Estudo demonstra níveis baixos de confiança na gestão das organizações sobre a segurança e privacidade

Inquérito realizado pela IDC, em conjunto com a Devoteam Cyber Trust demonstra aumento dos orçamentos para a segurança prevalecendo, no entanto, a falta de meios e ineficiência operacional

Note-se que este estudo é lançado pela IDC e pela Devoteam Cyber Trust, o novo nome adotado pela Integrity Part of Devoteam, que passa assim a ser o motor dos Managed Services da Devoteam Cyber Trust

Lisboa, 30 Maio 2023 – Um novo estudo levado a cabo pela Devoteam Cyber Trust, braço especializado em Cibersegurança do Grupo Devoteam, juntamente com a IDC, mostra que somente 31% das organizações consegue gerir todos os aspetos de conformidade referentes à segurança e privacidade e prevê que, até 2025, 70% dos CEOs de grandes organizações europeias serão incentivados a gerar pelo menos 40% das suas receitas provindas de iniciativas digitais.

Estas conclusões resultam de um inquérito feito junto de 700 profissionais de IT e segurança da Europa (incluindo Portugal) e Médio Oriente, cujos resultados ajudam a elucidar quanto à questão das políticas e estratégias de segurança e conformidade de terceiras partes.

À medida que os ataques cibernéticos aumentam, também aumentam os orçamentos e a importância estratégica dada à questão da segurança.

Na verdade, o crescente risco cibernético, juntamente com o foco no digital, leva a um reforço nos orçamentos de segurança: as empresas enfrentam cada vez mais ataques cibernéticos, e por isso devem reforçar ainda mais a sua "ambição" digital. **Este estudo mostra um certo aumento nos orçamentos de segurança**, juntamente com uma antevisão mais estratégica das questões de segurança, o que sugere que muitas empresas reconhecem os desafios que têm pela frente, mas carecem dos meios para os enfrentar. Basta olhar para os números e ver que a ***security-by-design*** **– conceito extremamente importante na prevenção de todo o tipo de riscos - é praticada apenas por pouco mais de metade das organizações (53%)**.

É um facto que a resiliência cibernética é uma prioridade, no entanto as organizações têm dificuldade na parte da sua execução: **55% dos entrevistados disse que a resiliência cibernética é a "principal prioridade com uma estratégia definida" em vigor**, sugerindo que mais de metade das organizações europeias e no Médio Oriente têm uma abordagem madura em relação à resiliência cibernética. No entanto, os resultados do estudo também mostram que, apesar de definir prioridades, **as organizações estão ainda**

a lutar para corrigir os riscos de segurança conhecidos e que melhorar ou fortalecer a postura de segurança ao longo do tempo é um desafio.

O que significa que, apesar dos crescentes orçamentos de segurança e maior influência estratégica, a **maioria das organizações ainda sofre com baixa eficiência e capacidade operacional**. E aqui falamos tanto de empresas que trabalham com equipas de segurança internamente, como as que trabalham com MSSP.

Nesta mesma linha, o estudo avançou ainda que empresas menos maduras usam MSSP (Provedores de Serviços Geridos de Cibersegurança) mais extensivamente, para ter melhor capacidade de segurança (exceto para serviços financeiros).

Existe uma forte correlação inversa entre a extensão do uso de MSSPs por um setor e a sua visão estratégica de segurança. Basicamente, **as indústrias mais maduras adotam menos o MSSP**. E isto faz sentido, pois os setores que exibem capacidade em funções de segurança têm menos necessidade de terceirizar, optando por ser seletivos no uso de MSSP. Por sua vez, indústrias menos maduras precisam de aceder a recursos de segurança mais sofisticados que não podem obter por conta própria e, portanto, precisam de terceirizar. Estes também podem considerar terceirizar a segurança, pois não a veem como uma competência estratégica e essencial que precisam manter internamente.

O outsider óbvio são os serviços financeiros. Esta é uma indústria particularmente madura no que diz respeito à segurança. O que pode parecer estranho, já que os bancos geralmente têm recursos financeiros para financiar este tipo de serviços, porém **segundo o estudo é um setor que valoriza a entrada de MSSPs** de terceiros e são mais propensos a usar as funções e tecnologias mais sofisticadas disponíveis, e os MSSPs são uma forma eficiente para adquiri-los.

Independentemente da sua dimensão, todas as empresas passam pelo mesmo processo ao considerar a possibilidade de acelerar a terceirização da segurança. O principal impulsionador é uma maior vulnerabilidade a novas ameaças, o que não é surpresa. Curiosamente, o aumento da complexidade também é um acelerador, implicando que as empresas vêem o MSSP como um caminho para a simplificação ou, mais provavelmente, uma forma de lidar com a complexidade que na verdade não conseguem gerir sozinhas.

Quanto à seleção de um parceiro de segurança, o estudo mostra que apesar de haver outros, os compradores consideram os seguintes fatores os mais importantes:

- 36% Acesso a ferramentas avançadas, como resposta a incidentes, inteligência de ameaças e XDR (Extended detection and response);
- 35% Maior monitorização de ameaças com visibilidade em tempo real e resposta mais rápida;
- 32% Equipa alargada de especialistas e consultores de segurança certificados;
- 28% Ajuda para evitar configurações incorretas.

Ou seja, é dada prioridade às capacidades técnicas, rapidez e eficiência no tempo de resposta e know-how especializado.

Por fim, mas não menos relevante, o estudo é claro no que toca ao sucesso do funcionamento com o MSSP: é necessário que as organizações tenham uma visão holística do relacionamento para desenvolver uma verdadeira parceria, com base num alinhamento perfeito entre a visão, cultura e respetivas métricas.

"Tendo como foco a atual importância do papel da Segurança para as organizações na sua jornada digital, este estudo tenta compreender a visão, motivações, prioridades e desafios dos profissionais de IT e de Segurança perante a decisão da escolha de um MSSP (Managed Security Service Provider). conclui Rui Shantilal, Managing Partner da Integrity Part of Devoteam que, a partir de hoje, adota o nome de **Devoteam Cyber Trust**, mantendo-se a mesma equipa de gestão, estrutura e apoio direto aos clientes.

No fundo, esta etapa conclui o processo da aquisição feita pela Devoteam em 2021, quando a Integrity passou a ser Integrity Part of Devoteam, com o principal intuito de fortalecer o braço de Cibersegurança da Devoteam, com a forte componente de serviços geridos pela Integrity, passando na verdade a Integrity a ser o motor dos Managed Services da Devoteam Cyber Trust.

Para mais informações, aceda ao estudo: https://bit.ly/45pFcbd

Sobre a Integrity part of Devoteam agora Devoteam Cyber Trust

A INTEGRITY é uma empresa fundada em 2009, que agora se passa a denominar Devoteam Cyber Trust e com enfoque nas práticas de Consultoria e Auditoria Tecnológica de Cibersegurança, certificada na ISO 27001, ISO 9001, certificada pelo PCI e membro CREST e do CIS – Center for Internet Security. Conta com uma experiência de 14 anos, e opera em 20 países na EMEA oferecendo serviços de valor acrescentado em Cibersegurança, que combinam a sua experiência e tecnologia proprietária para reduzir, de forma consistente e eficaz, o risco cibernético dos seus clientes. As gamas de serviços abrangentes incluem Testes de Intrusão Persistentes, Consultoria e Soluções de ISO 27001, PCI-DSS, GRC e gestão de risco de terceiros.

Sobre a Devoteam Cyber Trust

A Devoteam Cyber Trust é a unidade especializada em cibersegurança do Grupo Devoteam. Com mais de 800 especialistas localizados em toda a Europa, Médio Oriente e África, o nosso objetivo é estabelecer a cibersegurança como um facilitador do sucesso dos negócios, em vez de um obstáculo. Utilizamos uma abordagem abrangente de Resiliência Cibernética, Segurança Aplicada e Gestão de Serviços de Segurança para proteger a jornada tecnológica de empresas de grande e média dimensão de todos os setores e indústrias.

A Devoteam é uma empresa líder em consultoria focada em estratégia digital, plataformas tecnológicas e cibersegurança. Ao combinar criatividade, tecnologia e

insights de dados, capacitamos nossos clientes a transformar os seus negócios e desbloquear o futuro. Com 25 anos de experiência e 10.000 funcionários em toda a Europa, Oriente Médio e África, a Devoteam promove tecnologia responsável para as pessoas e trabalha para criar mudanças positivas.

Press Contacts

Sofia Alcobia
Executive Manager

BE IDEAS – Boutique PR Agency
M: +351 962 615 717
E: sofia.alcobia@beideas.pt
W: beideas.pt