manchete

Jornal Económico
Suplemento Especial
18-05-2018

Periodicidade: Semanário | Temática: Justica
Classe: Economia/Negócios | Dimensão: 468 cm²
Âmbito: Nacional | Imagem: S/Cor
Tiragem: 20000 | Página (s): 3

OPINIÃO

A Cybersegurança no apoio ao combate da Fraude e Corrupção

SÉRGIO SÁ
Associate Partner, EY

De acordo com o 15th EY Fraud Survey recentemente publicado, os Cyberataques (37%) e a Fraude e Corrupção (36%) foram identificados pelos responsáveis das organizações entre os 4 principais riscos (1) para as mesmas. A importância destes dois riscos tem vindo a aumentar por estarem a tornar-se cada vez mais direcionados, complexos e a serem utilizados de forma persistente.

Isto é uma das consequências da conectividade global, em que qualquer pessoa com acesso aos dados da organização, pode explorar os seus pontos fracos. Os ativos críticos (físicos e digitais) das organizações têm assim, mais do que nunca, uma maior exposição ao risco: roubo, danos e sua manipulação.

Prioritização da Cybersegurança e Combate à Fraude/Corrupção

Em resultado disso, e devido ao seu impacto, os riscos de Cybersegurança e Fraude já fazem parte da agenda dos responsáveis das organizações e começam a fazer parte dos relatórios anuais.

Alinhamento das estratégias de Gestão de Fraude/Corrupção e Cybersegurança

Por outro lado, uma parte significativa das organizações ainda aborda estes dois riscos de forma separada e desalinhada, no entanto o canal digital é hoje o principal meio para a ocorrência destes riscos, pelo que urge repensar uma estratégia integrada de abordagem aos mesmos com vista obter-se uma visibilidade clara e global dos riscos da organização para uma tomada de decisão rápida.

Medidas a ter em conta

- **Transformação:** Alinhamento da estratégia das áreas de: risco, jurídico, conformidade, cibersegurança e fraude a nível de modelo de governo, processos e formação. Sendo o elemento humano a peça chave, as organizações deverão definir de forma clara as expetativas aos colaboradores e terceiros sobre as suas responsabilidades para assegurarem a integridade da organização
- **Gestão de Ameaças:** De forma a melhorar a capacidade de monitorização e reporting deverão ser adotadas novas tecnologias (artificial intelligence, machine learning e automation) de forma integrada e colaborativa entre as várias áreas envolvidas de forma a ser possível obter-se uma análise preditiva, alertas em tempo real e capacidade de análise forense
- **Gestão de Identidades:** Sendo os ativos de informação um elemento critico das organizações, os mesmos deverão ser dotados de controlos que permitam definir os seus acessos em termos de: O quê, Quem, Como e Quando
- **Proteção de Dados e Privacidade:** Em particular na europa, com entrada em efeito do RGPD (Regulamento Geral de Proteção de Dados) a partir de 25 de Maio, irá implicar alterações nas organizações a nível de serviço, processos, tecnologia e jurídico
- **Resiliência:** O sucesso das organizações depende da capacidade de resposta quer em operação normal quer em caso de incidente possa colocar o serviço em causa. Pelo que deverá ser elaborado um plano em caso de disrupção de forma a minimizar o impacto.

Nota (1): Os outros dois riscos: Alteração da Regulação (43%) e o Ambiente Macroeconómico (42%).