Regulação e confiança são os motores da cibersegurança

Nos setores mais regulados, como o financeiro, sempre houve investimento, no entanto os reguladores tornaram-se mais exigentes. Nos setores menos regulados, a confiança dos consumidores é a motivação para o investimento.

FILIPE S. FERNANDES

"A cooperação é um passo fundamental para a segurança no ciberespaço. As organizações têm de criar o hábito de 'aprender a partilhar' as boas práticas, a forma como lidaram com determinado evento", refere Miguel Dias Fernandes, consulting partner da PwC.

Licenciado em Economia pelo ISEG, a sua carreira foi feita nas consultoras Everis e EY, com foco sobretudo nas questões digitais, e adianta que "há setores que já o fazem, talvez ainda não com a profundidade desejável, mas é um princípio e claramente uma aposta de futuro, com benefício para todos os elos da cadeia de colaboração".

Na sua perspetiva como é que as empresas e as organizações em Portugal olham para a cibersegurança?

Nos últimos anos temos assistido ao aumento do investimento das organizações em cibersegurança e na segurança da informação em geral. Há duas grandes razões pelas quais as empresas fazem este investimento: regulação e manutenção da confiança dos consumidores nas organizações. Nos setores mais regulados, como o financeiro, sempre houve investimento, no entanto, os reguladores tornaram-se mais exigentes, o que obriga as instituições a responderem a essa exigência com medidas mais concretas, a prepararem-se melhor e não só a escreverem ou enunciarem políticas, mas também a implementarem as políticas. Nos setores menos regulados, a confiança dos consumidores é a motivação para o investimento.

Neste caso, o Regulamento Geral de Proteção de Dados (RGPD) veio ajudar, pois a discussão pública foi tão alargada que acabou por trazer para a ribalta os direitos dos titulares dos dados e isso implicou uma maior consciencialização das empresas, porque em caso de uma violação de dados, a reputação da organização pode ser largamente afetada e, como é sabido, pode haver segurança da informação sem preocupações de privacidade, mas não há privacidade sem segurança da informação.

Quais foram os casos mais graves de ataques cibernéticos realizados em Portugal? Quais são os tipos de ataques e crimes cibernéticos mais comuns?

Não sei se alguém sabe quais foram os ataques mais graves em Portugal, pois as empresas não estão obrigadas à sua divulgação. No entanto, nos últimos anos temos assistido a alguns casos que chegaram ao conhecimento público, sendo talvez os mais emblemáticos o wannacry, em 2017, que levou algumas instituições financeiras a 'desligarem-se' da internet e alguns operadores de telecomunicações a isolarem alguns troços da rede interna.

Em 2018, de forma pública, conhecemos outro ataque de ransomware que cifrou os sistemas de um grupo no setor da Saúde e, já em 2019, tivemos uma empresa industrial a ser alvo de ransomware. No panorama internacional os databreaches são talvez, a par com o ransomware, o tipo de ataque mais popular.

Diz-se que qualquer organização vai acabar por ser atacada, não se sabe quando nem com que intensidade. Quais são os princípios a que deve obedecer uma estratégia de cibersegurança numa organização?

Um bom princípio, e como ponto de partida, consiste em definir o modelo de governo. A definição de responsabilidades em cada uma das linhas de defesa e os mecanismos de articulação, comunicação e monitorização entre as várias áreas envolvidas ditam o sucesso da estratégia e da intervenção. Muitas vezes as organizações tendem a saltar este ponto. Outro ponto fundamental é identificar os assets mais críticos e que, de acordo com o risco existente, merecem particular foco. No essencial é crucial criar e manter uma cultura de segurança onde as pessoas são o elo diferencial. Elas têm de ter noção das decisões críticas que tomam em matéria de segurança. Em termos de estratégia, é fundamental prioritizar investimentos, alocar recursos e alinhar capacidades de segurança com os imperativos estratégicos e as iniciativas da organização.

Em que é que novas tecnologias como o blockchain podem contribuir para fazer face a estes ataques cibernéticos?

Tecnologias como o block-

Miguel Dias Fernandes diz que é fundamental prioritizar investimentos.

"É crucial criar e manter uma cultura de segurança onde as pessoas são o elo diferencial."

"Tecnologias com o blockchain podem efetivamente ajudar na proteção de informação."

Uma iniciativa do Negócios em parceria com a PwC

DR

Funcionários são a principal fonte de falhas

Apenas 44% dos entrevistados dizem que seus conselhos de administração participam ativamente da estratégia geral de segurança das suas empresas.

A principal origem de incidentes em cibersegurança está nos funcionários das empresas, como revela o Global State of Information Security Survey 2108 da PwC, que entrevistou 9.500 executivos de 122 países. Os incidentes atribuídos a hackers (23%), concorrentes (22%) e outros fatores externos diminuíram. No entanto, os atribuídos a insiders (26%), como terceiros – incluindo fornecedores e consultores – e funcionários (30%), permaneceram iguais ou aumentaram.

Os líderes empresariais entrevistados para o Global State of Information Security Survey 2108 sublinham os novos riscos ligados às tecnologias emergentes com a sua multiplicidade de conexões. Assim, 40% dos entrevistados de organizações que usam robótica ou automação dizem que a interrupção das operações, o comprometimento de dados sensíveis e os danos à qualidade do produto, seriam a consequência mais crítica de um ataque cibernético a esses sistemas. Além disso, apenas 34% dizem que as suas organizações planeiam avaliar os riscos de segurança da Internet das coisas (IoT) em todo o ecossistema de negócios.

As ameaças de perdas, roubos e quebras de integridade de dados são uma preocupação crescente. Os ataques cibernéticos que manipulam ou destroem dados podem prejudicar os sistemas confiáveis sem o conhecimento do proprietário e têm o potencial de danificar a infraestrutura crítica.

Uma das conclusões do estudo mostra que há pouca participação das administrações e do governo das empresas na determinação das estratégias de segurança ou dos planos de investimento das suas empresas. Apenas 44% dos entrevistados dizem que seus conselhos de administração participam ativamente da estratégia geral de segurança de suas empresas.

Por outro lado, os receios de falhas de segurança mobilizam os gestores. Assim, 87% dos CEO globais dizem que estão a investir em segurança para gerar a confiança dos clientes e 81% dizem estar a investir na prática da transparência no uso e armazenamento de dados. Cerca de dois terços dos entrevistados em todo o mundo dizem que sua organização tem um chief privacy officer (CPO) ou um executivo com competências para as questões da privacidade. ■

chain podem efetivamente ajudar na proteção da informação, logo à partida pela natureza descentralizada, tornando assim os ataques dirigidos a um só ponto (vulnerável) teoricamente ineficazes.

Os negócios e a vida estão cada vez mais tecnológicos, a conectividade é quase universal. Isto não aumenta a vulnerabilidade a ataques, roubos e fraudes digitais? Como é que se minimizam estes fatores de risco?

Sem dúvida que há uma exposição crescente, o que significa que os níveis de vulnerabilidade são proporcionalmente crescentes. Para tal, apenas através de um modo de alteração comportamental alargada e profunda, mas também natural e intrínseca, será possível evitar "males maiores". Mesmo nas coisas mais simples – as aplicações que "corremos" nos nossos telefones ("não há almoços grátis"), aquilo que publicamos nas redes sociais sobre a nossa vida, a reutilização de passwords em diversos sites, são elementos decisivos e constantes. ■

O check-list da digitalização

PRIORIDADES
NÃO É POSSÍVEL PROTEGER TUDO
É fundamental conhecer os ativos e definir prioridades para proteger o que é mais relevante na organização.

RISCO
GESTÃO DO RISCO
A gestão de topo deve garantir que todos os riscos e questões regulatórias estão identificados e têm uma adequada resposta em termos de cibersegurança.

CRISES
A QUESTÃO NÃO É SE... MAS QUANDO
Em caso de ataques as organizações devem estar dotadas de planos que permitam agir rapidamente.

TECNOLOGIA
FIX THE BASICS
É possível tirar o máximo proveito da evolução tecnológica e obter retorno dos investimentos em segurança através de uma adequada escolha de tecnologia e a sua correta parametrização.

CONEXÕES
SISTEMAS CONECTADOS
Num mundo digital e com informação partilhada entre entidades, é fundamental garantir que estas conexões estão seguras e com controlos para impedir acessos indevidos ou a adulteração dos dados.

PESSOAS
A definição e disseminação de campanhas de awareness de segurança de informação e comunicação das políticas permite que toda a organização conheça os princípios de segurança da informação.

Fonte: Cibersecurity – Framework PwC