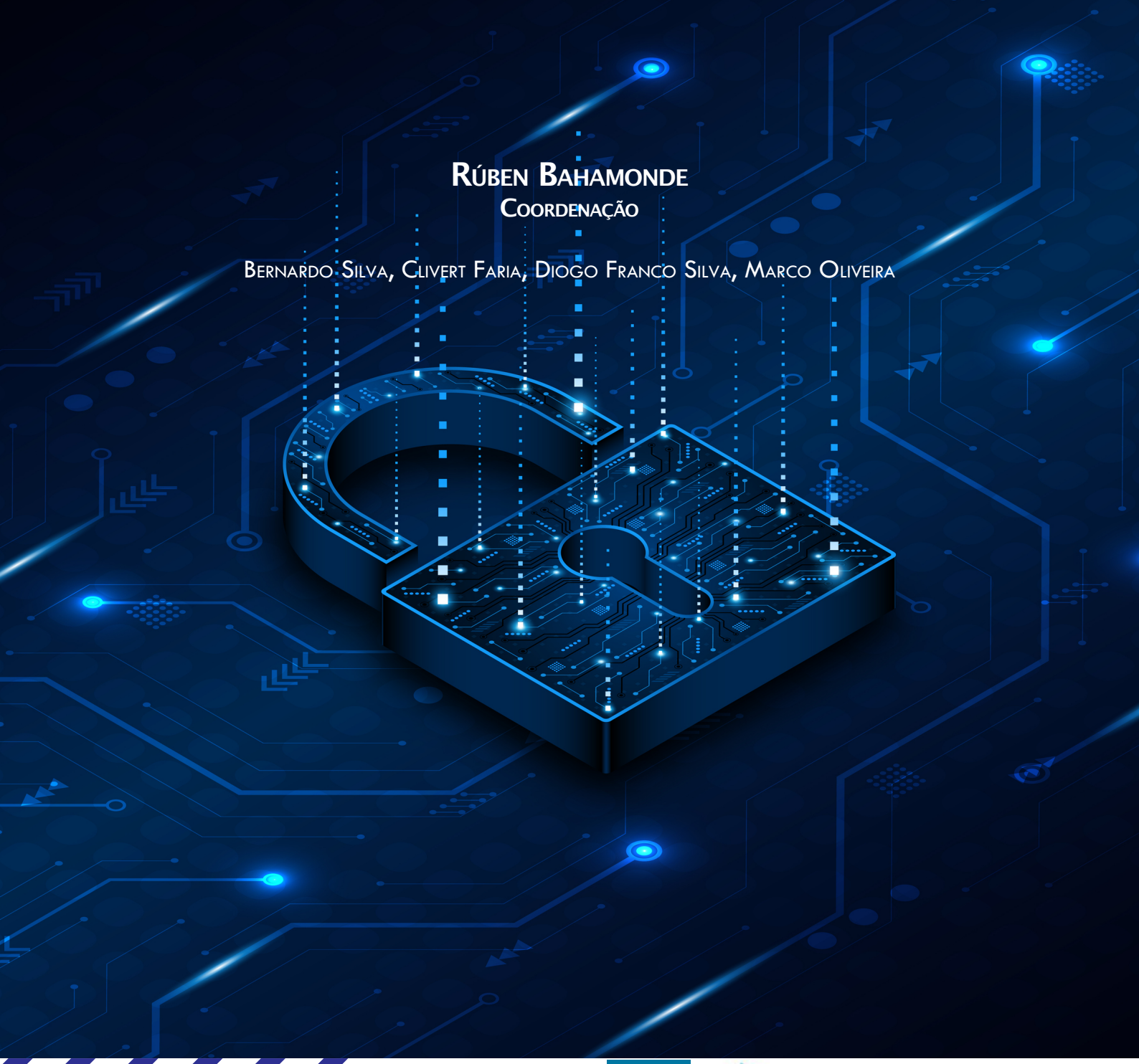
Rúben Bahamonde
Coordenação

Bernardo Silva, Clivert Faria, Diogo Franco Silva, Marco Oliveira



Guia de Cibersegurança

PRR Plano de Recuperação e Resiliência
República Portuguesa
Financiado pela União Europeia NextGenerationEU

Rúben Bahamonde
Coordenação

Bernardo Silva, Clivert Faria, Diogo Franco Silva, Marco Oliveira

Guia de Cibersegurança

FICHA TÉCNICA

TÍTULO *Guia de Cibersegurança*

CORDENAÇÃO Rúben Bahamonde

AUTORES Bernardo Silva, Clivert Faria, Diogo Franco Silva, Marco Oliveira

COORDENAÇÃO EDITORIAL Raquel Medina Cabeças

EDITORA Universidade Autónoma de Lisboa - Autónoma Edições

PAGINAÇÃO E DESIGN Raquel Medina Cabeças

CAPA IStock - Natthaphon Wanason

ISBN 978-989-9002-60-9

DOI https://doi.org/10.26619/978-989-9002-60-9

COMO CITAR ESTA PUBLICAÇÃO

Bahamonde, Rúben (Coord.) (2025). *Guia de Cibersegurança*. Universidade Autónoma de Lisboa - Autónoma Edições. https://doi.org/10.26619/978-989-9002-60-9

Centro de Competências de Cibersegurança de LVT
Rua General Firmino Miguel, 8A, 1600-300 Lisboa, Portugal
Tel: 211 300 362
e-mail: info@ccc-lisboavt.pt

PRR Plano de Recuperação e Resiliência
REPÚBLICA PORTUGUESA
Financiado pela União Europeia NextGenerationEU
network ccclisboa e vale do tejo

A Cooperativa de Ensino Universitário, entidade instituidora da Universidade Autónoma de Lisboa, promove a produção científica em vários segmentos culturais, valorizando a relação entre a comunidade académica e a sociedade. Desta forma, apoia a edição desta publicação, contribuindo para a divulgação do conhecimento.

ÍNDICE

1. Quem Somos

O Centro de Competências em Cibersegurança de Lisboa e Vale do Tejo (CCC-LVT) apoia as empresas a compreender onde se encontram no caminho da segurança digital e a traçar um percurso mais sólido rumo à ciber-resiliência.

Fonte: IStock - Thapana Onphalai

Orienta as Pequenas e Médias Empresas (PME) na avaliação da resiliência em cibersegurança, fortalecendo os seus ativos digitais e alinhando-se com a Estratégia Nacional de Segurança do Ciberespaço (ENSC).

A segurança da informação é essencial para a continuidade dos negócios, a confiança dos clientes e a conformidade legal. Este guia oferece ferramentas para as PMEs classificarem o seu estado na evolução da defesa cibernética. De forma a identificarem as próximas medidas preventivas que sejam de implementação recomendada, promovendo a cibersegurança como um investimento estratégico.

Financiado pelo PRR e pela União Europeia, este projeto visa criar um ambiente digital mais seguro e sustentável, incentivando as PMEs a evoluírem continuamente na proteção dos seus ativos digitais.

Através da análise de riscos, deteção de vulnerabilidades e planeamento de ações, capacitamos as empresas para tomarem decisões informadas adaptadas as realidade de cada empresa, garantindo um futuro digital mais seguro e preparado para os desafios emergentes.

Servimos de ponte e facilitador com a C-Academy, com o Pólo de Inovação Digital – C-HUB, e disponibilizar orientações com vista ao cumprimento dos requisitos legais e de certificação.

2. Introdução
O INICIO DA CIBERSEGURANÇA

Na era digital, a cibersegurança é essencial para a continuidade operacional e proteção de ativos digitais, especialmente para as Pequenas e Médias Empresas. Estas enfrentam ciberataques crescentes, muitas vezes sem os recursos necessários para implementar medidas de proteção robustas.

Os ataques podem resultar em interrupções operacionais, perdas financeiras significativas e danos à reputação, afetando a confiança de clientes e parceiros. Além disso, a má gestão de dados sensíveis pode levar a multas elevadas e responsabilização dos gestores. O Regulamento Geral sobre a Proteção de Dados (RGPD) prevê coimas que podem atingir 20 milhões de euros ou 4% do volume de negócios anual, consoante o valor mais elevado[1].

Diversos estudos indicam que as PMEs são frequentemente vistas como alvos fáceis devido à falta de medidas de proteção adequadas. Em média, uma organização em Portugal sofre 2.116 ataques cibernéticos por semana[2]. Além disso, nos EUA, as pequenas empresas gastam, em média, 955 mil dólares por ataque para restaurar as suas operações normais, um custo que pode ser insustentável para muitas PMEs[3].

1 PHC business software (2023). RGPD em Portugal: multas mínimas de 1000€ para PME. Disponível em: https://phcsoftware.com/pt/artigo/rgpd-portugal-multas

2 Duro, R. (2024). PME "gravemente vulneráveis" aos desafios da cibersegurança. Diário de Notícias. Disponível em: https://www.dn.pt/conferencia-novo-regime-juridico- da-ciberseguranca-em-portugal/pme-gravemente-vulneraveis-aos-desafios-da-ciberseguranca

3 Minolta, K. (2024). As PME estão mais vulneráveis a ciberataques? Konica Minolta. Disponível em https://www.konicaminolta.pt/pt-pt/rethink-work/security/as-pme- estao-mais-vulneraveis-a-ciberataques; Allianz (2023). Allianz Risk Barometer - Identifying the major business risks for 2023. Disponível em: https://commercial.allianz.com/content/dam/onemarketing/commercial/commercial/reports/Allianz-Risk-Barometer-2023.pdf.

DESAFIOS DAS PME

Apesar de representarem uma grande parte da economia global, muitas PMEs subestimam o risco em cibersegurança, acreditando que os atacantes visam apenas grandes corporações.

"As empresas identificam os ciberataques, especialmente as violações de dados, como a sua principal preocupação empresarial para o ano 2025"

Allianz, 2025

"[As PMEs] constituem a espinha dorsal da economia portuguesa mas continuam gravemente vulneráveis devido à falta de recursos, conhecimento e maturidade para gerir incidentes em cibersegurança"

Duro, 2024

- As PMEs são frequentemente vistas como alvos fáceis devido à falta de medidas de proteção adequadas.
- Os cibercriminosos exploram vulnerabilidades como software desatualizado, redes mal configuradas e colaboradores sem formação específica.

As PMEs constituem a espinha dorsal da economia portuguesa, mas continuam gravemente vulneráveis devido à falta de recursos, conhecimento e maturidade para gerir incidentes em cibersegurança, representando 99,9% do total das empresas em Portugal[5].

Os benefícios de um ambiente seguro para adotar uma estratégia de cibersegurança robusta traz inúmeras vantagens:

1. Proteção de Dados e Privacidade: A implementação de boas práticas de cibersegurança protege dados sensíveis, como informações financeiras, pessoais e comerciais, prevenindo o roubo de dados e garantindo o cumprimento das leis de proteção de dados, como o RGPD[6].

2. Redução de Perdas Financeiras: Com medidas de cibersegurança adequadas, as empresas podem evitar prejuízos financeiros significativos, como os causados por ataques de ransomware e fraudes. Isso inclui a proteção contra custos de resgates e reparações de sistemas[7].

3. Fortalecimento da Confiança dos Clientes Empresas: Garantem que a segurança dos dados dos clientes aumentam a confiança e fidelização dos mesmos, o que é essencial para a manutenção de bons relacionamentos comerciais e competitividade no mercado.

4. Continuidade dos Negócios: Com práticas de segurança eficazes, as empresas garantem a continuidade das suas operações, minimizando o impacto de incidentes cibernéticos e evitando interrupções nos serviços que possam afetar a experiência do cliente[8].

5. Redução de Riscos Reputacionais: Investir em cibersegurança ajuda a proteger a reputação da empresa, evitando danos à imagem causados por fugas de dados ou ataques. Isso contribui para a manutenção da confiança do público e parceiros comerciais.

A cibersegurança não deve ser encarada como um simples centro de custos, massim como um ativo estratégico que desempenha um papel crucial nasustentabilidade e competitividade das empresas.

5 Pordata. (2022). Empresas: Total e por dimensão. Disponível em https://www.pordata.pt/pt/documentos-indicadores
6 Alves, D. L. (2021). O papel fundamental da Cibersegurança na Proteção de Dados Pessoais. Anuário da Proteção de Dados. Disponível em: https://protecaodedadosue.cedis.fd.unl.pt/wp-content/uploads/2022/10/5.-Diogo-Lopes-Alves.pdf
7 Na conferência Web Summit 2024 que se realizou em Lisboa, de 11 a 14 de novembro, foram muitos os oradores que se debruçaram sobre a cibersegurança, e algumas startups apresentaram ideias e plataformas com inovações para minimizar efeito de ciberataques. TV Europa. (2024, novembro 14). A fraude está a ser reinventada pela tecnologia digital. Disponível em https://www.tveuropa.pt/noticias/a-fraude-esta-a-ser-reinventada-pela-tecnologia-digital/. Acresce que, como se verá em seguida, apenas 8% das empresas que pagam o resgate recuperam todos os seus dados.
8 Silva, N. (2022). A importância da Continuidade do Negócio para a Ciber-resiliência. IT Security. Disponível em: https://www.itsecurity.pt/news/opinion/a-importancia- da-continuidade-do-negocio-para-a-ciber-resiliencia

3. Riscos no Setor
A atualidade das ameaças no setor da Educação/Ensino

Riscos no Setor da Educação

A Atualidade das Ameaças

O setor da educação enfrenta desafios crescentes em cibersegurança devido à digitalização acelerada. Escolas e universidades tornaram-se alvos privilegiados para cibercriminosos, que exploram vulnerabilidades em sistemas de gestão académica, plataformas de ensino e redes institucionais.

Segundo um relatório da Check Point Research (2024), a educação foi o setor mais atacado globalmente, com uma média de 3.086 ataques semanais por instituição, um aumento de 37% face ao ano anterior. Portugal encontra-se entre os países mais afetados[9].

O setor da educação enfrenta riscos de cibersegurança cada vez mais sofisticados, exigindo um investimento contínuo em segurança digital, formação de utilizadores e implementação de medidas de mitigação. Soluções como autenticação multifator, encriptação de dados e monitorização ativa são essenciais para proteger a integridade das instituições de ensino e a privacidade dos seus membros[10].

Principais Ciber-riscos na Educação

1. Roubo de Dados Académicos

As instituições de ensino armazenam dados sensíveis, incluindo informações pessoais, financeiras e acadêmicas de alunos, professores e funcionários. Estes dados são altamente valiosos para cibercriminosos, que os utilizam para fraudes financeiras, roubo de identidade e venda na dark web. Ataques recentes, como a violação da PowerSchool em 2024, expuseram milhões de registos de estudantes e docentes nos EUA e Canadá[11]. Além disso, muitas instituições não possuem sistemas de proteção adequados, tornando-se alvos fáceis para hackers.

2. Ataques de Ransomware

Ransomware continua a ser uma das maiores ameaças, bloqueando sistemas críticos e exigindo resgates. Estes ataques podem paralisar por completo as operações escolares, impedindo o acesso a plataformas de ensino, notas e registos administrativos. Em 2023, um ataque a uma escola em Portugal bloqueou a plataforma de gestão académica, comprometendo notas e dados de matrículas[12]. Em muitos casos, mesmo após o pagamento do resgate, os sistemas não são totalmente recuperados, causando perdas permanentes.

3. Phishing e Engenharia Social

Emails fraudulentos dirigidos a professores e funcionários são uma via comum de ataque. O setor educativo está entre os cinco mais afetados por phishing, devido à elevada rotatividade de pessoal e à falta de formação

9 Check Point Research, "Every Day is a School Day for Cyber Criminals with the Education Sector as the Top Target in 2024," 2024. [Online]. Available: https://blog.checkpoint.com/research/check-point-research-warns-every-day-is-a-school-day-for-cybercriminals-with-the-education-sector-as-the-top-target-in-2024/

10 CNCS Portugal, "Relatório de Cibersegurança no Ensino," 2024. [Online]. Available: https://www.cncs.gov.pt/relatorios/relatorio-de-ciberseguranca-no-ensino-2024

11 J. Vincent, «PowerSchool data breach leaks info of students and staff at schools across the US and Canada,» The Verge, 2025. [Online]. Available: https://www.theverge.com/2025/1/10/24340556/powerschool-sis-data-breach-leak-student-data-us-canada-schools

12 Contacto, "Hackers Atacam Escola Portuguesa e Exigem Resgate," 2024. [Online]. Available: https://www.contacto.pt/noticias/hackers-atacam-escola-portuguesa-e-exigem-resgate

em cibersegurança[13]. Estes ataques aproveitam-se da falta de conhecimento dos utilizadores, levando-os a partilhar credenciais ou a instalar software malicioso. Com o aumento do ensino remoto, os ataques de phishing tornaram-se ainda mais sofisticados, utilizando inteligência artificial para personalizar mensagens fraudulentas.

4. Vulnerabilidades em Plataformas de Ensino Online

Plataformas de ensino remoto, como Moodle e Microsoft Teams, frequentemente apresentam falhas exploradas por hackers. Brechas de segurança permitem o roubo de credenciais e a modificação de notas[14]. Estas plataformas são essenciais para a aprendizagem moderna, mas muitas vezes não possuem os níveis de segurança adequados, expondo alunos e professores a riscos. Além disso, ataques direcionados podem comprometer a privacidade das aulas e até permitir a sua interrupção por agentes mal-intencionados.

5. Ataques a Sistemas de Matrículas e Pagamentos

Plataformas de matrícula e pagamento são alvos de fraudes e roubo de dados financeiros. Estes sistemas armazenam informações bancárias de alunos e encarregados de educação, tornando-os alvos valiosos para ciberataques. Em 2023, um ataque a uma universidade europeia comprometeu milhares de registos financeiros[15]. Além de perdas monetárias, estas falhas comprometem a confiança das famílias e alunos na instituição, afetando a sua reputação e credibilidade.

6. Ataques de Negação de Serviço (DDoS)

Ataques DDoS podem paralisar serviços online essenciais, como plataformas de ensino e portais administrativos, tornando-os inacessíveis para estudantes e professores[16]. Estes ataques são particularmente prejudiciais durante períodos de exames e inscrições, gerando caos no funcionamento das instituições. Muitos hackers utilizam redes de dispositivos IoT comprometidos para lançar estes ataques, sobrecarregando servidores e interrompendo o acesso a serviços críticos.

7. Espionagem e Roubo de Propriedade Intelectual

Universidades e centros de pesquisa são alvos de ciber-espionagem, visando o roubo de propriedade intelectual e inovação tecnológica. Estados-nação e grupos organizados tentam obter acesso a pesquisas valiosas em áreas como inteligência artificial, biotecnologia e defesa[17]. O roubo de dados de pesquisa pode comprometer anos de trabalho académico e científico, além de colocar em risco parcerias internacionais e financiamento de projetos inovadores.

8. Comprometimento de Infraestruturas Tecnológicas

O aumento do uso de dispositivos IoT em escolas criou novas vulnerabilidades. Sistemas de controlo de acessos, câmaras de vigilância e sensores inteligentes podem ser comprometidos, pondo em risco a segurança física[18]. Um ataque bem-sucedido pode permitir a intrusão em edifícios escolares ou mesmo a manipulação de sistemas críticos, como alarmes de incêndio e iluminação. A falta de encriptação adequada e a utilização de senhas fracas tornam estes dispositivos alvos fáceis para hackers.

13 CrowdStrike, «Phishing in Education: A Growing Concern,» 2024. [Online]. Available: https://www.crowdstrike.com/blog/phishing-in-education-a-growing-concern/
14 CISA, «Cybersecurity Risks in Remote Learning Platforms,» 2024. [Online]. Available: https://www.cisa.gov/news-events/alerts/2024/01/21/cybersecurity-risks-remote-learning-platforms
15 Executive Digest, "Ataques a Universidades Europeias Comprometem Dados Financeiros," 2023. [Online]. Available: https://executivedigest.sapo.pt/ataques-a-universidades-europeias-comprometem-dados-financeiros/
16 Akamai, «Education Sector Among Top DDoS Attack Targets,» 2024. [Online]. Available: https://www.akamai.com/blog/security/education-sector-among-top-ddos-attack-targets
17 ENISA, «Cybersecurity Threats in Higher Education,» 2024. [Online]. Available: https://www.enisa.europa.eu/publications/cybersecurity-threats-in-higher-education
18 IT Security, «IoT Vulnerabilities in Schools: A Growing Risk,» 2024. [Online]. Available: https://www.itsecurityguru.org/2024/02/15/iot-vulnerabilities-in-schools-a-growing-risk/

A atualidade das ameaças no setor da Hotelaria

O setor da hotelaria enfrenta hoje desafios crescentes no mundo digital. Com a transformação digital a acelerar, as empresas deste setor dependem cada vez mais de tecnologias para gerir operações, reservas e a comunicação com os hóspedes. Contudo, esta modernização vem acompanhada de riscos – especialmente porque os hotéis processam dados extremamente sensíveis, tornando-os alvos atrativos para cibercriminosos.

Segundo um relatório da IT Security, o setor da hotelaria sofre em média milciberataques por semana[19]. Além disso, 89% das empresas hoteleiras sãovítimas de pelo menos dois ciberataques bem-sucedidos por ano[20].

19 IT Security. (2023). Setor de viagens e hotelaria sofre mil ciberataques por semana. Disponível em: https://www.itsecurity.pt/news/threats/setor-de-viagens-e-hotelaria- sofre-mil-ciberataques-por-semana
20 Reis, R. A. (2023). Quase 90% do setor hoteleiro sofre dois ataques informáticos por ano com sucesso. Jornal Económico. Disponível em: https://jornaleconomico.sapo.pt/noticias/quase-90-do-sector-hoteleiro-sofre-dois-ataques-informaticos-por-ano-com-sucesso/

1. Roubo de Dados de Clientes

Os hotéis processam diariamente grandes volumes de informações pessoais e financeiras, como números de cartões de crédito, passaportes e contactos. Estes dados têm um valor elevado no mercado negro digital, tornando os sistemas de gestão de reservas e pagamento alvos frequentes de ciberataques.

2. Ataques de Ransomware

Em 2022, um hacker russo roubou meio milhão de euros de um hotel em Lisboa, explorando vulnerabilidades nos sistemas de pagamento[21]. O ransomware continua a ser uma das maiores ameaças ao setor. Neste tipo de ataque, os criminosos bloqueiam o acesso a sistemas críticos - como as de reservas, check-in e faturação – e exigem um resgate para a sua libertação.

Em 2017, um hotel austríaco viu-se forçado a pagar um resgate para recuperar o acesso às fechaduras eletrónicas dos quartos, impedindo temporariamente os hóspedes de entrarem nos seus aposentos[22]. Segundo a Sophos Cybersecurity, 92% das empresas que pagam resgates acabam por ser atacadas novamente[23]. De acordo com o relatório Sophos State of Ransomware 2021, o número de organizações que decidem pagar um resgate aumentou e a mesma pesquisa global descobriu que apenas 8% deles recuperaram todos os seus dados. Quase um terço, 29%, não conseguiu recuperar mais da metade dos dados criptografados[24].

21 Lopes, S. (2022). Hacker russo atacou um hotel em Lisboa — e roubou meio milhão de euros. NiT. Disponível em: https://www.nit.pt/fora-de-casa/turismos-rurais-e- hoteis/hacker-russo-atacou-um-hotel-em-lisboa-e-roubou-meio-milhao-de-euros

22 Bilefsky, D. (2017). Hackers use new tactic at Austrian hotel: Locking the doors. The New York Times. Disponível em: https://www.nytimes.com/2017/01/30/world/europe/hotel-austria-bitcoin-ransom.html
23 Shulmistra, D. (2023). 6 Reasons Not to Pay the Ransom in a Ransomware Attack (Updated with Negotiation Tips). Invenio IT. Disponível em: https://invenioit.com/security/pay-the-ransom/#:~:text=A%20staggering%2092%25%20of%20companies,to%20research%20by%20Sophos%20Cybersecurity
24 Sophos. (2024). The State of Ransomware 2024. Disponível em: https://www.sophos.com/en-us/content/state-of-ransomware

3. Phishing e Engenharia Social

Os funcionários dos hotéis são frequentemente visados em campanhas de phishing, através de emails fraudulentos que os induzem a divulgar credenciais de acesso ou a instalar software malicioso.

De acordo com a CrowdStrike, a hotelaria está entre os cinco setores mais afetados por ataques de phishing, devido à elevada rotatividade de colaboradores e à falta de formação contínua. Recentemente, técnicas sofisticadas como deepfakes e mensagens altamente personalizadas têm vindo a aumentar a taxa de sucesso destes ataques[25].

4. Vulnerabilidades em Redes Wi-Fi

Muitos hotéis oferecem Wi-Fi gratuito aos hóspedes. Redes mal configuradas ou sem encriptação adequada podem permitir que cibercriminosos acedam a dispositivos conectados, monitorizem o tráfego de dados e intercetem informações sensíveis.

Um estudo da IT Security revelou que mais de 75% das redes Wi-Fi de hotéis testadas apresentavam vulnerabilidades críticas, permitindo o roubo de credenciais de acesso a sites bancários e redes sociais[26].

5. Fraudes em Plataformas de Reserva Online

As plataformas de reserva online, sejam internas ou de terceiros, são frequentemente alvo de ataques que visam desviar transações ou manipular preços, causando perdas financeiras e danos reputacionais.

6. Exploração de Sistemas de Pagamento e Ponto de Venda (PoS)

Os sistemas de pagamento e terminais de ponto de venda (PoS) são alvos frequentes de ataques que instalam malware para capturar os dados dos cartões de crédito dos clientes. O ciberataque ao grupo MGM Resorts em 2023 ilustra bem este risco: o ataque paralisou os sistemas de pagamento, os serviços de check-in e até as máquinas de jogo dos casinos, resultando em milhões de euros de prejuízo[27].

7. Ataques de Negação de Serviço (DDoS)

Os ataques de DDoS visam sobrecarregar os sistemas dos hotéis, tornando-os inacessíveis para reservas online e operações internas. Estes ataques podem resultar em perda de reservas e causar impactos negativos na experiência do cliente[28].

8. Espionagem e Roubo de Propriedade Intelectual

Hotéis de luxo e as cadeias de hotéis internacionais são locais estratégicos para reuniões de negócios e conferências, tornando-se alvos preferenciais de espionagem industrial.

A ENISA (Agência da União Europeia para a Cibersegurança) alerta que hotéis em cidades com elevada concentração de eventos empresariais são frequentemente alvo de ataques para obtenção de informações sensíveis, que pode ser conprovado através do relatório sobre o estado do Ransomware da SOPHOS[29].

O setor hoteleiro enfrenta riscos de cibersegurança cada vez mais sofisticados, exigindo um investimento contínuo em infraestruturas de TI, formação dos colaboradores e monitorização ativa.

25 Faulhaber, J., & Moon, B. (2023). Small Business Cyberattack Analysis: Most-Targeted SMB Sectors and Key Prevention Tips. CrowdStrike. Disponível em: https://www.crowdstrike.com/en-us/blog/small-business-cyberattack-analysis-most-targeted-smb-sectors/

26 IT Security. (2022). Cibercriminosos apagam dados de grupo hoteleiro "por diversão". Disponível em: https://www.itsecurity.pt/news/news/cibercriminosos-apagam- dados-de-grupo-hoteleiro-por-diversao

27 Gomez, F. (2025). Cyber Attack & Breach on the MGM Resort Explained. Inszone Insurance. Disponível em: https://inszoneinsurance.com/blog/cyberattack-mgm- resort-explained

28 IT Security. (2023). Setor de viagens e hotelaria sofre mil ciberataques por semana. IT Security. Disponível em: https://www.itsecurity.pt/news/threats/setor-de- viagens-e-hotelaria-sofre-mil-ciberataques-por-semana

29 Sophos. (2024). The State of Ransomware 2024. Disponível em: https://www.sophos.com/en-us/content/state-of-ransomware

4. Fundamentos
COMEÇAR PELO FUNDAMENTAL

Fonte: IStock - Urupongi

A cibersegurança tornou-se um pilar essencial na era digital, desempenhando um papel fundamental na proteção de sistemas, redes e dados contra acessos não autorizados e ataques maliciosos. Num mundo altamente interligado, onde a tecnologia é a espinha dorsal da sociedade moderna, garantir a segurança dos ambientes digitais deixou de ser uma preocupação exclusiva das áreas técnicas para se tornar uma prioridade estratégica. Esta proteção não se limita apenas à salvaguarda da informação, mas abrange a privacidade dos utilizadores, a integridade dos dados críticos, a confiança nas transações eletrónicas e a continuidade das operações empresariais e institucionais[30].

Embora a Internet tenha sido uma das maiores revoluções tecnológicas da humanidade, também se tornou um campo fértil para ameaças cibernéticas cada vez mais sofisticadas.

Entre os perigos mais comuns, destaca-se o malware, um termo abrangente para programas maliciosos desenvolvidos para infiltrar, danificar ou roubar informações. Este inclui vírus, worms, trojans e spyware, cada um com métodos distintos de infetar sistemas e comprometer a segurança.

O phishing, uma das técnicas de ataque mais eficazes, explora a manipulação psicológica para levar as vítimas a fornecerem credenciais de acesso ou dados bancários, através de comunicações fraudulentas que imitam entidades legítimas.

O ransomware, uma ameaça crescente, encripta os ficheiros da vítima e exige um resgate para a sua recuperação, afetando desde indivíduos a grandes organizações e infraestruturas críticas.

Outra técnica frequentemente utilizada por atacantes é o ataque de força bruta, que explora credenciais fracas através da tentativa sistemática de múltiplas combinações de palavras-passe, expondo contas e sistemas a acessos indevidos.

30 No plano nacional, o Centro Nacional de Cibersegurança identificou especificamente três cenários de ameaça ao ciberespaço que permitem ter uma maior consciência da realidade do problema que se defronta. O primeiro cenário, com especial relevo para as PME´s resulta da cibercriminalidade internacional, alguma dela cibercrime-como-serviço, altamente organizada e profissionalizada. O segundo cenário, mais centrado na administração pública, resulta do contexto geopolítico e estratégico das guerras/conflitos existentes que fomentam a beligerância político-ideológica e a prática de atos de ciberespionagem ou de cibersabotagem. Por fim, o terceiro cenário, que implica um risco específico das PME´s e outros agentes económicos, está relacionado com a disseminação de plataformas de IA generativa com grande capacidade para a criação de conteúdos falsos e muito verosímeis e para a automatização de processos de desenvolvimentos técnicos maliciosos. Centro Nacional de Cibersegurança. (2024). Relatório de Cibersegurança em 2024. p. 12. Disponível em: https://www.cncs.gov.pt/docs/rel-riscosconflitos2024- obcibercncs.pdf

AUTOAVALIAÇÃO: O PRIMEIRO PASSO PARA

As empresas devem encarar o processo de autoavaliação acríticamente, pois o seu objetivo não consiste em distinguir boas empresas de empresas menos boas, mas apenas determinar o patamar de ciberresiliência de uma específica entidade para poder identificar e implementar as medidas que mais facilmente e eficientemente possam incrementar o seu grau de cibersegurança. Não existem entidades imunes a ciberataques, mas apenas entidades conscientes dos seus pontes fortes e das suas fraquezas, assentes num processo constante de reduzir os seus pontos menos fortes.

Uma avaliação inicial de cibersegurança deve incluir uma análise detalhada das infraestruturas tecnológicas, processos internos e nível de consciencialização dos colaboradores. Muitas vezes, as maiores vulnerabilidades não estão na tecnologia, mas sim na falta de conhecimento dos utilizadores que operam os sistemas[31]. Um erro humano, como clicar num link malicioso ou utilizar palavras-passe fracas, pode ser a porta de entrada para um ataque devastador[32]. Por isso, avaliar e reforçar a cultura de cibersegurança dentro da empresa é tão importante quanto investir em tecnologia.

Além disso, a avaliação permite que as PMEs reconheçam quais os ativos mais críticos para o funcionamento do seu negócio, definindo prioridades na implementação de medidas de proteção. Nem todas as ameaças representam o mesmo risco para todas as empresas. Uma PMEs de hotelaria, por exemplo, pode estar mais vulnerável a ataques que comprometem os dados dos clientes, enquanto uma PMEs de comércio eletrónico pode estar mais exposta a fraudes online, e uma PME de comércio alimentar pode ver afetado o fornecimento dos seus alimentos[33].

Compreender as especificidades de cada negócio é crucial para adotar uma abordagem personalizada e eficaz. Este processo de avaliação também é essencial para garantir a conformidade com regulamentos e normativas legais, como o Regulamento Geral sobre a Proteção de Dados (RGPD) e o Regime Jurídico do Ciberespaço (NIS 1 e NIS 2).

Fonte: IStock - Supatman

31 IBM Global Technology Services. (2014). IBM Security Services 2014 Cyber Security Intelligence Index for Financial Services. Disponível em https://bankwatch.ca/wp- content/uploads/2015/01/ibm-cybersecurity-threat-financial-services.pdf

32 Verizon Business. (2024). 2024 Data Breach Investigations Report. Disponível em https://www.verizon.com/business/resources/reports/dbir/

33 Gregory, J. (2025). How cyberattacks on grocery stores could threaten food security. Security Intelligence. Disponível em: https://securityintelligence.com/articles/how- cyberattacks-on-grocery-stores-could-threaten-food-security/

Questionário de Autoavaliação de Cibersegurança

A. Identificação e Gestão de Ativos

- A sua organização tem um inventário atualizado dos ativos tecnológicos (computadores, dispositivos e sistemas) e sabe quais são críticos para a continuidade do negócio?

- Existe um conhecimento claro sobre os dados mais sensíveis (como informações de clientes e dados financeiros) e quem tem acesso a essas informações?

B. Políticas de Segurança e Controlo de Acesso

- A sua organização tem um documento formal que define as políticas de segurança para proteção de dados, sistemas e dispositivos tecnológicos, e este documento é comunicado e seguido por toda a equipa?

- O acesso a sistemas e informações é limitado ao estritamente necessário para cada colaborador? São utilizadas senhas fortes e autenticação multifator para reforçar a segurança?

C. Formação e Consciencialização

- A sua organização promove regularmente ações de formação e sensibilização sobre cibersegurança, incluindo a identificação de ameaças como phishing, engenharia social e fraudes online?

D. Cópias de Segurança e Recuperação

- São realizadas cópias de segurança (backups) dos dados críticos de forma regular, incluindo cópias armazenadas fora das instalações (off-site)? A sua organização testa periodicamente a recuperação desses backups?

- Existe um plano estruturado para a recuperação rápida das operações após um incidente de cibersegurança, como perda de dados ou indisponibilidade dos sistemas?

E. Proteção de Dispositivos e Dados Sensíveis

- Os dispositivos utilizados na organização (como computadores, portáteis e smartphones) estão protegidos contra malware e acessos não autorizados? As atualizações de segurança são aplicadas regularmente?

- Os dados sensíveis (como informações de clientes e contratos) estão devidamente protegidos para evitar acessos não autorizados, mesmo em caso de perda ou roubo de dispositivos?

F. Monitorização e Registo de Atividades

- A sua organização monitoriza e regista acessos a sistemas e dados críticos, garantindo a rastreabilidade das ações realizadas?

G. Gestão de Incidentes e Resiliência

- Existe um plano definido para responder a ciberataques ou falhas de segurança, que inclui procedimentos claros para contenção, mitigação e comunicação do incidente?

- Em caso de incidente de segurança, a sua organização sabe exatamente quem deve ser contactado dentro e fora da empresa, bem como os passos a seguir?

- São analisados incidentes passados ou realizadas simulações para identificar vulnerabilidades e melhorar a resposta a futuras ameaças?

H. Como interpretar os resultados?

- Maioria das respostas "Sim": A organização tem uma postura madura em cibersegurança, mas deve continuar a monitorizar e aperfeiçoar as suas práticas regularmente.

- Maioria das respostas "Parcialmente": Algumas boas práticas já estão implementadas, mas há falhas que devem ser corrigidas para aumentar a resiliência digital.

- Maioria das respostas "Não": A empresa está exposta a riscos significativos e precisa de tomar medidas urgentes para melhorar a segurança dos seus sistemas e dados.

A cibersegurança é um processo contínuo. Em 2024 constatou-se um incremento de um investimento significativo em soluções para segmentação da rede interna, na compartimentação dos acessos relativamente às funções específicas desempenhadas pelos funcionários ou colaboradores e também em programas internos de formação e treino.

No entanto, apesar de esta ser uma tendência positiva, sucede que o incremento da escala das ameaças e da sua sofisticação, exigem o investimento de mais recursos neste domínio para poder manter um nível eficiente de proteção em função do volume de ataques realizados[34].

34 Fortinet. (2024). 2024 State of Operational Technology and Cybersecurity Report. p. 14. Disponível em: https://www.fortinet.com/content/dam/fortinet/assets/reports/report-state-ot-cybersecurity.pdf

5. Implementação
Medidas Preventivas

A cibersegurança é muitas vezes vista como um desafio complexo e dispendioso, levando muitas PMEs a adiar ou negligenciar a implementação de medidas de proteção. No entanto, existem várias ações simples e de baixo custo que podem ser aplicadas de imediato para reduzir significativamente o risco de incidentes em cibersegurança.

Estas medidas, conhecidas como quick wins, são passos essenciais para criar um ambiente digital mais seguro sem necessidade de investimentos elevados em infraestruturas tecnológicas ou equipas especializadas.

1. Atualizar regularmente software e sistemas

A vulnerabilidade causada por software desatualizado é uma das principais portas de entrada para ataques cibernéticos. As PME devem garantir que todos os sistemas operativos, aplicações e dispositivos utilizados na empresa são atualizados automaticamente ou regularmente verificados para aplicar patches de segurança. Esta prática reduz significativamente o risco de exploração de falhas conhecidas.

2. Implementar autenticação multifator (MFA)

A MFA adiciona uma camada extra de proteção aos acessos críticos da empresa, exigindo uma segunda forma de verificação além da palavra-passe. Isto pode ser feito através de um código enviado por SMS, uma app de autenticação ou uma chave de segurança física. Ativar a MFA nos e-mails corporativos, plataformas de gestão e contas de armazenamento na cloud dificulta significativamente acessos não autorizados, um estudo recente da Google revela que o simples fato de associar um número de telefone para recuperar o acesso através do envio de um código por meio de SMS pode bloquear 99% dos ataques massivos de phishing e 76% dos ataques direcionados[35].

Fonte: IStock - marchmeena29

35 Google Security Blog. (2019). New research: How effective is basic account hygiene at preventing hijacking. Google. Disponível em: https://security.googleblog.com/2019/05/new-research-how-effective-is-basic.html

Sensibilizar colaboradores para ameaças como phishing e engenharia social Os ataques de phishing continuam a ser um dos métodos mais eficazes de roubo de credenciais e infecção de sistemas. Uma ação simples e sem custos é a realização de sessões internas ou o envio de materiais explicativos sobre como identificar e evitar e-mails suspeitos, não clicar em links desconhecidos e não fornecer informações sensíveis sem verificar a legitimidade do pedido.

3. Criar e reforçar políticas de palavras-passe

Muitas PME ainda utilizam palavras-passe fracas ou repetidas em diferentes sistemas. Para aumentar a segurança de forma imediata, deve ser exigida a criação de palavras-passe robustas, combinando letras, números e caracteres especiais. Sempre que possível, devem ser utilizados gestores de palavras-passe para armazenar credenciais de forma segura e evitar reutilização.

4. Realizar backups regulares e testá-los

Criar cópias de segurança dos dados críticos da empresa é fundamental para prevenir a perda de informação devido a ataques de ransomware ou falhas técnicas. O ideal é que os backups sejam automáticos, armazenados em locais externos (off- site) ou na cloud, e testados regularmente para garantir que podem ser recuperados em caso de necessidade, a eliminação intencional de dados por hackers ou falhas no sistema, poderiam ser significativamente reduzidos com a utilização de backups offline, evitando entre 50% e 70% da perda de informação[36].

5. Restringir acessos e aplicar o princípio do privilégio mínimo

Nem todos os colaboradores precisam de ter acesso a todas as informações e sistemas da empresa. Implementar o princípio do privilégio mínimo significa que cada funcionário tem apenas acesso ao que é estritamente necessário para desempenhar as suas funções. Isto reduz o risco de exposição de dados sensíveis e de acessos indevidos.

6. Proteger redes Wi-Fi e dispositivos da empresa

A rede Wi-Fi da empresa deve estar protegida por uma palavra-passe forte e um protocolo de segurança atualizado (WPA2/WPA3). Sempre que possível, as empresas devem criar redes separadas para colaboradores e visitantes para evitar acessos indevidos a sistemas internos. Além disso, dispositivos móveis e portáteis devem estar encriptados e protegidos com bloqueios de ecrã para evitar acessos em caso de perda ou roubo.

7. Criar um plano básico de resposta a incidentes

Ainda que simples, um plano de resposta a incidentes pode fazer a diferença na rapidez e eficácia da reação a um ataque cibernético. A empresa deve definir quem deve ser contactado em caso de incidente, como isolar sistemas afetados e quais os passos a seguir para recuperação de dados e comunicação com clientes e fornecedores.

36 Microsoft Learn. (2024). Plano de backup e restauração para proteger contra ransomware. Microsoft. Disponível em: https://learn.microsoft.com/pt- pt/azure/security/fundamentals/backup-plan-to-protect-against-ransomware

8. Monitorizar acessos e atividades suspeitas

Muitas PME não têm visibilidade sobre quem acede a informações críticas ou se há atividades invulgares nos seus sistemas. Ativar alertas de login suspeitos, monitorizar acessos a dados sensíveis e rever registos de atividade são medidas fáceis de implementar que ajudam a detetar ameaças em tempo útil.

9. Desativar contas de ex-colaboradores e rever permissões regularmente

Um erro comum nas PME é manter contas ativas de antigos colaboradores, o que representa um risco significativo caso essas credenciais sejam comprometidas. Sempre que um funcionário sai da empresa, as suas credenciais devem ser imediatamente revogadas ou desativadas, e as permissões de acesso devem ser revistas periodicamente.

Melhorar o nível de cibersegurança da sua empresa, depende mais da sua boa gestão, do que de grandes investimentos ou conhecimentos técnicos.

Assegure-se de implementar as boas práticas, que não acrescem custos à sua atividade, e que fortalecem a sua defesa perante os ataques de que poderá ser alvo!

6. Conformidade
Requisitos legais e normas aplicáveis

A conformidade em cibersegurança refere-se ao cumprimento de normas, regulamentos e leis que garantem a proteção de dados e sistemas contra ameaças digitais. Num cenário de ameaças em constante evolução[37], garantir a conformidade com as legislações nacionais e internacionais tornou-se essencial para as organizações.

Fonte: IStock - Thitima Uthaiburom

Regulamento Geral De Proteção De Dados (RGPD)

O RGPD implementado em 2018, estabeleceu normas rigorosas para a proteção dos dados pessoais dos cidadãos da União Europeia, para assegurar a execução deste regulamento em Portugal foi adotada a Lei 58/2019, de 8 de agosto. O RGPD define direitos dos utilizadores, como o acesso, retificação e apagamento de dados pessoais.

As organizações são obrigadas a implementar medidas adequadas para garantir a segurança dos dados, sendo que as violações ao RGPD podem resultar em multas significativas.

Lei do CiberCrime

Em Portugal a Lei 109/2009 de 15 de setembro desempenha um papel crucial na regulamentação e combate aos crimes informáticos. Esta legislação adapta o ordenamento jurídico nacional à Convenção de Budapeste sobre a Criminalidade, de 2001.

Lei 46/2018, de 13 de agosto (Regime Jurídico de Segurança no Ciberespaço) Estabelece o regime jurídico da segurança do ciberespaço, transpondo a Diretiva (UE) 2016/1148 (NIS 1), do Parlamento Europeu e do Conselho, de 6 de julho de 2016, relativa a medidas destinadas a garantir um elevado nível comum de segurança das redes e da informação em toda a União, sendo regulamentada através do Decreto- Lei 65/2021, de 30 de julho. Sendo que este regime de cibersegurança é um marco, ou um passo que requer das entidades um esforço além dos diplomas anteriores.

37 Fortinet, "State of Operational Technology and Cybersecurity Report," 2024. [Online]. Available: https://www.fortinet.com/content/dam/fortinet/assets/reports/report- state-ot-cybersecurity.pdf. [Acedido em 18 02 2025].

Diretiva NIS2

A Diretiva NIS2, publicada a 27 de dezembro de 2022, reforça a postura de cibersegurança dos Estados-Membros, alargando o seu âmbito e introduzindo novas medidas:

Cerca de 160.000 empresas de 18 setores críticos devem cumprir a NIS2, incluindo entidades essenciais (exemplo: infraestruturas críticas) e entidades importantes (demais organizações que integram setores identificados nos Anexos I e II da diretiva);

- Empresas de média e grande dimensão são automaticamente abrangidas, bem como organizações menores consideradas essenciais pelos Estados-Membros;

Os Estados-Membros deviam transpor a diretiva até 17 de outubro de 2024 e aplicar as disposições a partir de 18 de outubro de 2024, só que em Portugal, assim como em outros países da UE, só agora está em curso o processo de transposição legislativa. E, embora esteja em atraso, é recomendável que as entidades abrangidas comecem desde já a adaptação à NIS2.

ISO/IEC 27001

A ISO/IEC 27001 é um padrão internacional para sistemas de gestão de segurança da informação (SGSI). Seus principais benefícios incluem:

- Identificação e mitigação de riscos de segurança da informação. • Definição de controles para proteção de dados sensíveis.
- Melhoria contínua da postura de segurança organizacional.

ISO/IEC 27002

Complementar à ISO 27001, a ISO/IEC 27002 fornece um conjunto detalhado de práticas recomendadas para implementação dos controles de segurança da informação.

NIST Cybersecurity Framework (CSF)

Desenvolvido pelo National Institute of Standards and Technology (NIST), este framework foca em cinco funções essenciais:

- Identificar: Compreender riscos e ativos críticos;
- Proteger: Implementar salvaguardas para limitar impactos;
- Detectar: Monitorar continuamente atividades suspeitas;
- Responder: Desenvolver planos de resposta a incidentes;
- Recuperar: Restaurar operações e reduzir impactos futuros.

CIS Controls

Os CIS Controls são um conjunto de 20 controles de segurança prioritários que ajudam as organizações a minimizar riscos cibernéticos de forma prática e eficiente.

Framework MITRE ATT&CK

O MITRE ATT&CK é um modelo que documenta táticas, técnicas e procedimentos (TTPs) usados por cibercriminosos, permitindo melhor defesa contra ameaças avançadas.

7. Recursos
Ferramentas Recomendadas

A implementação de boas práticas de cibersegurança não precisa de ser dispendiosa. Existem diversas ferramentas gratuitas e de código aberto que permitem às Pequenas e Médias Empresas (PME) reforçar a proteção dos seus dados, redes e dispositivos sem grandes investimentos. Abaixo, apresentamos uma seleção de recursos essenciais divididos por categorias, incluindo software gratuito e plataformas úteis para gestão e mitigação de riscos cibernéticos.

1. Proteção de Endpoints (Antivírus e Antimalware)

Microsoft Defender – Antivírus nativo do Windows que oferece proteção gratuita contra malware.
https://www.microsoft.com/en-us/windows/comprehensive-security

Malwarebytes Free – Ferramenta especializada na deteção e remoção de malware, spyware e ransomware.
https://www.malwarebytes.com

ClamAV – Antivírus de código aberto para Windows, macOS e Linux, útil para servidores e redes empresariais.
https://www.clamav.net

Avast Free Antivirus – Solução gratuita que protege dispositivos contra vírus e ataques online.
https://www.avast.com

Ferramenta-web do Guia de Transição Digital e Cibersegurança – mapeia riscos nos dispositivos (inclui antivírus e patch-management).
https://www.cncs.gov.pt/pt/guia-de-transicao-digital/

Roteiro para Capacidades Mínimas de Cibersegurança – checklist interactivo que valida se a PME tem anti-malware activo.
https://www.cncs.gov.pt/docs/cncs-roteiro-capacidades-minimas-ciberseguranca.pdf

2. Firewalls e Proteção de Redes

pfSense – Firewall e router open-source com funcionalidades avançadas para proteção de redes empresariais.
https://www.pfsense.org

OPNsense – Alternativa ao pfSense, oferece segurança de rede robusta com monitorização e proteção contra ameaças.
https://opnsense.org

GlassWire – Ferramenta de monitorização de tráfego de rede que ajuda a identificar acessos suspeitos.
https://www.glasswire.com

WebCheck.PT – analisa DNSSEC, SPF, DKIM, DMARC, TLS e HTTPS do domínio.
https://www.cncs.gov.pt/pt/webcheck

3. Gestão de Senhas e Autenticação Multifator

Bitwarden – Gestor de senhas gratuito e de código aberto, permitindo armazenamento seguro de credenciais.

https://bitwarden.com

KeePass – Alternativa gratuita para armazenar senhas localmente com encriptação forte.

https://keepass.info

Authy – Aplicação gratuita para autenticação multifator (MFA) que reforça a segurança no acesso a contas.

https://authy.com

Google Authenticator – Aplicação simples e eficaz para geração de códigos MFA.

https://play.google.com/store/apps/details?id=com.google.android.apps.authenticator2

Guia para a Seleção de Soluções de Autenticação Multifator (PDF + matriz de avaliação de fornecedores).

https://www.cncs.gov.pt/docs/guia-mfa.pdf

Ficha prática Ciber-Higiene e Boas Práticas (secção passwords).

https://www.cncs.gov.pt/docs/2ciberhig.pdf

4. Análise de Segurança e Testes de Vulnerabilidades

OpenVAS – Scanner gratuito para identificar vulnerabilidades em redes e servidores.

https://www.greenbone.net/en/openvas

Nikto – Scanner para servidores web que identifica falhas de configuração e vulnerabilidades.

https://cirt.net/nikto2

Metasploit Framework – Ferramenta avançada de testes de penetração para avaliar a segurança de sistemas.

https://www.metasploit.com

Have I Been Pwned? – Serviço online que permite verificar se credenciais da empresa já foram comprometidas.

https://haveibeenpwned.com

Shodan – Motor de busca que identifica dispositivos ligados à internet e potenciais vulnerabilidades.

https://www.shodan.io

CiberCheckup – questionário online que devolve relatório de maturidade e lista de vulnerabilidades a corrigir.

https://www.cncs.gov.pt/pt/ferramentas

5. Monitorização e Deteção de Intrusões (IDS/IPS)

Snort – Sistema de deteção de intrusões (IDS) open-source para monitorizar tráfego de rede.

https://www.snort.org

Suricata – Ferramenta IDS/IPS que analisa pacotes de rede em tempo real para detetar ataques.

https://suricata.io

Zeek (ex-Bro) – Plataforma de análise de tráfego de rede focada na deteção de anomalias.

https://zeek.org

Observatório de Cibersegurança – dashboards interactivos com estatísticas de incidentes em Portugal; permite fazer benchmark ao sector.
https://www.cncs.gov.pt/pt/observatorio

6. Cópias de Segurança (Backup & Recovery)

Veeam Backup Free – Solução gratuita para cópias de segurança de servidores e ambientes virtuais.
https://www.veeam.com/free-backup.html
Duplicati – Software open-source para backups encriptados em cloud ou armazenamento local.
https://www.duplicati.com
AOMEI Backupper – Ferramenta gratuita para criar imagens de backup e restaurar sistemas.
https://www.aomeitech.com
Guia para Gestão dos Riscos em Segurança da Informação – capítulo "Recuperação" com plano de backup 3-2-1.
https://www.cncs.gov.pt/pt/gestao-de-risco/

7. Ferramentas de Educação e Formação em Cibersegurança

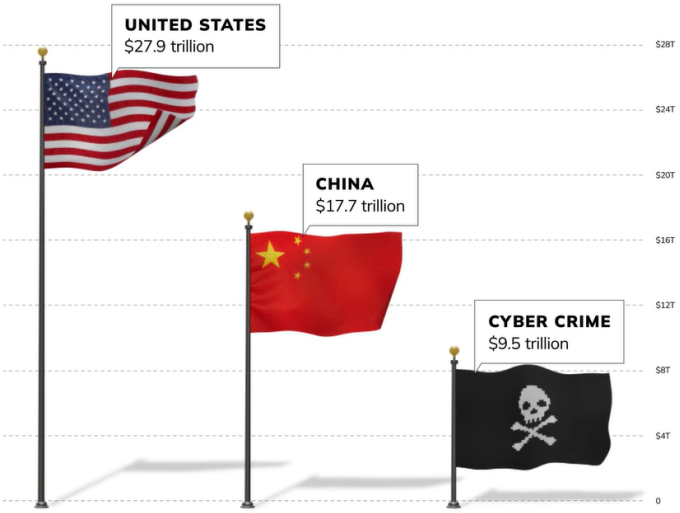
Cybrary – Plataforma gratuita de cursos sobre cibersegurança e boas práticas para empresas.
https://www.cybrary.it
Cisco Networking Academy – Formação gratuita sobre redes, segurança e administração de sistemas.
https://www.netacad.com
MITRE ATT&CK – Base de conhecimento sobre técnicas e táticas utilizadas por atacantes.
https://attack.mitre.org
Google Phishing Quiz – Teste interativo gratuito para treinar colaboradores a identificar tentativas de phishing.
https://phishingquiz.withgoogle.com
C-Academy – plataforma de cursos avançados PRR (online/híbrido).
https://www.cncs.gov.pt/pt/c-academy
Cursos e-learning curtos (Cidadão Ciberseguro, Consumidor Ciberseguro, etc.)
https://www.cncs.gov.pt/pt/cursos-e-learning

Com o crescimento das ameaças cibernéticas, as PME precisam de adotar ferramentas eficazes para proteger os seus dados, redes e sistemas. Felizmente, existem soluções gratuitas e de código aberto que oferecem uma excelente camada de defesa sem necessidade de grandes investimentos. Desde a implementação de antivírus, firewalls e encriptação, até à monitorização de acessos e realização de backups, estas ferramentas fazem uma grande diferença na resiliência digital da organização.

Ao integrar estas soluções no dia a dia da empresa, as PME irá fortalecer a sua postura de segurança, reduzir vulnerabilidades e garantir um ambiente digital mais seguro para os seus negócios e clientes.

TENHA PRESENTE!

A INDÚSTRIA DO CIBERCRIME,
SE FOSSE UMA ECONOMIA
REPRESENTARIA A
3ª MAIOR ECONOMIA!



Fonte: *Bloomerang*, "The World's Third-Largest Economy Has Bad Intentions — and It's Only Getting Bigger", in https://sponsored.bloomberg.com/quicksight/check-point/the-worlds-third-largest-economy-has-bad-intentions-and-its-only-getting-bigger

O tecido das PME, representa 99% das empresas da UE, o que as torna o principal alvo dos cibercriminosos[38].

38 *European Comission*, Entrepreneurship and small and medium-sized enterprises (SMEs). https://single-market-economy.ec.europa.eu/smes_en

8. Conclusão
Ferramentas Recomendadas

Na era digital, a cibersegurança não é apenas uma questão tecnológica – é um fator essencial para a proteção das pessoas que fazem parte de uma organização e da confiança dos seus clientes e parceiros. As PMEs dependem cada vez mais dos meios digitais para operar, comunicar e inovar, mas essa transformação também traz riscos que podem comprometer a privacidade dos dados, a continuidade dos negócios e a credibilidade da marca como uma responsabilidade partilhada por todos dentro da organização.

A proteção contra ameaças não depende apenas de ferramentas tecnológicas avançadas, mas, sobretudo, uma formação contínua e a promoção de boas práticas são fundamentais para que cada membro da empresa compreenda o seu papel na prevenção de incidentes.

A liderança também tem um papel crucial, ao incentivar hábitos seguros, fornecer recursos adequados e demonstrar que a segurança digital é uma prioridade estratégica e não apenas uma obrigação regulatória.

Afinal, a cibersegurança começa nas pessoas.

Fonte: IStock - Natthaphon Wanason

Aquele que se antecipa ao perigo transforma a incerteza em força e a ameaça em uma oportunidade de crescer.

Sun Tzu

LISTA DE INFORMAÇÃO COMPLEMENTAR

Para complementar este guia e fornecer recursos práticos às Pequenas e Médias Empresas (PME), apresentamos uma lista de recursos que podem ajudar na implementação de medidas de cibersegurança. Estes documentos oferecem diretrizes, modelos e informações essenciais para reforçar a resiliência digital da organização.

1 – Glossário de Termos Essenciais em Cibersegurança e TI (pp. 35-43)

Descrição dos principais conceitos e terminologias utilizadas em cibersegurança, facilitando a compreensão dos temas abordados no guia.

2 – Checklist de Boas Práticas de Cibersegurança para PME

- CNCS Ciber-Higiene e Boas Práticas (PDF) - https://www.cncs.gov.pt/docs/2ciberhig.pdf
- NCSC Small-Business Guide – Actions (PDF) - https://www.ncsc.gov.uk/files/NCSC_SBG_Actions.pdf

3 – Guia de Criação de Senhas Seguras & MFA

- CNCS Guia MFA (PDF) - https://www.cncs.gov.pt/docs/guia-mfa.pdf
- NCSC Infográfico Using Passwords to Protect Your Devices & Data (PDF) - https://www.ncsc.gov.uk/files/NCSC-using-passwords-infographic.pdf

4 – Plano de Resposta a Incidentes

- NIST SP 800-61 Rev. 3 (PDF) - https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-61r3.pdf
- ENISA Good Practice Guide for Incident Management (PDF) - https://enisa.europa.eu/sites/default/files/publications/Incident_Management_guide.pdf

5 – Plano de Backups e Recuperação de Dados

- Microsoft Learn Backup & Restore Plan to Protect Against Ransomware - https://learn.microsoft.com/en-us/azure/security/fundamentals/backup-plan-to-protect-against-ransomware
- ENISA Cyber Hygiene – Backup Best Practices - https://www.enisa.europa.eu/topics/cyber-hygiene

6 – Política de Segurança da Informação

- SANS Security Policy Templates - https://www.sans.org/information-security-policy/
- CIS Critical Security Controls v8 - https://www.cisecurity.org/controls/v8

7 – Contactos de Emergência e Autoridades Competentes

- CERT.PT – contactos oficiais - https://www.cncs.gov.pt/pt/certpt
- ENISA CSIRTs by Country – Interactive Map https://www.enisa.europa.eu/tools/csirts-by-country-interactive-map

1. Glossário - Termos de Cibersegurança e TI

A

Ameaça – Causa potencial de incidente indesejável que pode resultar em danos para uma organização ou qualquer dos sistemas por ela utilizados. Estas ameaças podem ser acidentais ou deliberadas (com dolo) e caracterizam-se por elementos ameaçadores, alvos potenciais e métodos de ataque;

Ataque DDoS – Os ataques DDoS (Distributed Denial of Service) tem como objetivo causar disrupções no funcionamento de um servidor, serviço ou rede. Para tal é utilizada uma rede de computadores comprometidos (botnet) para sobrecarregar os alvos com um elevado número de pedidos, ultrapassando os seus limites de tráfego;

Antivírus – São programas informáticos responsáveis pela deteção de malware ou software potencialmente nocivo;

Ataque – Qualquer tipo de atividade maliciosa que tenta recolher, perturbar, negar, degradar ou destruir recursos de sistema de informação ou a informação em si;

Autenticação de Dois Fatores (2FA) – A autenticação de dois fatores é uma camada extra de segurança usada para garantir que as pessoas tentando ganhar acesso a uma conta online sejam quem dizem ser. Primeiro, o usuário insere sua senha. Em seguida, em vez de obter acesso imediatamente, ele é solicitado a fornecer outra informação, como um código enviado para seu telemóvel;

Autenticação de Identidade – Verificação ou validação da identidade de uma pessoa ou da identificação de qualquer outra entidade através de um sistema de segurança;

Autenticidade – Num contexto informacional, propriedade de uma informação cuja origem e integridade são garantidas;

B

Backup – É um processo, técnica ou equipamento usado para ajudar a recuperar dados perdidos ou destruídos ou para manter um sistema em funcionamento. No contexto do software usado para realizar a salvaguarda de ficheiros (software de salvaguarda), obtemos as chamadas “cópias de segurança” (backup copies); No contexto de equipamentos, temos, por exemplo, “fontes de alimentação de reserva” (backup power supplies) ou mesmo “discos de reserva” (backup disks);

Botnet – Uma botnet é uma rede de computadores infetados por software malicioso, sendo controlada remotamente por cibercriminosos. Estas redes podem depois ser utilizadas para uma variedade de ações, entre levar a cabo campanhas de spam em larga escala, executar ataques DDoS ou disseminar malwares;

Browser – Um browser é um software que é utilizado para aceder à Internet. Os navegadores web mais populares são o Google Chrome, Firefox, Safari, Internet Explorer, e o Microsoft Edge;

Buffer Overflow – Também conhecido como estouro de buffer (região de memória física utilizada para armazenar temporariamente os dados enquanto eles estão sendo movidos de um lugar para outro), ocorre quando a quantidade de dados no buffer excede sua capacidade de armazenamento. Esses dados extras transbordam para locais de memória adjacentes e corrompem ou copiam os dados nesses locais;

C

Cavalo de Tróia (ou Trojan) – é um tipo de malware que se disfarça de software legítimo. Ele engana os usuários para que o instalem em seus dispositivos, permitindo que os cibercriminosos tenham acesso não-autorizado aos sistemas e dados;

Ciber – Termo que se relaciona com as tecnologias da informação;

Ciberataque – Ataque realizado através das tecnologias de informação no ciberespaço dirigido contra um ou vários sistemas, com o objetivo de prejudicar a segurança das tecnologias de informação e da comunicação (confidencialidade, integridade e disponibilidade), em parte ou totalmente;

Ciberdefesa – O termo "ciberdefesa" refere-se a todas as medidas utilizadas para defender o espaço cibernético com os meios militares e outros apropriados para alcançar objetivos estratégico militares. A ciberdefesa é um sistema integrado, que compreende a implementação de todas as medidas relacionadas com as TIC e a segurança da informação, os recursos, equipas de resposta a incidentes no ciberespaço (milCERT) e operações de rede do computador (CNO), bem como o apoio dos recursos físicos do exército;

Cookie – Pacote de informação enviado de um servidor Web para um programa de navegação, e depois reenviado sempre que este aceda ao servidor;

Correio Eletrónico – Qualquer mensagem textual, vocal, sonora ou gráfica enviada através de uma rede pública de comunicações que possa ser armazenada na rede ou no equipamento terminal do destinatário até que este a recolha;

Crime Informático – Atos criminosos cometidos on-line utilizando redes de comunicação eletrónicas e sistemas de informação;

Criptografia – é o processo de codificar informações para que apenas as pessoas autorizadas possam acessá-las. Ela é usada para proteger dados sensíveis, tanto em trânsito quanto em repouso, garantindo que, mesmo que os dados sejam intercetados, eles não possam ser lidos sem a chave de decriptação correta.

Cross-site Scripting (XSS) – Um ataque de cross-site scripting ocorre quando os criminosos cibernéticos injetam scripts maliciosos no conteúdo do site alvo, que é então incluído com o conteúdo dinâmico entregue ao navegador da vítima. O navegador da vítima não tem como saber que os scripts maliciosos não são confiáveis e, portanto, os executa. O XSS difere de outros ataques da Web porque não tem como alvo direto a própria aplicação. Em vez disso, os usuários da aplicação Web são os que correm risco.

Cryptojacking – Neste tipo de ameaça os cibercriminosos recorrem a um software malicioso para obter o controlo dos equipamentos das vítimas, utilizando-os para minerar criptomoedas sem que estas se apercebam;

D

Dados de Tráfego – São os dados informáticos relacionados com uma comunicação efetuada por meio de um sistema informático, gerados por este sistema como elemento de uma cadeia de comunicação, indicando várias informações, tais como a origem da comunicação, o destino, o trajeto, a hora, a data, o tamanho, a duração ou o tipo do serviço subjacente;

Dados Informáticos – É qualquer representação de factos, informações ou conceitos sob uma forma suscetível de processamento num sistema informático, incluindo os programas aptos a fazerem um sistema informático executar uma função;

Dados Pessoais – É qualquer informação, de qualquer natureza e independentemente do respetivo suporte, incluindo som e imagem, relativa a uma pessoa singular identificada ou identificável ('titular dos dados'); é considerada identificável a pessoa que possa ser identificada direta ou indiretamente, designadamente por referência a um número de identificação ou a um ou mais elementos específicos da sua identidade física, fisiológica, psíquica, económica, cultural ou social. Os dados pessoais são dados relativos a uma pessoa física e devem ser reservados à pessoa a que correspondem. Estes dados, que incluem informação como identidade, estado civil, situação profissional, financeira, médica, jurídica, etc., permitem a identificação direta ou indireta da pessoa em causa e desse modo comprometer a sua segurança ou legitimidade;

Dark Web – É a camada profunda da Internet que, além de não ser indexada por motores de busca, não consegue ser acedida através de meios mais "convencionais", requerendo um tipo de browser específico, com o Tor a destacar-se como uma das opções mais populares. É composta por um conjunto de redes restritas (darknets). A dark web é conhecida maioritariamente por servir como plataforma para atividades ilegais, no entanto, também pode ser utilizada para outros propósitos. Esta camada da Internet é utilizada por pessoas que vivem em países onde a liberdade de expressão é limitada, de modo a poderem aceder

a informação que não é controlada por entidades estatais, assim como por whistleblowers, dissidentes políticos e ativistas perseguidos por sistemas de governo mais autoritários.

Deep Web – É um "local" que visita com mais frequência do que possa pensar. Dela constam websites e serviços que não são indexados por motores de busca, em muitos dos casos, por motivos de segurança, com conteúdos protegidos por passwords. Nesta camada incluem-se, por exemplo, contas em serviços de email e mensagens ou serviços de bancos, bases de dados e redes internas de comunicações de empresas, organizações ou instituições.

E

Endereço IP (Internet Protocol address) – Endereço de 32 bits de um computador ou outro dispositivo ligado à Internet, representado habitualmente por uma notação decimal de quatro grupos de algarismos separados por pontos;

Endereço URL (Uniform Resource Locator) – Endereço pelo qual documentos e outros recursos são conhecidos e acedidos na Internet com a ajuda de um programa de navegação. Integra carateres identificadores do protocolo, do domínio e do caminho para atingir o recurso e apresenta-se com a seguinte estrutura: id. do protocolo://nome do domínio/nome do caminho/nome do recurso;

Engenharia Social – Técnicas utilizadas para obter informações importantes ou sigilosas através de ações que enganam ou exploram a confiança das pessoas;

Ethernet – Arquitetura muito utilizada para conexão física de redes locais, desenvolvida pela Xerox. Uma rede Ethernet usa uma topologia em barramento (sistema de comunicação que transfere dados entre componentes dentro de um computador, ou entre computadores) ou em estrela e suporta um tráfego de alto débito;

F

Firewall – Em tecnologias da informação e da comunicação, é o sistema informático concebido para proteger uma rede de computadores do acesso externo de utilizadores não autorizados;

G

Gestor de palavras-passe – É uma aplicação dedicada ao armazenamento de palavras-passe numa base de dados encriptada, que está protegida por uma palavra-passe mestre. Os gestores geram frequentemente palavras-passe fortes, suficientemente longas e combinando letras, números e caracteres

estranhos para criar palavras sem sentido, aumentando assim a sua força, ou seja, evitando os ataques e a utilização de padrões previsíveis;

H

Hardware – Totalidade ou parte dos componentes físicos de um sistema de processamento de dados;

Hiperligação – Referência de algum ponto de um hipertexto para um ponto do mesmo ou de outro documento; uma tal referência é normalmente especificada de uma forma diferenciada do resto do hipertexto (por exemplo, usando palavras sublinhadas).

HTML – Linguagem de marcação de hipertexto que possibilita a preparação de documentos com gráficos e hiperligações, para visualização na World Wide Web (WWW) ou em sistemas compatíveis;

I

Injeção de SQL (ou SQLi) – É um tipo de vulnerabilidade em que um invasor usa uma parte do código SQL (Structured Query Language) para manipular um banco de dados e obter acesso a informações potencialmente valiosas. Esse é um dos tipos de ataque mais comuns e perigosos porque pode ser usado contra qualquer aplicação de Web ou site que utilize um banco de dados SQL - ou seja, a maioria deles;

Inteligência Artificial – A inteligência artificial (IA) refere-se à simulação da inteligência humana em máquinas que são programadas para pensar como os humanos e imitar as suas ações;

Internet – Rede de área alargada que é uma confederação de redes de computadores das universidades e de centros de pesquisa, do Governo, do comércio e da indústria, com base no protocolo TCP/IP. Proporciona acesso a sítios Web, correio eletrónico, bases de dados, fóruns de discussão, etc…

Intranet – Rede corporativa baseada no protocolo TCP/IP e acessível apenas aos membros ou colaboradores de uma organização, ou a outros desde que autorizados;

L

LAN – Rede de área local onde a transmissão de sinais é efetuada sem recorrer a fios ou a cabos como, por exemplo, através da utilização de ondas rádio;

M

Malvertising – É a utilização de publicidade online para transferir malwares;

Malware – É a definição para todo software malicioso, ou seja, programas indesejados que causam riscos para computadores, telemóveis e redes. Entre os exemplos mais comuns estão os vírus e os ransomware, que podem causar danos significativos se não forem devidamente controlados;

Man-in-the-Middle (MITM) – É um ataque cibernético em que o invasor transmite secretamente e, possivelmente, altera as comunicações entre duas partes que acreditam estar a comunicar-se diretamente uma com a outra, mas não, pois o invasor se inseriu entre as duas partes. Como resultado, os scripts maliciosos podem acessar quaisquer cookies, tokens de sessão ou outras informações confidenciais retidas pelo navegador e usadas nesse site. Os invasores também podem usar Cross-site Scripting (XSS) para espalhar malware, reescrever o conteúdo de sites, causar problemas em redes sociais e phishing para credenciais de usuário;

Masquerade Attack – É um ataque cibernético em que um atacante se faz passar por um utilizador ou dispositivo legítimo para obter acesso não-autorizado a uma rede ou sistema. Os ataques deste tipo podem ser utilizados para contornar controlos de segurança, como firewalls e controlos de acesso, e para roubar informações sensíveis ou lançar outros ataques a partir da rede comprometida;

N

Norma – Em engenharia de software, requisitos obrigatórios utilizados e impostos para atingir uma abordagem disciplinada e uniforme no desenvolvimento de software.

P

Packet sniffer – É uma captura de pacotes, ou seja, o processo de intercetação e registro de tráfego. Como fluxos de dados trafegam por meio de uma rede, o sniffer captura cada pacote e, se necessário, decodifica os dados brutos do pacote, mostrando os valores de vários campos no pacote, e analisa seus conteúdos de acordo com a RFC ou outras especificações apropriadas. O sniffing pode ser utilizado tanto para propósitos maliciosos como também para a gestão de rede, monitorização e diagnóstico de ambientes computacionais. Em relação aos propósitos malaciosos, os invasores podem tentar capturar o tráfego da rede com diversos objetivos, dentre os quais podem ser citados, obter cópias de arquivos importantes durante sua transmissão, e obter senhas que permitam estender o seu raio de penetração em um ambiente invadido ou ver as conversações em tempo real;

Phishing – É o envio aos internautas de mensagens de correio eletrónico, com a aparência de terem origem em organizações financeiras credíveis, mas com ligações para falsos sítios Web que replicam os originais, e nos quais são feitos pedidos de atualização de dados privados dos clientes;

Pirata Informático (Hacker) – Pessoa que explora as falhas da segurança de um sistema com o intuito de violar a sua integridade, destruindo ou alterando a informação que ali reside, ou de copiar fraudulentamente os seus ficheiros;

Política de Privacidade – Conjunto das medidas administrativas, técnicas e físicas destinadas a impedir as intrusões na vida privada das pessoas ou nos negócios privados das organizações;

Privacidade de Dados – Característica de segurança de um sistema de informação que permite definir quais os dados que podem, ou não, ser acedidos por terceiros;

Proteção de Dados Pessoais – Implementação de medidas para proteger dados pessoais e sensíveis de acessos públicos não-autorizados, e para controlar o fluxo desses dados;

Protocolo – Em tecnologias da informação e da comunicação é o conjunto das convenções e regras que devem ser seguidas no intercâmbio de dados entre computadores;

R

Ransomware – É um software malicioso usado para extorsão por meio de sequestro de dados digitais usando a criptografia; é um crime-cibernético que usa como refém arquivos computacionais pessoais da própria vítima, cobrando assim um resgate para restabelecer o acesso a estes arquivos;

Rede – É o conjunto formado por entidades e as suas interconexões. Em topologia de rede ou numa estrutura abstrata, as entidades interconectadas são pontos e as interconexões são linhas num esquema; numa rede de computadores, as entidades interconectadas são computadores ou equipamentos de comunicação de dados e as interconexões são ligações de dados;

Rede Privada Virtual (VPN) – Rede virtual de comunicação privada que utiliza uma infraestrutura pública de telecomunicações para transmitir dados que são protegidos devido à utilização de técnicas de cifragem ou de encapsulação;

Risco de Segurança – A probabilidade de as vulnerabilidades inerentes a sistemas de comunicação e informação serem exploradas por ameaças, podendo pôr em perigo os sistemas;

S

Segurança da Informação – Proteção dos sistemas de informação contra o acesso ou a modificação não autorizada da informação, durante o seu armazenamento, processamento ou transmissão, e contra a negação de serviço a utilizadores autorizados ou o fornecimento de serviço a utilizadores não-autorizados, incluindo as medidas necessárias para detetar, documentar e contrariar tais ameaças;

Segurança de Redes – Conjunto de regras que devem ser respeitadas no acesso a redes de comunicação, na navegação na Web, no uso de palavras-passe e de chaves criptográficas, e nos ficheiros anexados a mensagens de correio eletrónico. Habitualmente são integradas num documento que expõe a arquitetura do ambiente de segurança da empresa;

Servidor – Programa informático que recebe e satisfaz pedidos de outros programas (programas clientes), no mesmo ou noutros computadores;

Software – Totalidade ou parte dos programas, dos procedimentos, das regras e da documentação associada, pertencentes a um sistema de processamento de informação;

SPAM – Mensagens de correio eletrónico não solicitadas, geralmente enviadas de uma forma massiva e indiscriminada, que, para além do incómodo provocado aos usuários, podem comprometer o bom funcionamento dos sistemas informáticos;

Spoofing – Através desta tática, cibercriminosos imitam uma entidade legítima de modo a ganhar acesso não autorizado a um sistema. Pode ser utilizada de múltiplas formas, entre spoofing de endereços IP, de DNS, websites, emails, ou de números de telefone;

T

Tecnologias de Informação e de Comunicação (TIC) – Integração de métodos, processos de produção, hardware e software, com o objetivo de proporcionar a recolha, o processamento, a disseminação, a visualização e a utilização de informação, no interesse dos seus utilizadores;

Tratamento de Dados Pessoais – Qualquer operação ou conjunto de operações sobre dados pessoais, efetuadas com ou sem meios automatizados, tais como a recolha, o registo, a organização, a conservação, a adaptação ou alteração, a recuperação, a consulta, a utilização, a comunicação por transmissão, por difusão ou por qualquer outra forma de colocar à disposição, com comparação ou interconexão, bem como o bloqueio, eliminação ou destruição;

V

Vírus – Classe de software malicioso que tem a capacidade de se auto-replicar e "infetar" partes do sistema operativo ou de outros programas, com o intuito de causar a perda ou alteração da informação;

Vulnerabilidade – Insuficiência, seja de que natureza for, que possa ser explorada por uma ou mais ameaças. A vulnerabilidade pode consistir numa omissão ou estar relacionada com uma insuficiência dos controlos no que se refere ao rigor, coerência ou exaustividade destes últimos, podendo ser de natureza técnica, processual, material, organizativa ou operacional;

W

WI-FI – Abreviatura de «wireless fidelity», termo usado para designar determinados tipos de redes locais sem fios.

Wi-Fi Security (Segurança Wi-Fi) - Práticas e medidas destinadas a proteger redes sem fios contra acessos não autorizados e ataques cibernéticos, incluindo encriptação WPA3, autenticação multifator e segmentação de redes.

White Hat Hacker - Termo usado para descrever hackers éticos que utilizam os seus conhecimentos para testar e reforçar a segurança de sistemas de informação.

Worm (Verme Informático) - Tipo de malware autorreplicante que se propaga automaticamente através de redes, explorando vulnerabilidades para comprometer dispositivos e sistemas.

Web Application Firewall (WAF) - Firewall específica para aplicações web, que protege contra ataques como SQL injection e cross-site scripting (XSS), bloqueando tráfego malicioso.

Whaling (Ataque do Tipo "Caça à Baleia") - Variante avançada de phishing que visa altos executivos ou pessoas com elevado acesso a dados críticos de uma empresa, utilizando engenharia social sofisticada.

Wireless Intrusion Detection System (WIDS) - Sistema de deteção de intrusões em redes sem fios, que monitoriza e analisa o tráfego para identificar e mitigar ameaças.

Weak Password (Senha Fraca) - Senha considerada vulnerável devido à sua simplicidade ou previsibilidade, tornando-se um alvo fácil para ataques de força bruta.

Web Scraping (Extração de Dados da Web) - Técnica utilizada para recolher informações de websites de forma automatizada, podendo ser usada tanto para fins legítimos quanto para atividades maliciosas.


UAL
AUTÓNOMA
network
ccclisboa
e vale do tejo
PRR
Plano de Recuperação e Resiliência
REPÚBLICA PORTUGUESA
Financiado pela União Europeia
NextGenerationEU