HEXÁGONO

eBook Series | 2026

SEGURANÇA EM TECNOLOGIAS DE INFORMAÇÃO E COMUNICAÇÃO

ÍNDICE

01

Ameaças à segurança

As ameaças à segurança, das organizações e dos indivíduos, alteram-se com o tempo, com a adoção e adaptação de serviços digitais, criando inovações tecnológicas sofisticadas e complexas.

Perante esta realidade e instabilidade, é fundamental atualizar regularmente o conhecimento sobre as **ciberameaças.** No entanto, há ainda organizações que não são capazes de identificar ameaças e, consequentemente, não possuem defesas eficazes contra as mesmas, tornando-se alvos fáceis.

Em resposta a esta necessidade, **a Hexónio apresenta** aqui uma introdução a este tema, **identificando os tipos de ataque mais comuns** e **promovendo estratégias de mitigação dos riscos associados.**

"Os casos associados à exploração do fator humano tiveram muita importância, provocando amiúde prejuízos económicos nas vítimas."

Fonte: Relatório Cibersegurança em Portugal, CNCS, Dezembro 2024

125,0€ milhões

Valor relativo de bens relacionados com **fraudes online** que foram apreendidos, congelados ou confiscados.

Valor relativo de bens relacionados com **ciberataques** contra sistemas de informação que foram apreendidos, congelados ou confiscados.

124,9€ milhões

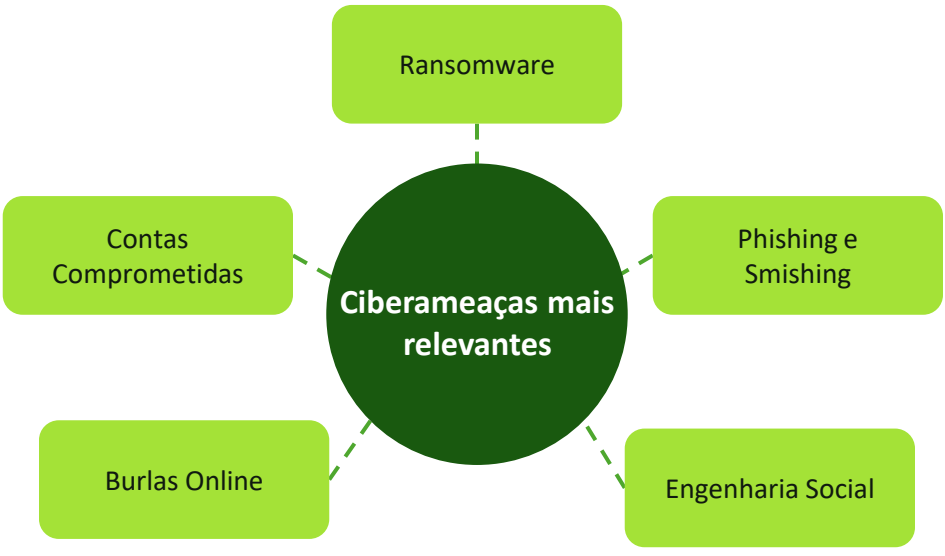
Fonte: EMPACT 2023 Results – Factsheets, Junho 2024

02

Tipos de ameaça comuns

Existem ameaças comummente usadas para furar a segurança das organizações.

Muitas destas ameaças são bastante avançadas, combinando técnicas como a engenharia social e a inteligência artificial para criar credibilidade e legitimidade, evitando a desconfiança.



Ransomware

Ransomware, ou *ransom malware*, é um tipo de ***malware*** (software malicioso) que impede o acesso ao sistema de ficheiros e exige o pagamento de um resgate para devolver o acesso.

Este tipo de **ataque tipicamente encripta**, não só os ficheiros do computador atacado, mas também os ficheiros partilhados nas redes às quais o computador tem acesso.

Neste caso, e no limite, todos os ficheiros da sua organização serão afetados.

Phishing

Phishing é um tipo de ataque que usa e-mail, SMS, WhatsApp, telefone, redes sociais e técnicas de engenharia social para induzir a vítima a partilhar informações confidenciais – como senhas ou números de contas. As informações podem ser ativamente divulgadas pela vítima, ou passivamente capturadas através de um ***software* malicioso** descarregado para o computador ou dispositivo móvel.

SMiShing

Smishing é um ataque que recorre ao envio de mensagens de texto fraudulentas (SMS) com o mesmo objetivo do *phishing*.

Um ataque de *smishing* pode envolver pessoas que fingem ser do seu banco, de um serviço de entregas ou outro tipo serviço comum.

Vishing

Vishing, é um ataque de ***phishing* por voz**. Este ataque recorre a chamadas telefónicas e mensagens de voz, muitas vezes usando vozes sintetizadas, e simula um contacto de uma organização confiável para assim convencer a serem reveladas informações como dados bancários ou credenciais de acesso.

Whaling

Um ataque de ***whaling*** é um tipo de **ataque de engenharia social** que visa especificamente executivos seniores ou de "nível C". Estes ataques têm como objetivos típicos o roubo de dinheiro, de informações, ou a obtenção de acesso ao computador do alvo para executar novos ataques cibernéticos.

Engenharia social

Este risco é de longe o **principal risco humano**.

A prová-lo está o facto de certas campanhas continuarem a ter um grande sucesso, como são exemplo:

- mensagens “olá pai, olá mãe”;
- pedido de códigos de acesso bancário;
- mensagens de falsas transportadoras a pedir para atualizar dados com o pretexto de uma entrega;
- burlas em sites de artigos em segunda mão;
- telefonemas com ofertas de emprego;
- e-mails que tentam passar por entidades bancárias ou governamentais.

A engenharia **social é agora potenciada pela inteligência artificial,** permite criar textos e guiões mais credíveis e personalizados, com menos erros ortográficos e sintáticos.

Ameaças internas

São efetuadas por pessoas intimamente ligadas à sua organização, tipicamente colaboradores, atuais ou antigos. Representam perigo pelo acesso que têm à rede interna, a dados confidenciais e a propriedade intelectual. Acresce o conhecimento que possuem sobre processos de negócios, políticas da organização e outras informações sensíveis.

As ameaças internas tendem a ser de natureza maliciosa. Nem sempre é assim, podendo ser apenas negligentes por natureza. Em qualquer caso, estas pessoas possuem conhecimento valioso que pode ajudar num **ataque forte e bem orquestrado contra a sua organização.**

03

Porquê as pessoas?

O esforço da sua equipa tornou a sua organização muito eficaz ao nível da proteção tecnológica.

Desta forma, os colaboradores da sua organização tornaram-se assim o lado mais vulnerável da componente da segurança.

Porquê?

Em parte devido à natureza humana, em parte por falha na formação e em parte por falha nos procedimentos.

Falta de consciencialização

As pessoas não têm conhecimento das diversas ameaças à segurança nem como as identificar.

Ficam assim mais expostas e vulneráveis, tornando-se um **alvo fácil e apetecível**.

Comportamento humano

As pessoas seguem o caminho que melhor conhecem por hábitos de trabalho, por vezes cortam atalhos e, mais vezes do que desejam, cometem erros. Partilhar credenciais de acesso, clicar em *links* maliciosos, compartilhar inadvertidamente dados e informações confidenciais ou abrir anexos de e-mail infetados, tudo compromete a segurança.

Complexidade tecnológica

Com a velocidade e crescente complexidade da tecnologia e das medidas de segurança, as pessoas tendem a achar que **é difícil compreender, acompanhar e implementar** práticas de segurança adequadas, ficando assim mais vulneráveis a ataques.

Políticas e procedimentos

Quando as organizações **não possuem procedimentos nem políticas** para lidar com informações confidenciais e incidentes de segurança, levam muitas vezes os seus colaboradores a tomarem más decisões ou a cometerem erros.

Quando essas políticas existem, nem sempre são claras ou nem sempre a sua aplicação é realmente imposta, tornando-se assim ineficazes.

A existência de políticas e procedimentos é tão ou mais importante como a consciencialização e a formação dos colaboradores, **por forma a que todos compreendam a melhor forma de se defenderem**.

04

Acessos, segurança e informação

A sua equipa de infraestruturas tecnológicas trabalha incansavelmente.

Só assim é possível garantir a segurança de todos os seus sistemas. Este esforço vai muito para lá do que é visível, como por exemplo a atualização do seu posto de trabalho ou a implementação de políticas de acesso seguro aos recursos da sua organização.

Provavelmente sabe que há um grande trabalho de bastidores para garantir **que toda a sua infraestrutura está atualizada**, **corretamente configurada e a funcionar da melhor forma.** Isto acontece, por exemplo, nos servidores, *routers*, *firewalls*, *VPNs*, serviços de Cloud mas também na componente de desenho de arquitetura, implementação de redundância, política de cópias de segurança e implementação de tolerância a falhas.

Tudo isto para criar resiliência e **garantir que a sua atividade não pára**.

O que provavelmente desconhece, é que o empenho da sua equipa de infraestruturas não se esgota aí.
Há **ainda exigentes desafios** que são abordados com afinco para manter a sua infraestrutura operacional e segura. São disso bons exemplos, a proativa monitorização de ativos de rede, a segmentação e segregação da rede informática e protocolos específicos no descarte de equipamentos.

Na sua organização todos **têm acesso a informação que é considerada sensível**, mas nem sempre existe a noção de que se lida com dados sensíveis e que estes podem comprometer a segurança da organização

No entanto:

- Informação marcada como confidencial ou de uso interno;
- Imagens das instalações próprias ou de clientes (tanto interiores como exteriores);
- Dados pessoais;
- Credenciais de acesso;
- Conteúdo de propostas;
- Informação financeira;
- Informação operacional;
- Informação de negócio;
- Informação de segurança;
- Formas de acesso, tanto físico como digital;

são exemplos de informação sensível que deverá estar estritamente acessível apenas a quem dela necessita para as suas funções.

05

Prevenção

Para combater as ameaças, a sua organização deve implementar um programa abrangente de **formação em segurança** que ensine a todas as partes interessadas a estarem cientes de qualquer potencial ataque, incluindo aqueles realizados por alguém interno.

Em qualquer organização, **as pessoas são a primeira linha de defesa** contra as ameaças à segurança. Embora as tecnologias e os sistemas avançados de defesa desempenhem um papel fundamental na proteção de dados e infraestruturas, a vigilância e a sensibilização dos colaboradores, internos e externos, e outros intervenientes são igualmente essenciais.

Seja um ativo de segurança!

Siga sempre as políticas e os protocolos de segurança instituídos na sua organização. Estando num cliente, cumpra igualmente com as políticas e protocolos de segurança do cliente. Na sua falta, pode seguir estas recomendações:

- Guarde sigilo;
- Não divulgue informação internamente a quem não está no âmbito do processo, projeto ou atividade;
- Não passe informação a terceiros, internos ou externos, sem o devido consentimento;
- Não use redes sociais como um canal de comunicação profissional;
- Não trate temas profissionais em locais públicos, isto inclui chamadas telefónicas e uso do computador;
- Se tiver dúvidas, consulte o seu superior direto e/ou a sua equipa de segurança.

Segurança comportamental

A segurança comportamental, tanto física como digital, é uma **componente crítica para garantir a segurança** na sua organização.

Recomendamos estas boas práticas:

- Nunca partilhar nem deixar credencias à vista (*post-its* no monitor; *sticky notes*; etc.);
- Nunca deixar o computador desbloqueado quando ausente do mesmo;
- Na presença de múltiplos fatores de autenticação, nunca aprovar pedidos que não sejam seus, nem com origem desconhecida ou duvidosa;
- Nunca responder a pedidos que incluam informações críticas ou confidenciais nas quais o seu supervisor direto não esteja envolvido ou das quais não tenha conhecimento;
- Usar exclusivamente os canais oficiais para comunicar informação sensível;

- Não usar redes sociais, ou semelhantes, como canal de comunicação profissional;
- Não enviar informações nem credenciais de acesso por WhatsApp, Telegram ou qualquer outro meio semelhante;
- Não enviar as várias componentes de acesso na mesma mensagem (por exemplo, não enviar o nome de utilizador juntamente com a senha) e, preferencialmente, evitar o mesmo meio de comunicação;
- Não partilhar informação com soluções de IA, *bots*, redes sociais e semelhantes;
- Não usar o computador, *tablet* e semelhantes em locais públicos, onde terceiros possam estar a ver (esplanadas, comboios, etc.);
- Não ter conversas telefónicas com conteúdo sensível em locais públicos como restaurantes, transportes públicos e ambientes semelhantes;

- Não utilizar redes públicas, com pouca segurança ou que não transmitam confiança (p.e. *wifi públicos*, *hotspots* gratuitos, etc.);
- Em caso de roubo, furto, suspeita de falha ou violação de segurança, contactar imediatamente o superior e/ou a sua equipa de segurança (física e digital).

Pedidos ou situações duvidosas

Em caso de dúvida quanto a um pedido ou situação:

- Caso não seja efetuado através do canal instituído, referir o uso o canal de comunicação oficial;
- Caso exista urgência, insistência ou pressão para agir no momento, referir que tem mesmo de se usar o canal oficial e escalar o assunto para o superior;
- Na eventualidade de um pedido ou situação não se encontrar coberto pelos procedimentos definidos, contactar o superior direto.

06

Equipa Hexónio

A Hexónio tem uma equipa de infraestruturas tecnológicas competente e dedicada

Temos ao seu dispor um conjunto de áreas e serviços para apoiar a sua organização:

- Service Desk
- Field Support
- Administração de Redes e Sistemas
- Segurança Informática
- Network Operations Center
- Administração e Operação de Aplicações
- Apoio ou expansão da sua equipa de TI
- Consultoria em Sistemas de Informação

Fale Connosco

O nosso CTO e responsável pela área de infraestruturas terá todo o gosto em falar consigo:

- **Jorge Ferreira**
- **jorge.ferreira@hexonio.com**

HEXONIO
CONSULTING

hexonio@hexonio.com

www.hexonio.com

+351 211 542 606

Rua Amélia Rey Colaço, 40
2790-017 Carnaxide
Portugal