CIBERSEGURANÇA

APOIOS:

CELFOCUS GALILEU KPMG UNICRE®

ENQUADRAMENTO

OS DESAFIOS DA CIBERSEGURANÇA

A CIBERSEGURANÇA TORNOU-SE NUM ENORME "QUEBRA-CABEÇAS" PARA AS EMPRESAS EM TODO O MUNDO

A adopção de novas tecnologias para melhorar a qualidade e a produtividade acarreta consigo diversos riscos que são desafiantes para ultrapassar.

À medida que a digitalização avança, os dados tornam-se o activo mais valioso de uma organização e a sua protecção é essencial para garantir a continuidade dos negócios e a confiança dos clientes e do mercado. Ransomware, Malware, Phishing, Firewall... São termos que estão cada vez mais associados ao quotidiano de todas as organizações, que vêm agora a necessidade de proteger um bem que não julgavam, há anos, tão valioso.

Desta forma, e para fazer frente aos desafios impostos por uma nova geração tecnológica, as empresas devem investir em medidas de cibersegurança, como a implementação de firewalls robustos, sistemas de detecção de intrusões, encriptação de dados sensíveis e práticas de cibersegurança em toda a cadeia de valor.

Para além disso, a conscientização e a formação dos colaboradores para as questões de cibersegurança são de uma importância crucial. Muitos ataques começam com erro humano, como clicar em links suspeitos ou usar senhas fracas. Portanto, educar os funcionários sobre os procedimentos de segurança adequados é uma importante linha de defesa.

CONSEQUÊNCIAS

As consequências de um ataque cibernético podem ser devastadoras para uma empresa. Desde a perda de dados confidenciais até a interrupção significativa das operações comerciais, as empresas podem ser severamente castigadas, quer nas suas relações comerciais como na sua reputação.

Acrescido a estes danos, surgem posteriormente os custos associados à recuperação dos dados e as medidas correctivas associadas a este ataque. Ou seja, os ciberataques não comprometem só a segurança digital, mas têm também implicações nos aspectos financeiros, reputacionais e legais das empresas.

Desta forma, urge a necessidade de as empresas se prepararem para estes cenários, estabelecendo parcerias com empresas especializadas em cibersegurança e através da implementação de políticas de resposta a incidentes.

A rápida detecção e resposta a um ciberataque pode minimizar os danos e acelerar a recuperação. De acordo com um estudo recente, os portugueses são os terceiros melhores do mundo em termos de conhecimento de privacidade online e cibersegurança. Obtiveram a sua melhor pontuação no reconhecimento de diversos perigos online e como os evitar (74%) e a pior em questões relacionadas com comportamentos e ferramentas de segurança online (51%).

O estudo da NordVPN mostra ainda que os portugueses são bons a criar palavras-passe fortes (98%) e que conhecem os riscos de guardar informações relativas a cartões de crédito no navegador (93%). No entanto, só 3% dos portugueses conhecem ferramentas online que protegem a privacidade digital, e apenas um em cada 10 sabe quais são as informações que os provedores de Internet (ISPs) colectam como parte de metadados.

Assim, é imperativo que as empresas e os cidadãos portugueses estejam plenamente preparados para enfrentar os desafios dos ciberataques e as questões de cibersegurança. As organizações devem adoptar medidas proactivas, investindo em tecnologias robustas, promovendo a conscientização e oferecendo treinamento contínuo para seus colaboradores.

Compra inesperada? ParcelaJá.

Parcela Já®
Compre Já. Pague depois.
COM UNICRE®

Pague até 6x s/juros

Parcela Já®
Compre Já. Pague depois.
COM UNICRE®

reduniq.pt

Para mais informações contacte a UNICRE – Instituição Financeira de Crédito, S.A., registada junto do Banco de Portugal com o n.º 698 e sujeita à respetiva supervisão, verificável em https://www.bportugal.pt/

CELFOCUS

OS DESAFIOS NA SEGURANÇA DE DESENVOLVIMENTO DE SOLUÇÕES

A PROTEÇÃO CONTRA AMEAÇAS CIBERNÉTICAS É UMA PRIORIDADE QUE NÃO PODE SER NEGLIGENCIADA NUM AMBIENTE DIGITAL EM CONSTANTE EVOLUÇÃO

DESAFIOS
OS TRÊS PRINCIPAIS DESAFIOS NA SEGURANÇA DE DESENVOLVIMENTO DE SOFTWARE - IGNORAR RISCOS, NÃO A TRATAR COMO UMA PRIORIDADE E NÃO DAR A DEVIDA IMPORTÂNCIA À SEGURANÇA DE APLICAÇÕES – DESTACAM A NECESSIDADE DE MEDIDAS PROACTIVAS

Num mundo cada vez mais digitalizado, onde produtos, serviços e processos do dia a dia dependem fortemente de software, a importância do desenvolvimento de software seguro não pode ser subestimada. As repercussões de uma falha de segurança podem ser devastadoras, o que mancha a reputação de uma empresa e leva a perdas substanciais. Há, portanto, vários desafios que se colocam na segurança do desenvolvimento de software, tornando ainda mais crucial adotar uma abordagem proativa e holística para garantir a segurança destes sistemas. A proteção contra ameaças relacionadas com cibersegurança é uma prioridade que não pode ser negligenciada num ambiente digital em constante evolução. Nesse contexto, a segurança de software surge como uma salvaguarda essencial, que assegura não apenas o funcionamento contínuo de sistemas críticos, mas também a confiança dos utilizadores e a integridade das atividades comerciais.

IGNORAR RISCOS DE SEGURANÇA

Um dos desafios mais prevalentes no desenvolvimento de software é a tendência de ignorar os riscos de segurança. Não abordar esses riscos pode deixar uma organização vulnerável a ataques maliciosos, o que pode recitar em roubo ou manipulação de dados sensíveis. Os riscos de segurança frequentemente resultam de vulnerabilidades, que são fraquezas ou lacunas num programa de segurança que podem ser exploradas por ameaças. Como praticamente todos os negócios dependem de informações, qualquer comprometimento dos sistemas de informação pode resultar em consequências graves, incluindo danos à reputação e perdas financeiras.

Além disso, as ameaças de segurança não se limitam a atacantes externos. Surpreendentemente, uma percentagem significativa de ataques tem origem interna, sendo as empresas de serviços públicos particularmente suscetíveis. Educar equipas sobre protocolos de segurança e o seu papel na manutenção da segurança é crucial para proteger produtos e serviços. Um recente estudo reportado pela InfoWorld. Com, mostrou que muitos programadores entendem a importância da segurança, mas têm dificuldade em alocar tempo suficiente devido a prioridades concorrentes.

» Pedro Tarrinho, Head of Application Security, Celfocus

EDUCAR EQUIPAS SOBRE PROTOCOLOS DE SEGURANÇA E O SEU PAPEL NA MANUTENÇÃO DA SEGURANÇA É CRUCIAL PARA PROTEGER PRODUTOS E SERVIÇOS

SEGURANÇA COMO ÚLTIMA AÇÃO

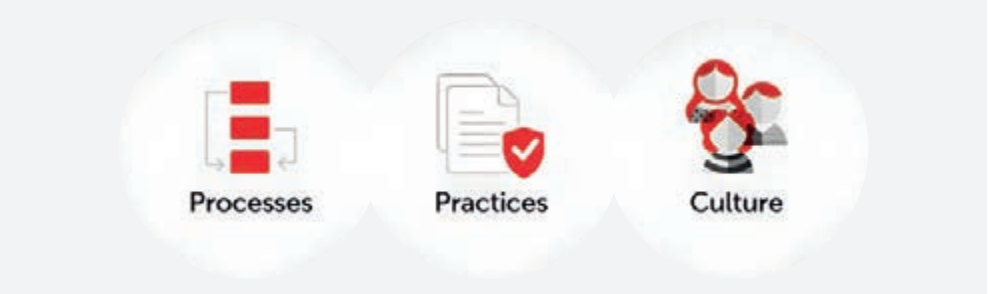
A segurança não deve ser uma ação final no processo de desenvolvimento de software. Não é algo que pode ser adicionado posteriormente ou comprado como um produto. Em vez disso, a segurança é um processo contínuo e evolutivo que deve ser integrado desde o início e continuamente aprimorado – "Shift Left Security". Esperar até as fases posteriores do desenvolvimento para abordar questões de segurança pode aumentar significativamente o custo e o esforço necessários para corrigi-las.

A implementação de uma estratégia de teste robusta, incluindo testes de segurança, no início do ciclo de desenvolvimento pode economizar recursos, tempo e dinheiro, permite assim identificar e corrigir questões de segurança num momento mais próximo da "criação" do problema. A segurança deve ser considerada "por design", o que significa que as soluções precisam ser construídas tendo a segurança como um elemento obrigatório.

SEGURANÇA DE APLICAÇÕES

A Segurança de Aplicações (AppSec) é um aspeto crítico da segurança de software em geral. Esta componente abrange processos para aprimorar a segurança e a resiliência de soluções de software. O seu foco passa por promover a segurança no desenvolvimento do código, das bibliotecas, dos sistemas de back-end, dos servidores web e das aplicações.

A atenção recente dada à AppSec levou ao desenvolvimento de projetos e guias de boas práticas.



O Open Web Application Security Project (OWASP) é uma organização notável dedicada à segurança de aplicações da web. O OWASP Top 10 é uma lista bem reconhecida das dez principais ameaças de segurança, atualizada recorrentemente. Além disso, o OWASP Application Security Verification Standard (ASVS) estabelece uma boa prática para testes de segurança de aplicações web, que especifica o grau de abrangência e o nível de teste com base na sensibilidade das informações e na exposição.

NUM MUNDO EM QUE O SOFTWARE É A BASE DE QUASE TUDO, GARANTIR A SUA SEGURANÇA É FUNDAMENTAL

A ABORDAGEM CERTA PARA A SEGURANÇA DE APLICAÇÕES

As empresas devem promover uma abordagem holística para a Segurança de Aplicações e essa abordagem deve ser construída sobre três pilares principais: Processos, Práticas e Cultura.

PROCESSOS

O foco está nos artefactos, soluções e políticas de suporte relacionadas com a implantação segura de software. Isso inclui controlos automáticos de segurança, soluções centralizadas de gestão de vulnerabilidades e políticas que estruturam a abordagem de entrega.

PRÁTICAS

Preocupação em fornecer às equipas as melhores práticas documentadas para o desenvolvimento de software seguro por meio de diretrizes, formação e sessões de demonstrações mensais.

CULTURA

Promover a consciencialização sobre segurança de soluções em equipas de projeto, com o incentivo a uma cultura de partilha de conhecimento e aprendizagem contínua.

A abordagem deve ser abrangente e garantir que a segurança é integrada em todos os aspetos do ciclo de desenvolvimento de software, desde o design e codificação até os testes e implementação. Essa filosofia de "Shift Left Security" enfatiza a importância de abordar questões de segurança no início do processo de desenvolvimento.

A SEGURANÇA É UM PROCESSO CONTÍNUO

Num mundo em que o software é a base de quase tudo, garantir a sua segurança é fundamental. Os três principais desafios na segurança de desenvolvimento de software - ignorar riscos, não a tratar como uma prioridade e não dar a devida importância à Segurança de Aplicações – destacam a necessidade de medidas proactivas.

Ao abordar a segurança em todas as etapas do processo de desenvolvimento, integrar a segurança desde o início e promover uma cultura de consciencialização sobre segurança, as empresas podem melhor proteger os seus clientes, ativos e reputação num cenário digital cada vez mais interconectado. Devemos nunca esquecer de que a segurança não é um produto, mas um processo, e deve ser uma preocupação de todos desde o início.

Executive
DIGEST

225 EDIÇÕES

17 ANOS a acompanhar as tendências do mundo da gestão

GALILEU

GALILEU

A SEGURANÇA INFORMÁTICA COMEÇA CONNOSCO

A CONSTANTE EVOLUÇÃO DAS AMEAÇAS CIBERNÉTICAS E A CRESCENTE INTERLIGAÇÃO DE SISTEMAS E DOS DADOS TORNAM AS EMPRESAS CADA VEZ MAIS VULNERÁVEIS A ATAQUES INFORMÁTICOS

É fundamental compreender que a segurança informática não trata apenas de tecnologia, de utilizar o melhor equipamento e software para fazer frente às ameaças. Ela começa connosco, com os colaboradores.

RISCOS E CONSEQUÊNCIAS PARA AS ORGANIZAÇÕES

Os ataques informáticos representam uma ameaça multifacetada que pode causar danos significativos às organizações em várias frentes: O roubo de dados e informação sensível pode ter consequências devastadoras. Por outro lado, o acesso a dados financeiros, propriedade intelectual ou informações estratégicas da organização pode prejudicar seriamente a sua competitividade e posição no mercado.

Acresce ainda o risco para a infraestrutura da organização: os ataques podem afetar o bom funcionamento da infraestrutura e têm o potencial para provocar enorme disrupção na atividade da organização e inclusivamente constituir um risco físico para colaboradores e clientes. Por tudo isto, a confiança dos clientes e parceiros é fortemente abalada por estes ataques, podendo resultar em perdas reputacionais e financeiras a longo prazo.

COLABORADORES COMO PRIMEIRA BARREIRA DE PROTEÇÃO

No que toca a ataques cibernéticos, o erro humano continua a ser a principal porta de entrada e com a expansão do trabalho remoto, os profissionais e os seus equipamentos de trabalho passaram a estar ainda mais expostos a riscos. Desta forma, é urgente a formação transversal dos colaboradores nesta área.

A formação em cibersegurança é crucial para mitigar riscos relacionados com estas ameaças e irá levar a uma maior consciencialização dos colaboradores para a cibersegurança, preparando-os para identificar as ameaças com que se irão deparar mais frequentemente, permitindo-lhes identificar os principais sinais de alerta para estas ameaças e sensibilizando-os para os riscos associados ao uso inadequado da tecnologia. Devidamente preparados, os colaboradores constituirão a primeira barreira de proteção da organização contra ciberataques.

UMA EQUIPA ESPECIALIZADA

Se por um lado uma abordagem transversal de formação permite aos colaboradores identificar ameaças, adotar boas práticas de segurança e responder a incidentes de forma adequada, conferindo um maior grau de proteção à organização, por outro, é necessário criar equipas especializadas em cibersegurança dentro da equipa de TI, acautelando também a segurança dos sistemas e infraestrutura da organização.

» Pedro Tavares, Head of Marketing, GALILEU

Dentro do campo da cibersegurança, existem diversas especializações, permitindo que os profissionais desenvolvam competências específicas para enfrentar desafios específicos. Estes profissionais são responsáveis por tornar a infraestrutura da organização mais robusta e, em caso de ataques, mitigar danos e manter ou retomar o mais rápido possível a atividade da empresa.

Em suma, a segurança cibernética surge como um fator crítico para o sucesso das empresas que não pode nem deve ser negligenciado. A formação é uma ferramenta importante para desenvolver uma "barreira humana" robusta, preparada para enfrentar os desafios do mundo digital e garantir a resiliência cibernética das organizações.

GALILEU

Focus on Success

FORMAÇÃO CYBER SECURITY

EARLY BIRD

10% DESCONTO

aplicado aos valores apresentados

cursos oficiais **EC-Council***

Classroom / Live Training

CCT
Certified Cybersecurity Technician
18 setembro
20 novembro
1.620€

CEH
Ethical Hacking and Countermeasures
9 outubro
2.130€

CND
Certified Network Defender
23 outubro
1.835€

CHFI
Computer Hacking Forensic Investigator
6 novembro
2.050€

CPENT
Certified Penetration Testing Professional
13 novembro
2.350€

E-Learning

Toda a oferta formativa E-Learning da EC-Council tem **desconto de 5%** durante o mês de outubro.

* Incluem Exame de Certificação, iLabs e documentação digital

EC-Council

O EC-Council Group é uma organização dedicada à segurança da informação que procura gerar conhecimento, facilitar a inovação, executar pesquisas, implementar o desenvolvimento e nutrir especialistas no assunto, para disponibilizar as competências e expertise em segurança informática.

oferta **GALILEU**

Segurança Informática para Utilizadores

Curso **E-Learning** de consciencialização de profissionais das diversas áreas para a cyber segurança.

~~120€~~ **96€**
para inscrições em outubro

Mais informações em:
www.galileu.pt/CyberOctober

info@galileu.pt
21 361 22 00

A GALILEU é reconhecida pela DGERT

uma marca Rumos training | Knowledge sharing

KPMG

UM MUNDO DIGITAL FIÁVEL

A KPMG TEM UMA POSIÇÃO PRIVILEGIADA PARA APOIAR AS EMPRESAS NESTE DESAFIO

A KPMG apoia os clientes na criação de um mundo digital robusto e fiável, oferecendo uma combinação de experiência tecnológica, conhecimento profundo do negócio e profissionais de excelência com uma paixão pela protecção e resiliência do negócio. Em entrevista à Executive Digest, Sérgio Martins, Partner da KPMG Portugal e responsável da área de cibersegurança, explica como as organizações se devem proteger ao nível da cibersegurança.

A Cibersegurança é um dos grandes desafios da nossa sociedade, nomeadamente, para as empresas. Que soluções é que a KPMG coloca à disposição dos clientes?

A cibersegurança está cada vez mais no topo das prioridades dos nossos clientes e na última edição do nosso estudo CEO Outlook, a cibersegurança destaca-se como um dos principais riscos para os próximos anos, ao lado de temáticas como incerteza geopolítica, alterações climáticas e aumento das taxas de juro.

Na KPMG apoiamos os nossos clientes na criação de um mundo digital robusto e fiável, oferecendo uma combinação de experiência tecnológica, conhecimento profundo do negócio e profissionais de excelência com uma paixão pela protecção e resiliência do negócio dos nossos clientes. As soluções vão desde a estratégia de governo, gestão de risco e conformidade da cibersegurança até à implementação e operação tecnológica, que inclui arquitecturas de segurança de centros de dados e Cloud, soluções de gestão de acessos e identidades, desenho de SOCs, testes de intrusão e resposta a incidentes. Pretendemos que o conjunto de serviços e soluções que disponibilizamos possa ser o mais transversal possível, de forma a ajudar a garantir uma segurança efectiva das operações dos nossos clientes.

Quais os tipos de ciberataques mais comuns que temos hoje em dia no sector empresarial português?

Tendo em conta que a internet é um meio global e os actores do cibercrime não têm fronteiras, os ataques a que temos assistido a nível nacional não diferem muito daquilo que são as tendências globais.

Assistimos a muitos ataques direccionados – Spearphising, tipicamente a pessoas de topo das empresas, onde os atacantes se fazem passar por entidades credíveis de modo a obter informação confidencial, como por exemplo as suas credenciais. Estas credenciais obtidas podem depois ser utilizadas para roubo de informação ou como porta de entrada para acederem a outros sistemas e continuarem assim a cadeia de ataque.

Os ataques de ransomware também são muito comuns, porque são um tipo de ataque que pode dar retorno financeiro imediato para os grupos de cibercrime organizado, e caso a empresa não tenha o nível de protecção e recuperação adequado, pode ficar completamente refém e ter de pagar quantias por vezes muito avultadas de forma a poder recuperar os seus dados.

Também existem alguns ataques perpetrados por Hacktivistas, que são grupos que defendem uma causa específica e que procuram

COMPETÊNCIAS

A KPMG DISPÕE DE UM CONJUNTO VASTO DE COMPETÊNCIAS QUE VAI MUITO PARA ALÉM DO CONHECIMENTO ESPECÍFICO DE CIBERSEGURANÇA, NOMEADAMENTE COMPETÊNCIAS NAS ÁREAS TECNOLÓGICA, FINANCEIRA, FISCAL, FRAUDE, ENTRE OUTRAS

exposição mediática nas suas acções de modo a promovê-la, tipicamente são ataques de negação de serviço com o objetivo de condicionar serviços online, como sites corporativos de empresas ou organismos governamentais.

Com a utilização cada vez mais massiva da Inteligência Artificial, quais os principais desafios ao nível da protecção de dados?

A adopção massiva de Inteligência Artificial pode ser analisada como uma faca de dois gumes. Por um lado, permite à comunidade de cibersegurança, e especificamente às empresas, terem acesso a tecnologias de detecção e prevenção de ataques mais sofisticadas, e um exemplo claro disso são os centros de operação de cibersegurança onde a Inteligência artificial pode ajudar na detecção de ataques e até automatizar alguns tipos de resposta num modo 24/7, assim como libertar os operadores humanos para outro tipo de actividades.

Por outro lado, os actores do cibercrime também já estão a recorrer à inteligência artificial para se munirem de técnicas de ataque mais complexas e estão a utilizar esta tecnologia para automatizar campanhas de phishing, criar imagens e vídeos deepfake para engenharia social e desenvolver código malicioso que seja mais evasivo à deteção.

Estamos a viver uma fase de grande transformação com a introdução de Inteligência artificial na sociedade e ainda ninguém sabe efectivamente qual vai ser a forma e a extensão do impacto que vai ter, pelo que a melhor maneira de nos prepararmos é apostar no conhecimento das equipas de cibersegurança e na criação de um ecossistema de colaboração com universidades, instituições públicas e empresas.

A CIBERSEGURANÇA ESTÁ CADA VEZ MAIS NO TOPO DAS PRIORIDADES DOS NOSSOS CLIENTES

Como é que a KPMG pode ser o parceiro ideal das empresas na adoção de soluções de segurança?

A KPMG tem uma posição privilegiada para apoiar as empresas neste desafio porque como empresa multidisciplinar, dispõe de um conjunto vasto de competências que vai muito para além do conhecimento específico de cibersegurança, nomeadamente competências na área tecnológica, financeira, fiscal, fraude, estratégia e operações. Esta multidisciplinariedade permite-nos ter uma visão clara do negócio dos nossos clientes e adequar a estratégia de cibersegurança ao negócio. Outro diferenciador é a escala global da rede KPMG: hoje somos mais de 9000 profissionais em cibersegurança em todo o mundo e trabalhamos em conjunto, sendo muito comum incluirmos profissionais de outros países nos projectos da KPMG em Portugal, bem como os profissionais portugueses participarem em projectos internacionais. Isto cria um ambiente de partilha e crescimento rápido que se reflecte na forma como abordamos os desafios dos nossos clientes, com a inclusão de aceleradores e ferramentas globais.

» Sérgio Martins, Partner da KPMG Portugal

Consideram que as empresas portuguesas estão bem preparadas para estes desafios?

As empresas portuguesas têm feito um investimento crescente em cibersegurança, no entanto esta é uma jornada contínua, o panorama de ameaças está sempre a mudar com novos tipos de ataque, pelo que é necessário continuar o investimento para manter e melhorar os níveis de maturidade e resiliência das empresas.

No meu entender o mercado nacional tem um grande desafio, que é a escassez de talento na área de cibersegurança, e as pessoas são o ingrediente chave para uma postura de segurança forte.

Existe uma falta reconhecida de profissionais de cibersegurança em todo o mundo e Portugal não é excepção. Em termos de oferta Portugal até já tem cursos de STEM, Pós-graduações e Mestrados especializados em cibersegurança, no entanto a procura interna e externa é bastante superior. Os muitos profissionais que emigraram durante a crise, as Nearshores com os seus centros de cibersegurança instaladas em Portugal, a competição natural por talento entre empresas em Portugal e mais recentemente a proliferação do trabalho remoto para empresas no estrangeiro está a causar uma grande pressão na captação e retenção de talento pelas empresas portuguesas nesta área. As empresas têm de ser muito criativas na forma como gerem e mantêm o talento motivado, sabendo de antemão que é muito difícil competir financeiramente contra projectos internacionais.

A KPMG PORTUGAL FEZ RECENTEMENTE UM GRANDE REFORÇO NA EQUIPA DE CIBERSEGURANÇA, COM A CONTRATAÇÃO DE MAIS DE 20 PROFISSIONAIS ALTAMENTE ESPECIALIZADOS

Ao fazerem parte de um mundo conectado, as organizações estão expostas a um maior número de ameaças. Como é que as empresas se podem proteger?

Em termos de prioridades considero que o mais relevante seja criar uma higiénica básica de segurança. Está provado estatisticamente que a grande maioria dos ataques bem-sucedidos são realizados explorando vulnerabilidades muito básicas, como emails de phishing para obtenção de credenciais a colaboradores desatentos; exploração de vulnerabilidades que já são conhecidas há algum tempo mas onde os sistemas ainda não foram actualizados; acessos a sistemas que foram deixados com as passwords de base ou com palavras chave muito fracas, etc. Ou seja, se conseguirmos ter dentro da organização uma boa higiene de segurança que garanta que os controlos básicos estão implementados conseguimos reduzir a nossa superfície de ataque drasticamente. Depois disto é importante ir investindo gradualmente na capacidade de protecção contra ameaças mais avançadas, sempre com uma visão de gestão de risco, até termos um nível de cibersegurança adequado.

Também é muito importante ter a noção de que por mais que se invista em cibersegurança, ninguém está 100% seguro e existe sempre um risco residual de sermos atacados. Nesse sentido, para além de investir na prevenção e protecção é fundamental estar preparado para a recuperação, caso o ataque seja bem sucedido, de forma a termos a capacidade de recuperar a informação que suporta o negócio em tempo útil e gerir eventuais impactos reputacionais e financeiros que daí advenham.

Ao nível da cibersegurança, como é que a KPMG olha para 2024?

A KPMG Portugal fez recentemente um grande reforço na equipa de cibersegurança, com a contratação de mais de 20 profissionais altamente especializados, sendo que em Setembro inaugurámos o nosso Hub Tecnológico de Évora, onde já começaram a ser contratados os primeiros profissionais de cibersegurança. Neste momento temos cerca de 40 profissionais espalhados pelos nossos escritórios de Lisboa, Porto e Évora, o que nos vai permitir continuar a apoiar de forma eficaz os nosso clientes. Em 2024 prevemos que o número de incidentes de cibersegurança continue a aumentar, com especial destaque para o incremento de ataques à internet das coisas – IoT, ataques suportados por inteligência artificial, ataques a redes 5G e provavelmente o tema dos ataques criptográficos utilizando computação quântica vai ganhar relevância. Também será de esperar a emergência de novas regulamentações de cibersegurança a nível europeu e nacional, bem como de reguladores em sectores específicos. Serão tempos desafiantes, mas com uma abordagem bem definida as organizações mais fortes neste capítulo vão certamente poder tirar vantagens competitivas.

ASSINE JÁ

ASSINATURAS.GREENSAVERS.PT

1 ANO
ASSINATURA DIGITAL
€9

VERSÃO EM PAPEL
€13,90

2 ANOS
ASSINATURA DIGITAL
€17,10

VERSÃO EM PAPEL
€26,60

NÃO PERCA
NENHUMA EDIÇÃO DA
GREEN SAVERS

Das empresas aos cidadãos, acompanhamos o impacto das nossas ações para o Planeta. Analisamos a sustentabilidade em todas as vertentes, apresentando uma visão global do país e do mundo.

UNICRE

EXPERIÊNCIAS DE PAGAMENTO ÚNICAS

OS PRÓXIMOS ANOS SERÃO DECISIVOS NO QUE TOCA A PROEMINÊNCIA QUE A CIBERSEGURANÇA TERÁ AO NÍVEL DA ESTRATÉGIA DE NEGÓCIO

Quando falamos do sector financeiro, e da área dos pagamentos especificamente, a inovação na forma como pagamos ou utilizamos o nosso dinheiro traz consigo novos desafios à segurança e, por consequência, uma ampla necessidade de actualização das normas e boas práticas de cibersegurança. Em entrevista à Executive Digest, Nuno Abrantes, CIO da UNICRE, explica como a empresa trabalha ao nível da cibersegurança.

A área dos pagamentos, principalmente quando falamos em conceitos como contactless e online, tem sempre associada alguma ideia de risco, de segurança. A cibersegurança é uma das vossas grandes prioridades?

Desde a sua fundação, há quase 50 anos, que a UNICRE tem tido uma forte ligação à tecnologia, acompanhando a evolução de um sector financeiro cada vez mais digital e em rápida transformação – realidade inerente ao propósito de ligar pessoas, empresas e tecnologia, proporcionando experiências de pagamento únicas. Neste propósito insere-se uma preocupação constante na garantia da total segurança ao nível da oferta que disponibilizamos aos clientes (consumidores e empresas) e ao nível dos processos internos, ambas realidades onde o risco cibernético é cada vez mais premente.

Nesse sentido, a cibersegurança é – e continuará a ser – uma prioridade na UNICRE. Prioridade essa que fazemos reflectir, reitero, em todo o nosso portefólio de produtos e serviços, através do qual trabalhamos para proporcionar experiências de pagamento únicas a cada cliente e a cada empresa, onde facilidade, rapidez, comodidade e segurança são elementos-chave. No fundo, queremos que, a partir de uma estratégia de negócio assente em princípios de cibersegurança, consigamos desenvolver soluções altamente seguras do ponto de vista da sua utilização, sem que para isso comprometamos uma melhor experiência de cada cliente.

Certo é que o trabalho de cibersegurança terá de passar também, e obrigatoriamente, por uma crescente consciencialização de consumidores e comerciantes, por um lado para as potencialidades

das soluções de pagamentos (ou aceitação de pagamentos) digitais, e por outro para os riscos cibernéticos, dotando-os para uma melhor resposta preventiva e reactiva a esta tipologia de risco.

Com o aumento da importância da cibersegurança, tendo em conta episódios recentes em algumas empresas nacionais, que trabalho tem sido desenvolvido para maximizar a segurança digital?

Apesar da crescente ocorrência de ataques cibernéticos a empresas em Portugal nos últimos anos ter sido um factor preponderante para uma maior actuação do sector empresarial ao nível da cibersegurança, acredito que o trabalho de maximização da segurança digital é uma constante, na medida em que a própria evolução tecnológica é também ela constante. Quando falamos do sector financeiro, e da área dos pagamentos especificamente, a inovação na forma como pagamos ou utilizamos o nosso dinheiro traz consigo novos desafios à segurança e, por consequência, uma ampla necessidade de actualização das normas e boas práticas de cibersegurança. E é por esse motivo que, na UNICRE, temos vindo a trabalhar, todos os dias, no sentido de garantir uma maior segurança dos nossos clientes e colaboradores no ecossistema digital, trabalho esse que reforçámos nos últimos anos e no seguimento da recente pandemia que "obrigou" o sector (e toda a economia) a acelerar a sua transição digital.

Concretamente, na área de Customer Support, temos vindo a trabalhar na garantia da protecção e integridade dos dados dos nossos clientes, quer clientes UNIBANCO (com quem aplicamos soluções de autenticação multifactor, regras de validação de transacções online, etc.), quer clientes REDUNIQ (com os quais colaboramos para mitigar fraudes com cartão e para aumentar os níveis de segurança das suas plataformas). Já a nível interno, estamos em permanente actualização das nossas práticas de protecção e acesso aos sistemas internos pelos nossos colaboradores, em resposta à crescente expansão dos nossos modelos de trabalho, cada vez mais orientados para um ambiente de trabalho digital, remoto e colaborativo.

Todas estas práticas são actualmente acreditadas pela certificação PCI-DSS (Payment Card Industry Data Security Standards), tornando-nos o primeiro e único acquirer em Portugal a deter esta norma de segurança internacional.

Consideram que é necessário combater o mito de que a cibersegurança é uma questão tecnológica? Temos de colocá-la ao nível do plano de negócio?

Creio que hoje essa questão se coloca cada vez menos, uma vez que as empresas e as suas respectivas lideranças estão cada vez mais conscientes do impacto que a cibersegurança pode trazer ao negócio. Se olharmos, por exemplo, para as conclusões do Global Risks Report 2023 desenvolvido pelo World Economic Forum, verifica-se que o alargamento do cibercrime e dos riscos cibernéticos representa o oitavo maior risco para as empresas em todo o mundo, tanto num horizonte a dois anos, como a 10. Perante este cenário, e olhando para a rápida transformação que tecnologias como a Inteligência Artificial estão a trazer ao mundo empresarial e à própria sociedade, arrisco-me a dizer que os próximos anos serão decisivos no que toca a proeminência que a cibersegurança terá ao nível da estratégia de negócio. Empresas que têm a estratégia de IT – onde a área de cibersegurança se insere – como um pilar da estratégia de negócio serão empresas mais competitivas e resilientes, não apenas no que à prevenção e mitigação dos riscos cibernéticos diz respeito, mas também relativamente à capacidade de adaptação e transformação da

» Nuno Abrantes, CIO da UNICRE

O RÁPIDO AVANÇO TECNOLÓGICO ESTÁ A ABRIR NOVOS CAMINHOS NA FORMA COMO COMUNICAMOS E INTERAGIMOS UNS COM OS OUTROS NO ECOSSISTEMA DIGITAL

sua oferta às necessidades de usabilidade e protecção exigidas cada vez mais pelos clientes, sejam estes consumidores finais ou negócios que necessitem de soluções de aceitação de pagamentos.

De que forma deve ser implementada e desenvolvida a Gestão de Risco Tecnológico?

A gestão de risco tecnológico é uma componente essencial para garantir a resiliência operacional e a protecção dos activos digitais de uma organização, na medida em que permite identificar, avaliar e mitigar potenciais riscos associados à tecnologia. A implementação eficaz desta gestão requer uma abordagem estruturada que começa com a identificação e avaliação dos riscos tecnológicos, desde as probabilidades ao grau, seguida pela formulação de estratégias de mitigação robustas.

A monitorização constante e a revisão periódica do processo (auditorias e incidentes) são fundamentais para garantir a eficácia ao longo do tempo, sem deixar de referir a formação contínua de todos os colaboradores e a aposta numa comunicação eficaz, os dois alicerces que vão permitir promover uma cultura de segurança da informação na organização. A conformidade com as normas legais e regulamentares é um requisito não negociável em todas as fases do processo. Sem esquecer que esta gestão deve ser adaptativa por natureza, permitindo um ciclo contínuo de avaliação de risco que se ajusta ao panorama tecnológico e ao ambiente de negócios em constante evolução.

» A transformação digital tem sido um elemento-chave ao longo da história da UNICRE, em que temos assistido a uma rápida transformação da forma como pagamos ou utilizamos o nosso dinheiro

Esta confiança transmite-se para os vossos clientes e comerciantes?

No que respeita aos pagamentos digitais, mais do que um cliente conhecer quais as soluções e inovações disponíveis, importa que este reconheça o seu valor acrescentado e o nível de segurança que aportam no momento de uma transacção financeira. Para tal, são fundamentais dois passos.

Em primeiro lugar, importa aos players do sector, como a UNICRE, ter a capacidade de desenvolver produtos de pagamento digitais cada vez mais seguros e que respeitem os padrões de segurança de excelência, sem que para isso seja comprometida a experiência de utilizador. Exemplo disso é a certificação PCI-DSS, norma de segurança internacional que legitima as boas práticas de segurança de uma determinada empresa, e da qual a REDUNIQ é o primeiro e único acquirer devidamente acreditado em Portugal.

Por fim, é crucial trabalhar a questão da literacia financeira (e dos pagamentos) junto de consumidores e empresas. Infelizmente, o preconceito – e diria até mesmo o medo – continuam a ser um dos principais entraves a um maior nível de penetração das soluções de pagamento digitais no mercado português, cenário que torna ainda mais relevante e necessária a implementação de um plano de educação da população e setor empresarial para a inovação nos pagamentos e nos negócios – cami-

nho que o Banco de Portugal coloca como prioritário na sua Estratégia Nacional para os Pagamentos de Retalho para 2025, onde refere como objectivo «reforçar a proximidade e transparência perante os utilizadores de serviços de pagamento e, de igual modo, aumentar o seu conhecimento e a sua confiança nas soluções disponibilizadas».

Como podemos lidar e potenciar a Protecção de Dados Pessoais, face a um mundo cibernético onde os nossos dados podem estar à disposição de qualquer pessoa?

Num ambiente onde os dados podem estar à disposição de qualquer pessoa, é essencial às empresas adoptar uma postura proactiva orientada para a constante garantia da confidencialidade e integridade dos dados dos seus clientes. Na área dos pagamentos, uma vez que lidamos diariamente com informação pessoal altamente sensível, esse desígnio é ainda mais premente, sendo, aliás, um dos focos do sector ao nível da cibersegurança. É por isso necessário que os players do sector financeiro invistam fortemente na implementação de soluções de cibersegurança e protecção de dados, em particular mecanismos como a autenticação forte, a tokenização de transacções, as assinaturas digitais certificadas e a assinatura com chave móvel digital. Ao mesmo tempo, torna-se fundamental assegurar uma maior integração entre as áreas de IT – em especial as equipas de cibersegurança – e de serviço ao cliente, de forma a que estas possam estar em permanente colaboração na prevenção, identificação e mitigação de riscos de segurança digital, para assim garantir a total segurança e a privacidade das informações pessoais que cada entidade financeira gere.

Nesta área de pagamentos, a tecnologia é o principal pilar. Como olham para o tema da transformação digital?

A transformação digital tem sido um elemento-chave ao longo da história da UNICRE, e em especial nos últimos anos, em que temos assistido a uma rápida transformação da forma como pagamos ou utilizamos o nosso dinheiro. Há uma década, seria impensável conceber a ideia de pagar apenas com um simples gesto de aproximar um cartão, um smartphone ou um wearable a um terminal de pagamento, enviar e receber dinheiro em segundos ou realizar compras que pudessem ser creditadas depois. Hoje, todos estes avanços e muitos mais são possíveis.

Acredito que, mais do que necessária, a transformação digital nos pagamentos é (e continuará a ser) um processo inevitável. O rápido avanço tecnológico está a abrir novos caminhos na forma como comunicamos e interagimos uns com os outros no ecossistema digital, e essa realidade traz, naturalmente, oportunidades ao sector financeiro, e à área dos pagamentos em particular, de criar formas diferenciadores de nós mesmos – consumidores e negócios – interagirmos com o dinheiro. Numa primeira camada, a transformação digital está a permitir-nos enquanto sector desenvolver um conjunto de soluções disruptivas que objectivam gerar experiências transacionais cada vez mais simples, rápidas e cómodas, que não só garantam elevados padrões de segurança, como também acompanhem as actuais e emergentes necessidades dos consumidores que, tal como a evolução tecnológica, também se transformam a uma velocidade alucinante. Já numa segunda camada, a transformação digital abre-nos espaço para criar uma plataforma capaz de impulsionar o crescimento dos negócios – sobretudo do pequeno negócio – que, tal como os consumidores, tenham a capacidade de modernizar a sua infra-estrutura de pagamentos como forma de se tornarem cada vez mais competitivos.

Olhamos, nesse sentido, para a transformação digital como um pilar fundamental da área dos pagamentos que nos irá permitir dar um passo em frente na construção de uma economia mais capacitada para enfrentar as exigências de um mercado cada vez mais polarizado e digital. ●

CERTO É QUE O TRABALHO DE CIBERSEGURANÇA TERÁ DE PASSAR TAMBÉM POR UMA CRESCENTE CONSCIENCIALIZAÇÃO DE CONSUMIDORES E COMERCIANTES

Assine já!

49,90€*

Assine a **MARKETEER** e receba um Creme de Dia Lift Integral Refirmante

LIERAC LABORATOIRES

CREME DE DIA LIFT INTEGRAL REFIRMANTE: É O ALIADO DIÁRIO DAS MULHERES. DIA APÓS DIA, A PELE RECUPERA FIRMEZA, PREENCHIMENTO E ELASTICIDADE. ENRIQUECIDA COM MANTEIGA DE KARITÉ, A FÓRMULA LEVE, MAS MUITO CONFORTÁVEL SUAVIZA E NUTRE A PELE. TUDO NUMA FÓRMULA COMPOSTA POR 97% DE COMPONENTES DE ORIGEM NATURAL. (PVP: 49,90€)

* Campanha limitada ao stock existente e válida para Continente e Ilhas. O produto será enviado após boa cobrança do Pack Assinatura Marketeer. Poderá consultar outras campanhas em vigor em assinaturas.multipublicacoes.pt. Venda limitada até ao máximo de 2 assinaturas por cliente. Para mais informações contacte-nos: 210 123 400 ou email assinaturas@multipublicacoes.pt.