço na cloud, oferece serviços de forma global, não diferenciando o mercado nacional e o mercado internacional em termos de oferta.

NUMA ALTURA EM QUE A APOSTA EM SERVIÇOS NA CLOUD É, CADA VEZ MAIS, UMA REALIDADE, A SEGURANÇA E PROTECÇÃO DE DADOS ENTRA EM CENA. QUE DESAFIOS ENFRENTA A TALKDESK A ESSE NÍVEL E A QUE TIPO DE CIBER AMEAÇAS ESTÁ SUJEITA?

A Talkdesk nasceu na cloud e isso permitiu-lhe criar de raiz um conjunto de medidas de segurança de forma nativa, ao invés de ter de adaptar-se de soluções mais "legacy" para soluções na cloud.
Os desafios da Talkdesk e as ameaças a que está sujeita não são muito diferentes das restantes empresas com forte presença na cloud. Contudo, pautamo-nos pela melhoria constante e pela prevenção, monitorizando constantemente as ameaças existentes e tentamos identificar novas ameaças de forma a garantir um nível de segurança adequado. São exemplos disso os DoS (Denial of Service) e os ataques de phishing para os quais temos medidas implementadas (obviamente distintas para cada ameaça).
Em termos de protecção de dados, um dos desafios é a evolução da legislação mundial em termos de privacidade. O RGPD foi uma legislação inovadora e, na sequência disso, vários países têm vindo reforçar a sua legislação sobre privacidade, como é o caso do Brasil e dos EUA. Neste último caso, o estado da Califórnia foi um dos estados que mais depressa avançou neste tema, com o CCPA (California Consumer Privacy Act).

DE FORMA A ASSEGURAR A PROTECÇÃO DE INFORMAÇÕES E DADOS DE CLIENTES, NOMEADAMENTE DURANTE O PROCESSO DE MIGRAÇÃO DE SERVIÇOS CRÍTICOS, QUE MEDIDAS FORAM DESENVOLVIDAS PELA TALKDESK? CONTAM COM UMA EQUIPA DEDICADA A ESTA ÁREA? QUE TIPO DE SOLUÇÕES/PROJECTOS FORAM DESENVOLVIDOS DE FORMA A GARANTIR QUE A SEGURANÇA DOS DADOS NÃO É COMPROMETIDA E AS OPERAÇÕES DAS EMPRESAS NÃO SÃO AFECTADAS?

Para a Talkdesk, a segurança da informação dos seus clientes e da sua própria informação é prioridade, pelo que utiliza diversas medidas nesta frente. Medidas essas que são constantemente monitorizadas, verificadas e se necessário, melhoradas. A aposta em certificações internacionais tais como a ISO27001 (Gestão de Segurança da Informação), PCI-DSS e a ISO22301 (Gestão de Continuidade de Negócio) vem ajudar a suportar esses processos de melhoria continua para além de serem verificações independentes.
A Talkdesk tem equipas dedicadas especificamente à segurança e que actuam em várias vertentes, desde as vertentes mais de Governance (que inclui, por exemplo, a definição de políticas de segurança, a gestão do risco de segurança de informação, a educação das pessoas, a gestão dos sistemas de melhoria contínua de segurança e continuidade de negócio e o acompanhamento das certificações) até às vertentes mais técnicas, como a definição de arquitecturas seguras, a gestão de vulnerabilidades, a realização de penetration testings, entre outras.

QUANTOS CIBER INCIDENTES SÃO REGISTADOS PELA TALKDESK ANUALMENTE, QUAIS OS SEUS IMPACTOS NA ORGANIZAÇÃO E QUE ESTRATÉGIAS FORAM DESENVOLVIDAS PARA CONTORNAR OS MESMOS?

É política da empresa não divulgar estes dados. Contudo, para que o impacto na organização seja o mais reduzido possível, a Talkdesk tem uma política e um processo de gestão de incidentes com procedimentos e tempos de actuação consoante o tipo e gravidade do incidente. A existência de procedimentos de actuação ajuda a tornar o processo de resposta mais consistente e mais rápido. Por fim, apostamos muito na sensibilização dos nossos colaboradores para que reportem as situações identificadas o mais rapidamente possível.

A CRIAÇÃO DE UMA CULTURA DE SEGURANÇA É CADA VEZ MAIS VALORIZADA POR PARTE DAS EMPRESAS. QUE MEDIDAS TÊM SIDO DESENVOLVIDAS PARA SENSIBILIZAR E CONSCIENCIALIZAR OS COLABORADORES DA TALKDESK PARA COMPORTAMENTOS POTENCIALMENTE PERIGOSOS NO CIBERESPAÇO?

A segurança é uma das áreas prioritárias para a Talkdesk, pelo que, além de adoptarmos um conjunto de políticas de segurança, executamos um programa de educação contínua dos colaboradores para as várias ameaças e cuidados a ter – através de sessões de onboarding para novos colaboradores e sensibilização recorrente através de vários métodos tais como vídeos educativos, pequenos jogos, questionários e outros. Adicionalmente, a Talkdesk associa-se a "eventos" internacionais, tais como o mês da cibersegurança (Outubro), onde reforçamos a comunicação sobre a área.

POR ONDE PASSA A EVOLUÇÃO DA TALKDESK EM MATÉRIA DE CIBERSEGURANÇA?

A Talkdesk pauta-se, tanto na cibersegurança, como noutras frentes de negócio, pela melhoria contínua e monitorização do contexto. A cibersegurança é algo que está em constante alteração e é preciso que as empresas se continuem a adaptar ao contexto e aos riscos (novos e já existentes) que daí podem surgir.•

EXPLOIT HUNTERS

EXPLOIT HUNTERS QUER PROMOVER A DEMOCRATIZAÇÃO DA SEGURANÇA

A EXPLOIT HUNTERS FOI FUNDADA O ANO PASSADO E QUER TER EM PORTUGAL A SUA BASE DE CONTROLO PARA OUTROS PAÍSES. PAULO GARCIA, CEO , AVANÇOU À SECURITY MAGAZINE QUE A EMPRESA ESTÁ A EXPANDIR-SE PARA OS ESTADOS UNIDOS, REINO UNIDO E IRLANDA. A EMPRESA DESENVOLVEU A ISMAC, UMA NOVA TECNOLOGIA QUE "PERMITE A DEMOCRATIZAÇÃO DO MESMO NÍVEL DE SEGURANÇA QUE AS EMPRESAS DA FORTUNE 500 USAM PARA SE PROTEGEREM, POR UMA FRACÇÃO DO PREÇO". O RESPONSÁVEL ALERTOU PARA O AUMENTO DE CIBERATAQUES NA PANDEMIA E SALIENTOU QUE AS "EMPRESAS QUE NÃO TIVEREM O CUIDADO AGORA EM CONTRATAR UMA FORMA EFECTIVA DE PROTECÇÃO DE DADOS ACABARÃO POR PERDER CLIENTES".

SECURITY MAGAZINE – QUANDO SURGIU A EXPLOIT HUNTERS?

PAULO GARCIA JR – A Exploit Hunters foi fundada por mim e pelo Hugo Moreira, no início de 2019, com carácter "stealth", com foco em reunir mentes brilhantes do mercado de inteligência e cibersegurança de diferentes países, assim como em criar uma solução única e escalável para os desafios criados pela RGPD e, principalmente, em promover a democratização do mesmo nível de segurança que as gigantes da Internet podem usar para proteger-se, mas por uma fracção do preço.

Por esse motivo, no início desse ano conhecemos a Aristi Labs, uma startup indiana, fundada por Urkarsh Bhargava. Esta já tinha o seu sistema a ser utilizado pelo Centro de Comando do Departamento de Satélites do Exército Indiano, localizado em Bhopal, além de ter uma tecnologia bastante complementar com a nossa. Por essa razão, resolvemos comprar a empresa e trazer a sua equipa, com o Utkarsh servindo agora como nosso CTO global.

Além disso, trouxemos o Daniel Arruda, advogado especialista em LGPD e RGPD para auxiliar-nos na parte de compliance, e professor de Direito Societário e Mercado de Capitais da FGV, a principal think tank brasileira.

Após essa parceria, desenvolvemos, a partir das nossas plataformas, uma tecnologia nova, chamada ISMAC (Integrated Security, Monitoring and Compliance), que une SIEM com Inteligência Artificial, SOC-over-Cloud e Compliance com a RGPD, tudo pré-configurado e sem nenhum custo de setup ou escondido.

O QUE LEVOU A EMPRESA A ENTRAR NO MERCADO PORTUGUÊS?

Vivi um tempo em Portugal e tenho origem portuguesa, e após ver que o país está a olhar de forma positiva para novos empreendedores com projectos realmente inovadores e escaláveis, decidimos apostar no país.

Além de ser uma excelente porta de entrada para outros países da Europa, temos um carinho muito especial pelos

portugueses e esperamos poder dar a nossa pequena contribuição para tornar o país numa referência mundial em cibersegurança.

QUE SERVIÇOS DISPONIBILIZA A EMPRESA EM PORTUGAL E EM QUE MEDIDA SE DIFERENCIA NO MERCADO?

Desenvolvemos uma tecnologia nova, chamada ISMAC, que permite a democratização do mesmo nível de segurança que as empresas da Fortune 500 usam para se protegerem, por uma fracção do preço.
Os nossos serviços incluem todo o espectro relacionado ao Purple Team, o que significa que os nossos planos não possuem setup, nem custos por retenção de dados ou mesmo por tráfego de dados.
Em comparação com outras empresas, a comparação mais próxima seria entre a NASA e a SpaceX nos seus conceitos. Enquanto a SpaceX reutiliza os seus foguetes, a NASA atirava-os no mar. De forma similar, actualmente, as empresas de SIEM e SOC criam configurações personalizadas para empresas, com base em SIEMs tercerizados e caríssimos, e ainda forçam os seus clientes a pagarem por todo o processo de instalação do sistema. No próximo cliente, toda a configuração, criação de regras de detecção de threats, regras de APTs, bem como a adaptação dos logs, acabam por ser trabalhos repetitivos e que têm de ser recomeçados do zero a cada nova instalação. Além disso, não possuem acesso ao sistema do SIEM, e ficam sem a possibilidade de fazer alterações ou evolui-lo da forma como bem entenderem, estão sempre presos ao que as empresas determinam que é prioridade.
Como exemplo, a IBM QRadar lançou recentemente a função relacionada ao MITRE ATT&CK, no entanto, já tínhamos essa função desde o lançamento da nossa plataforma ISMAC.
Por sermos donos do nosso próprio SIEM com AI, o seu preço já está incluído no plano, sem cobrança de taxa de instalação ou setup. Inclusive, para empresas com uma rede de carácter "flat", sem diferentes níveis, a instalação do ISMAC pode ser feita em apenas 24 horas.
Outra diferença é que como desenvolvemos o nosso próprio sistema, as opções de compliance com a RGPD, PCI-CSS, CCPA, LGPD, etc já estão inclusas e pré-configuradas, assim como mais de 250 regras de threat detection e diversas APTs, inclusive as APTs 28-34 do grupo hacker Fancy Bear. Além de estarmos a adicionar constantemente novas regras de detecção, das quais os clientes se beneficiam automaticamente.

POR ONDE PASSA A ESTRATÉGIA DA EMPRESA PARA OS PRÓXIMOS MESES?

Estamos actualmente a contratar pessoas em todas as áreas, mas principalmente atendimento e executivos em Portugal, das mais diversas nacionalidades, para ajudarem-nos a espalhar a novidade por todos os países da Europa, Ásia e Estados Unidos.
Estamos a iniciar parcerias com algumas empresas de grande porte para iniciar a oferta de aparelhos e estruturas inteiras já pré-configuradas com nosso ISMAC, com a intenção de massificar o uso da tecnologia e tornar a segurança na internet algo mais universalizado no mundo inteiro.
Esperamos que Portugal possa servir como a nossa base de comando para operacionalizar todas as nossas operações em outros países. Actualmente estamos a expandir para os Estados Unidos, Reino Unido e Irlanda, e esperamos expandir para muitos outros países em breve.

COMO AVALIA O ESTADO DA CIBERSEGURANÇA NO MUNDO, RELATIVAMENTE À PREPARAÇÃO DAS EMPRESAS PARA RESPONDEREM A ESSES DESAFIOS? QUE IMPACTOS ESTÁ A TER A ACTUAL PANDEMIA NO QUE TOCA À CIBERSEGURANÇA EM AMBIENTE CORPORATIVO?

Acredito que muitas empresas têm a falsa percepção de que estão protegidas ao utilizar um antivirus ou um firewall. Se isso fosse o suficiente, as empresas da Fortune 500 não gastariam milhões para empregar exactamente a mesma solução que estamos a disponibilizar para as massas.
No entanto, num cenário onde não existia uma solução com custo viável para as pequenas e médias empresas, não teria como haver o estímulo para se buscar uma solução.
Esperamos que agora que existe uma solução com custo viável para empresas menores que estas possam passar a proteger-se e parar de serem exploradas por hackers e governos estrangeiros com intenções maliciosas.
A actual pandemia resultou num aumento dramático no número de casos de hacking e até mesmo no número de pessoas a procura por termos como "como hackear", dentre outros relacionados a ameaças virtuais.
Nesse cenário, junto com o RGPD e uma possível guerra fria entre as principais potências do mundo, ter uma forma de protecção efectiva passa a ser fundamental. Ao menos, agora que existe uma opção, esperamos que mais pessoas fiquem alertas à protecção dos seus dados e também aos dados de terceiros que guardam.
As empresas que não tiverem o cuidado agora em contratar uma forma efectiva de protecção de dados acabarão por perder clientes, e sem entender porquê. Para deixar claro que a empresa está protegida e afastar o temor dos clientes, também oferecemos a possibilidade de a empresa colocar no seu website um botão que demonstra se o ISMAC e o Compliance com a RGPD está activo naquele momento.•

> "ESTAMOS A CONTRATAR PESSOAS EM TODAS AS ÁREAS PARA AJUDAREM-NOS A ESPALHAR A NOVIDADE POR TODOS OS PAÍSES DA EUROPA, ÁSIA E ESTADOS UNIDOS"

PERFIL DE UM CISO

CONSCIENCIA DE CIBERRISCO

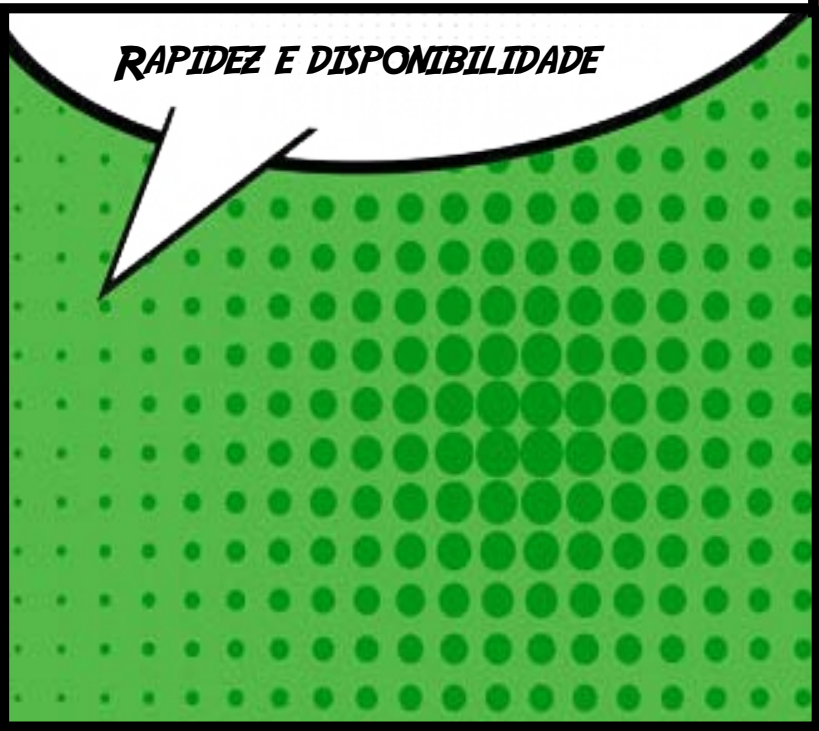
CAPACIDADES DE COMUNICAÇÃO E RELACIONAMENTO

AS EMPRESAS PROCURAM RESPOSTAS RÁPIDAS A QUALQUER INCIDENTE, REDUZINDO AO MÁXIMO OS IMPACTOS NANCEIROS E REPUTACIONAIS. É ESSENCIAL MANTER O FOCO, NÃO BAIXAR OS BRAÇOS, NÃO VACILAR, MANTENDO O CONHECIMENTO ACTUALIZADO. GERIR OS DESAFIOS DA CIBERSEGURANÇA É UMA TAREFA STRESSANTE. A PALAVRA DE ORDEM É RESILIÊNCIA PESSOAL

AS PRIORIDADES DA GESTÃO DE RISCO NECESSITAM SER SISTEMATICAMENTE ABORDADAS AO NÍVEL DO TOP MANAGEMENT, EQUIPAS DE NEGÓCIOS E TI, ASSIM COMO AO NÍVEL DAS OPERAÇÕES. É IMPORTANTE CONSEGUIR ADAPTAR A COMUNICAÇÃO A DIFERENTES INTERLOCUTORES. UMA EQUIPA MOTIVADA É MEIO CAMINHO PARA IMPLEMENTAR E DESENVOLVER UMA CULTURA DE SEGURANÇA. UM BOM RELACIONAMENTO COM COLABORADORES E O BOARD PERMITE GERAR CONFIANÇA E ASSEGURAR O BUDGET NECESSÁRIO

PENSAMENTO PRÓ-ACTIVO E FORA DA CAIXA

CRIAR CENÁRIOS, QUESTIONAR, TESTAR, PENSAR EM RESPOSTAS PREVIAMENTE PODERÁ AJUDAR A SUPERAR UMA SITUAÇÃO REAL MAIS RAPIDAMETNE, COM MENOR STRESS, REDUZINDO O IMPACTO SOBRE AS EQUIPAS E NEGÓCIOS. CAPACIDADE PARA ALINHAR A SEGURANÇA COM O NEGÓCIO, PERCEBENDO AS VULNERABILIDADES DO PONTO DE VISTA TÉCNICO E RISCOS ASSOCIADOS E A CAPACIDADE DE TRADUZIR ESSA REALDIADE PARA O NEGÓCIO



A INFFLUÊNCIA DO CHIEF INFORMATION SECURITY OFFICER CHEGA A TODA A ORGANIZAÇÃO. AS SUAS RESPONSABILIDADES PODEM INCLUIR RESPOSTA A EMERGÊNCIAS INFORMÁTICAS, RESPOSTA A INCIDENTES DE SEGURANÇA INFORMÁTICA, CIBERSEGURANÇA, RECUPERAÇÃO EM CASO DE CATÁSTROFE E GESTÃO DA CONTINUIDADE DO NEGÓCIO, GESTÃO DE IDENTIDADE E ACESSO, PRIVACIDADE DA INFORMAÇÃO, CONFORMIDADE REGULAMENTAR, GESTÃO DE RISCO, SEGURANÇA E GARANTIA DA INFORMAÇÃO, ENVOLVIMENTO NO CENTRO DE OPERAÇÕES DE SEGURANÇA DA INFORMAÇÃO, CONTROLO DAS TECNOLODIAS DE INFORMAÇÃO PARA SISTEMAS FINANCEIROS E OUTROS, INVESTIGAÇÕES INFORMÁTICAS E PERÍCIA DIGITAL

UTILIZAR FERRAMENTAS PARA GERAR MAPAS DE RISCO, PERMITINDO MANTER A CONSTANTE ATENÇÃO RELATIVAMENTE À CIBEREXPOSIÇÃO DA EMPRESA, CONHECER AS VULNERABILIDADES E REUNIR ESFORÇOS PARA PRIORIZAR O RISCO E DIMINUIR VULNERABILIDADES

[RE]INVENTE O SEU NEGÓCIO