O Setup de Cibersegurança para PMEs

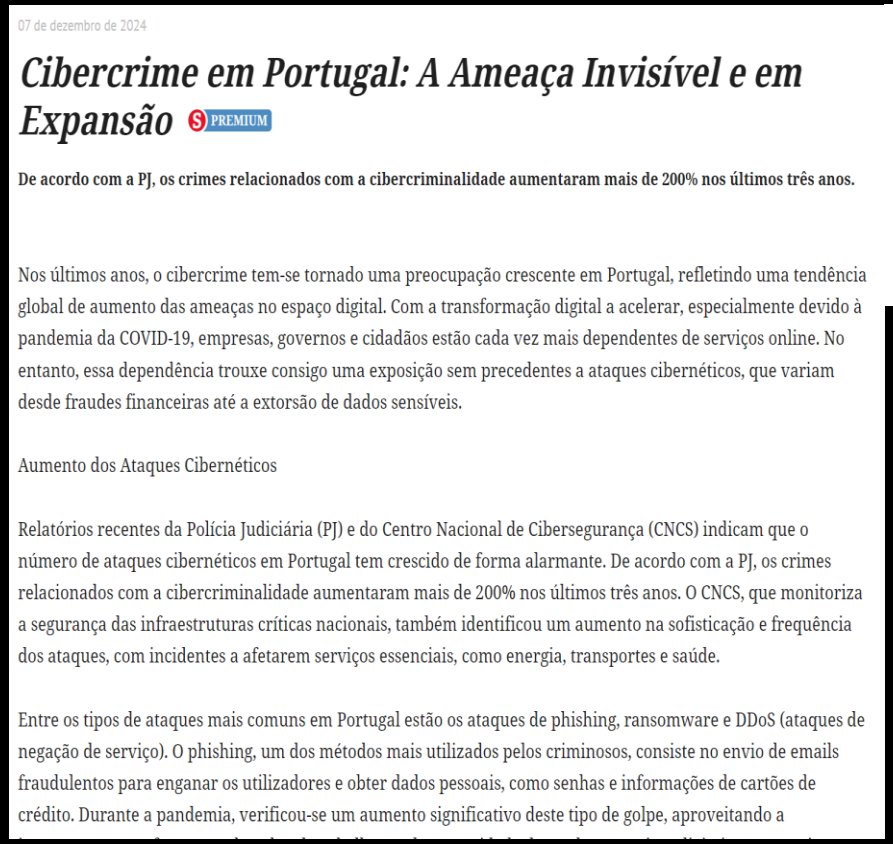
Versão: 1.0

Data: Maio 2025

Cibersegurança como prioridade nas organizações

O que é a Cibersegurança?

A proteção de sistemas, redes e dados contra acessos não autorizados, ataques digitais e interrupções, garantindo a confidencialidade, integridade e disponibilidade da informação.



07 de dezembro de 2024

Cibercrime em Portugal: A Ameaça Invisível e em Expansão PREMIUM

De acordo com a PJ, os crimes relacionados com a cibercriminalidade aumentaram mais de 200% nos últimos três anos.

Nos últimos anos, o cibercrime tem-se tornado uma preocupação crescente em Portugal, refletindo uma tendência global de aumento das ameaças no espaço digital. Com a transformação digital a acelerar, especialmente devido à pandemia da COVID-19, empresas, governos e cidadãos estão cada vez mais dependentes de serviços online. No entanto, essa dependência trouxe consigo uma exposição sem precedentes a ataques cibernéticos, que variam desde fraudes financeiras até a extorsão de dados sensíveis.

Aumento dos Ataques Cibernéticos

Relatórios recentes da Polícia Judiciária (PJ) e do Centro Nacional de Cibersegurança (CNCS) indicam que o número de ataques cibernéticos em Portugal tem crescido de forma alarmante. De acordo com a PJ, os crimes relacionados com a cibercriminalidade aumentaram mais de 200% nos últimos três anos. O CNCS, que monitoriza a segurança das infraestruturas críticas nacionais, também identificou um aumento na sofisticação e frequência dos ataques, com incidentes a afetarem serviços essenciais, como energia, transportes e saúde.

Entre os tipos de ataques mais comuns em Portugal estão os ataques de phishing, ransomware e DDoS (ataques de negação de serviço). O phishing, um dos métodos mais utilizados pelos criminosos, consiste no envio de emails fraudulentos para enganar os utilizadores e obter dados pessoais, como senhas e informações de cartões de crédito. Durante a pandemia, verificou-se um aumento significativo deste tipo de golpe, aproveitando a

Cibercrime em Portugal: A Ameaça Invisível e em Expansão - Pedro Ledo - SÁBADO

De acordo com a PJ, os crimes cibernéticos aumentaram mais de **200%** nos **últimos 3 anos**.

Dados da **ENISA** (Agência da União Europeia para a Cibersegurança), referem que **41%** das **PME** afirmam ter sido vítimas de um **ataque de phishing***.

* Phishing - técnica usada por criminosos na internet para enganar as pessoas, fazendo-as acreditar que estão a falar com uma entidade ou pessoa confiável, como um banco ou uma empresa. O objetivo é roubar informações pessoais, como senhas e números de cartão, através de e-mails ou mensagens falsas que parecem legítimas.

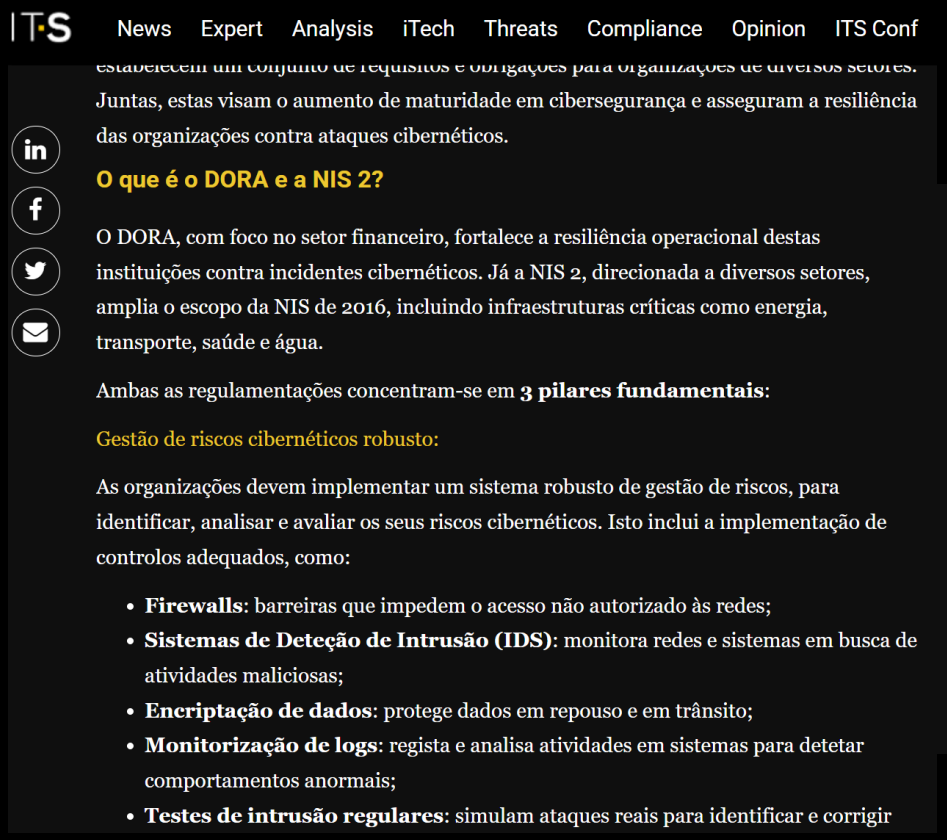
Exemplo de ataque digital

Um colaborador recebe um e-mail falso que parece ser do banco da empresa, solicitando que atualize suas credenciais. Ao clicar no link, foi-lhe roubado o nome de utilizador e a senha, permitindo o acesso não autorizado aos sistemas internos da empresa.

Normas e Diretivas para a Cibersegurança

A União Europeia considera o risco dos ataques cibernéticos significativo, estabelecendo requisitos obrigatórios nas novas legislações DORA (Regulamento) e NIS 2 (Diretiva).

Compliance



ITS News Expert Analysis iTech Threats Compliance Opinion ITS Conf

estabelecem um conjunto de requisitos e obrigações para organizações de diversos setores. Juntas, estas visam o aumento de maturidade em cibersegurança e asseguram a resiliência das organizações contra ataques cibernéticos.

O que é o DORA e a NIS 2?

O DORA, com foco no setor financeiro, fortalece a resiliência operacional destas instituições contra incidentes cibernéticos. Já a NIS 2, direcionada a diversos setores, amplia o escopo da NIS de 2016, incluindo infraestruturas críticas como energia, transporte, saúde e água.

Ambas as regulamentações concentram-se em **3 pilares fundamentais**:

Gestão de riscos cibernéticos robusto:

As organizações devem implementar um sistema robusto de gestão de riscos, para identificar, analisar e avaliar os seus riscos cibernéticos. Isto inclui a implementação de controlos adequados, como:

- **Firewalls**: barreiras que impedem o acesso não autorizado às redes;
- **Sistemas de Deteção de Intrusão (IDS)**: monitora redes e sistemas em busca de atividades maliciosas;
- **Encriptação de dados**: protege dados em repouso e em trânsito;
- **Monitorização de logs**: regista e analisa atividades em sistemas para detetar comportamentos anormais;
- **Testes de intrusão regulares**: simulam ataques reais para identificar e corrigir

https://www.itsecurity.pt/news/slabs/o-dora-e-a-nis2-as-novas-regras-do-jogo-para-a-europa

DORA
Digital Operational Resilience Act

Regulamento que surge na perspetiva de uma harmonização e uniformização das regras mínimas relativas à **segurança das redes e sistemas de informação** atualmente em vigor ao nível da **União Europeia**.

NIS 2
Network and Information Systems Directive

Diretiva relativa a medidas destinadas a garantir um elevado nível comum de cibersegurança na União Europeia

Normas e Diretivas para a Cibersegurança

A União Europeia considera o risco dos ataques cibernéticos significativo, estabelecendo requisitos obrigatórios nas novas legislações DORA (Regulamento) e NIS 2 (Diretiva).

DORA
Digital Operational Resilience Act

Artigo 38 - Penalidades e Medidas Corretivas

Define as penalidades e medidas corretivas que podem ser aplicadas aos prestadores de serviços de TIC em caso de não conformidade com o regulamento.

NIS 2
Network and Information Systems Directive

Artigo 21

d) Segurança da cadeia de abastecimento, incluindo aspetos de segurança respeitantes às relações entre cada entidade e os respetivos fornecedores ou prestadores de serviços diretos;

Considerando 85 – (…) incentivadas a incorporar medidas de gestão dos riscos de cibersegurança nos **acordos contratuais** com os seus fornecedores e prestadores de serviços diretos. (podem considerar os riscos decorrentes de **outros níveis de fornecedores**)

Artigo 25 - Obrigações dos órgãos de gestão, direção e administração

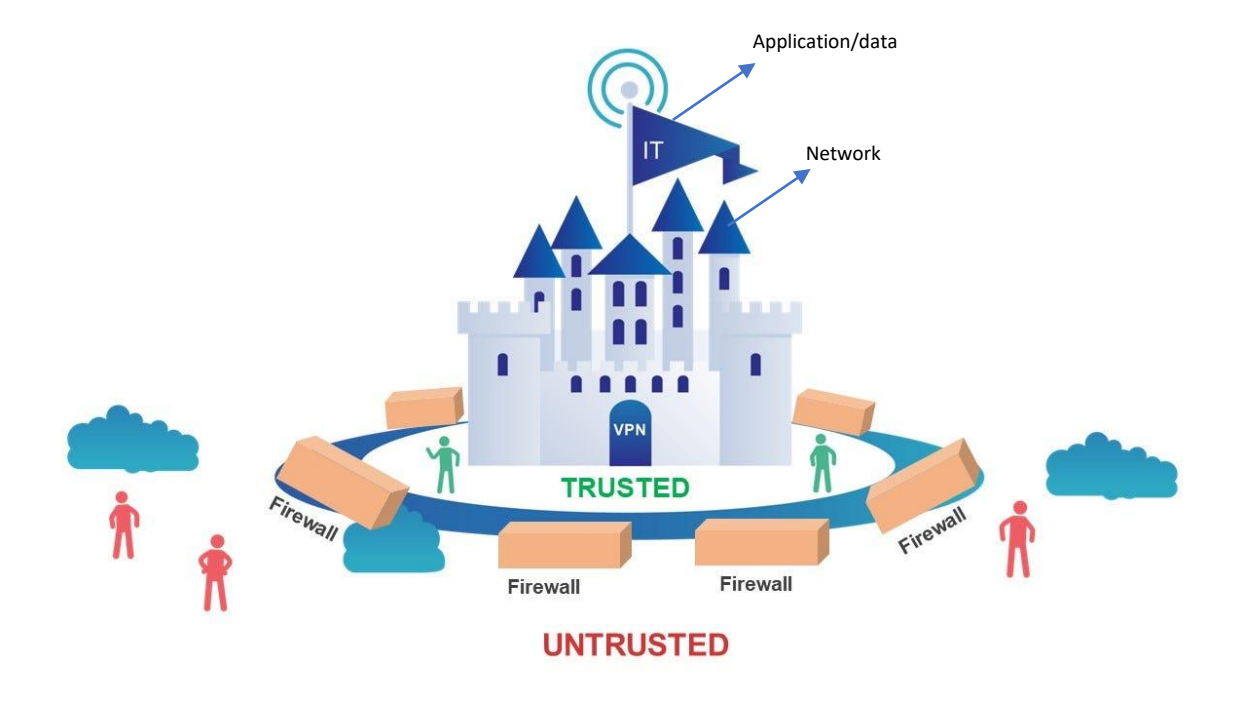
Os órgãos de gestão, direção e administração das entidades essenciais e importantes:

a) Supervisionam a aplicação das medidas de gestão dos riscos de cibersegurança;

b) Asseguram a frequência, numa base anual, de **ações de formação em cibersegurança**, bem como aos seus colaboradores ou trabalhadores, de forma a promover uma cultura de gestão interna sobre práticas de gestão dos riscos de cibersegurança.

2. Os titulares dos órgãos de gestão, direção e administração podem **responder por ação ou omissão**, com dolo ou culpa grave, nos termos da legislação aplicável, pelas **infrações previstas** no presente decreto-lei.

Componentes da Cibersegurança



Segurança dos Elementos

- Proteção de Perímetro
- Proteção de Aplicações
- Proteção de Dados
- Níveis de Criticidade Segmentados
- Utilizadores e Dispositivos Seguros

Princípios Essenciais

Atualizar Aplicações

Aplicar patches ou atualizações de segurança às aplicações de software para corrigir vulnerabilidades que possam ser exploradas por atacantes.

Atualizar Sistemas Operativos

Instalar regularmente atualizações e patches de segurança nos sistemas operativos para protegê-los contra ameaças conhecidas e melhorar a segurança geral do sistema.

Autenticação Multifator

Verificação da identidade do colaborador por meio de dois ou mais fatores independentes antes de conceder acesso a recursos, como um código enviado para o telemóvel e uma senha.

Restringir Privilégios Administrativos

Limitar o acesso e os direitos de colaboradores a operações críticas e funções administrativas do sistema para minimizar o potencial de abuso de privilégios ou danos causados por ciber ataques.

FONTE: ENISA

Princípios Essenciais

Controlo de Aplicações

Implementação de políticas que permitem somente a execução de aplicações confiáveis e autorizadas, bloqueando a execução de software malicioso ou não autorizado.

Restringir Macros do Microsoft Office

Desabilitar ou restringir a execução de macros em documentos do Microsoft Office para prevenir a execução de código malicioso que possa ser embutido em documentos.

Reforço da Segurança nas Aplicações

Aplicar configurações de segurança para tornar as aplicações usadas pelos usuários mais resistentes a ataques, como desabilitar funções desnecessárias ou vulneráveis.

Backups Regulares

Realizar cópias de segurança frequentes de dados importantes para permitir a recuperação de informações em caso de perda de dados.

FONTE: ENISA

Soluções

PESSOAS

Soluções para **garantir um acesso seguro**:

MFA

Sistema de autenticação que exige a combinação de dois ou mais fatores independentes (como senha, dispositivo físico ou biometria) para validar a identidade do utilizador, reforçando a segurança no acesso.

PLATAFORMA AWARENESS

Ferramenta educacional que promove a sensibilização dos utilizadores sobre boas práticas de cibersegurança, ajudando a prevenir erros humanos e ataques baseados em engenharia social

DISPOSITIVOS

Soluções para **proteger os dispositivos** da sua empresa:

MDM

Solução que permite às organizações gerirem, monitorizarem e protegerem dispositivos móveis, garantindo conformidade e segurança no uso de dispositivos corporativos ou pessoais.

DADOS

Soluções para **preservar a integridade dos dados** do seu negócio:

BACKUP

Processo de criação de cópias de segurança de dados, armazenadas em locais distintos, para garantir a sua recuperação em caso de falhas, perdas ou ataques cibernéticos.

REDE

Soluções para **definir perímetro e proteger a rede** da sua empresa:

FIREWALL

Ferramenta que atua como uma barreira de proteção entre redes, filtrando tráfego e bloqueando acessos não autorizados com base em regras de segurança definidas

ANTI DDOS

Solução que identifica e mitiga ataques de negação de serviço distribuídos (DDoS), garantindo a disponibilidade e o desempenho dos sistemas durante tentativas de sobrecarga maliciosa

CONSULTORIA

Soluções para garantir **conformidade e alinhamento da estratégia**:

PENTEST

Simulação controlada de ataques para identificar vulnerabilidades em sistemas, redes e aplicações, com o objetivo de reforçar a segurança antes que sejam exploradas.

A NOS é o parceiro de referência para a cibersegurança e oferece uma proposta de valor integrada que permite centralizar o ecossistema de soluções num único *provider*

Proposta de Valor Totalmente Integrada

A NOS tem condições únicas para entregar uma proposta de valor integrada nas suas áreas de especialização: Redes e Comunicações, Cloud e Datacenter, Serviços Geridos, Segurança.

Com esta proposta de valor, as empresas podem centralizar o seu ecossistema de soluções num único Provider, o que potencia a redução do risco e da complexidade operacional.

E com um conjunto de parcerias estratégicas com players das diferentes áreas tecnológicas, a NOS entrega as melhores soluções aos seus clientes.

Parceiro de referência para a Cibersegurança

Com uma vasta experiência no mercado, a NOS tem diversas certificações reconhecidas, é promotor de excelência do projeto Cyber Test-Bed que visa a aceleração de serviços inovadores de segurança e trabalha em cooperação com o CNCS, sendo membro da rede CSIRT, onde atua no tratamento e prevenção de incidentes e promove a adoção de boas práticas no mercado.

Certificações de segurança

A NOS é certificada pela norma ISO 27001 e NATO Secret.

Promotor Test-Bed

A NOS é promotor de excelência do projeto Cyber Test-Bed Multisector

160 +

Pessoas com certificações Fortinet, Cisco, Microsoft, AWS, Google, entre outros

1 000 +

Clientes que confiam diariamente na NOS na sua jornada de cibersegurança

Obrigado

Rui Custódio