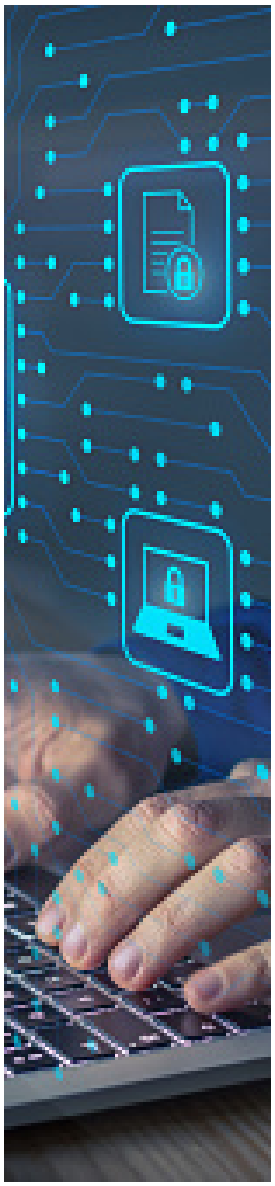
TECNOLOGIASIMAGINADAS
Tecnologias de Informação e Comunicação

Cibersegurança

Conceitos e Significados

POR CARLOS JOSÉ SANTOS SILVA
Consultor em Segurança da Informação

A SEGURANÇA DO DIGITAL



A segurança digital das entidades públicas e privadas do nosso país é uma prioridade

A consciencialização das organizações para a temática da segurança das redes e dos sistemas de informação nunca foi tão relevante como é hoje em dia.

A cada ano que passa, existe um maior número de dispositivos conectados entre si através da internet,. Alguns deles mal protegidos ou mal configurados, que acabam por se traduzir em ameaças aos ativos das empresas e organizações.
A cibersegurança, em todas as suas vertentes, deve ser uma preocupação central da sociedade e empresas.
Um ambiente seguro é fundamental para estabelecer e desenvolver qualquer atividade económica ou social.

Mundo Digital – Novo Paradigma

Na presente era da economia digital em que vivemos as infraestruturas funcionam baseadas na premissa de que:

Os elementos tecnológicos são robustos e fiáveis;
As tecnologias emergentes e complexas (por exemplo: IoT, Cloud Computing, Big Data) têm o potencial para oferecer uma elevada flexibilidade e eficiência na comunicação e coordenação de serviços e processos.

MAS...

O uso crescente de tecnologias de informação também significa que:

- As tecnologias se tornam mais vulneráveis a atividades ilícitas e maliciosas e a processos de manutenção operacionais mal planeados;
- Aumentaram os riscos relacionados com incidentes de segurança da informação
- Os operadores de serviços e as empresas devem tomar as medidas técnicas e organizacionais adequadas e proporcionais para gerir os riscos que se colocam à segurança das redes e dos sistemas de informação que utilizam nas suas operações.

SEGURANÇA DE INFORMAÇÃO

A Segurança da Informação inclui medidas necessárias para detetar, documentar e contrariar tais ameaças.

A Cibersegurança é uma das áreas de Segurança da Informação.

Cibersegurança é a prática que protege computadores e servidores, dispositivos móveis, sistemas eletrónicos, redes e dados contra ataques maliciosos.

Conjunto de medidas e ações:

- De prevenção, monitorização, deteção, reação, análise e correção;
- Que visam manter o estado de segurança desejado;
- e garantir a confidencialidade, integridade e disponibilidade da informação, das redes digitais e dos sistemas de informação no ciberespaço, e das pessoas que nele interagem.

Segurança da Informação define-se como a proteção dos sistemas de informação contra o acesso ou a modificação não autorizados 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

CONCEITOS

1. **Informação** -Dados que foram interpretados ou organizados de forma coerente e posteriormente comunicados sob qualquer forma.

2. **Ciberespaço** -Ambiente complexo, de valores e interesses, materializado numa área de responsabilidade coletiva, que resulta da interação entre pessoas e redes e sistemas de informação.

3. **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.

CONCEITOS

4. **Incidente** - evento com um efeito adverso real na segurança das redes e dos sistemas de informação; (2) Ações tomadas através da utilização de uma rede de computadores que resultam num efeito atual ou potencialmente adverso sobre um sistema de informação e/ou a informação aí armazenada

5. **Risco** - Uma circunstância ou um evento, razoavelmente identificáveis, com um efeito adverso potencial na segurança das redes e dos sistemas de informação.

6. **Ataque** - Qualquer tipo de atividade maliciosa que tenta coletar, perturbar, negar, degradar ou destruir recursos de sistema de informação ou a informação em si.

CONCEITOS

7. CIBER-HIGIENE – aplicação de boas práticas do mundo digital. (Por exemplo: Manter sempre os sistemas autorizados; Fazer cópias de segurança; Proteger sistemas com password forte)

8. 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.

9. CIBERESPAÇO FÍSICO - computadores, periféricos associados e os seus utilizadores.

CONCEITOS

10. COMUNICAÇÃO DO RISCO - consciencializar os grupos de utilizadores de sistemas de comunicação e informação para os riscos, informar as autoridades de aprovação desses riscos e reportá-los às autoridades operacionais.

11. COMPUSEC - a aplicação de atributos de segurança no hardware, firmware e software de um sistema de computador para proteção ou prevenção da perda de integridade, disponibilidade dos sistemas, a divulgação não autorizada, manipulação, modificação/eliminação de informação e negação de serviço.

TIPO DE ATAQUES CIBERNÉTICOS

- **Rasonware**- tipo de malware (vírus, trojans, etc.) que infetam os sistemas informáticos dos utilizadores e manipulam o sistema de forma a que a vítima não consiga utilizar, parcial ou totalmente, os dados armazenados que estão armazenados. A vítima geralmente recebe um aviso de chantagem por pop-up, pressionando a vítima a pagar um resgate para recuperar o acesso total ao sistema e aos arquivos.

- **Engenharia Social** - ato de enganar um indivíduo no sentido de este revelar informação sensível, assim obtendo-se acesso não autorizado ou cometendo fraude, com base numa associação com este indivíduo de modo a ganhar a sua confiança.

- **Espionagem informática** - Ciberataques dirigidos contra a confidencialidade de um sistema de tecnologias da informação.

- **Pharming** - uso de meios técnicos para redirecionar os utilizadores para páginas web falsas disfarçadas de páginas legítimas de modo a que esses utilizadores partilharem os seus dados pessoais.

- **Phishing** - mecanismo de elaborar mensagens que usam técnicas de engenharia social de modo a enganar os recetores de emails ou mensagens de phishing para que estes abram anexos maliciosos, cliquem em URL's inseguros, revelem as suas credenciais através de páginas de phishing aparentemente legítimas, façam transferências de dinheiro, etc.

POLÍTICA DE CIBERSEGURANÇA

Em 2016, foi aprovada a Diretiva (UE) 2016/1148 do Parlamento Europeu e do Conselho, de 6 de julho, relativa a medidas destinadas a garantir um elevado nível comum de segurança das redes e dos sistemas de informação em toda a União (Diretiva SRI).

• A Lei n.º 46/2018, que estabelece o regime jurídico da segurança do ciberespaço, transpondo a Diretiva SRI.

A Política de Segurança da Informação define um conjunto de orientações ou diretrizes relativas à utilização ou divulgação de informação, tais como as respeitantes à privacidade, aos direitos de cópia e à propriedade intelectual.

A sua aplicação ao meio digital coloca novos desafios, tanto ao nível da redefinição da política como da sua aplicabilidade e do seu controlo.

Uma Política de Cibersegurança tem como objetivo:

- **Estabelecer as diretrizes de Cibersegurança, visando proteger os ativos de tecnologia e os dados dos clientes da empresa;**

- **Informar as áreas e atribuir as responsabilidades para cumprimento desta Política e garantia da segurança da informação.**

PROCESSO DE GESTÃO DE RISCO DE CIBERSEGURANÇA

- Todos os procedimentos e normas de identificação, controlo e minimização de eventos incertos que tenham a potencialidade de afetar os recursos do sistema;
- Processos de gestão de riscos de segurança aplicados para monitorizar, reduzir, eliminar, evitar ou aceitar riscos;

- Todos os procedimentos e normas de identificação, controlo e minimização de acontecimentos indeterminados que possam afetar a segurança de determinada organização ou qualquer dos sistemas por ela utilizados. Este processo abarca todas as atividades relacionadas com o risco, designadamente avaliação, tratamento, aceitação e comunicação.

- Tomada de decisão de forma priorizada e informada, no contexto da cibersegurança.

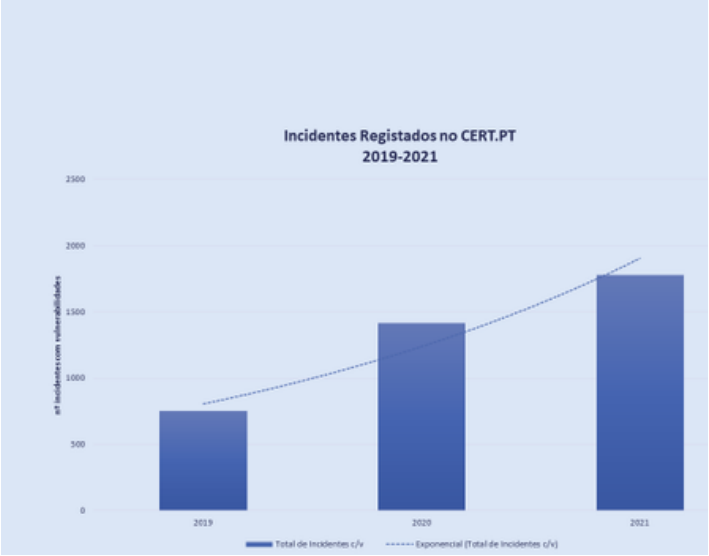
- Gestão da incerteza e determinação das ações necessárias, para que a gestão do risco possa ser minimizada para níveis considerados aceitáveis por parte da organização.

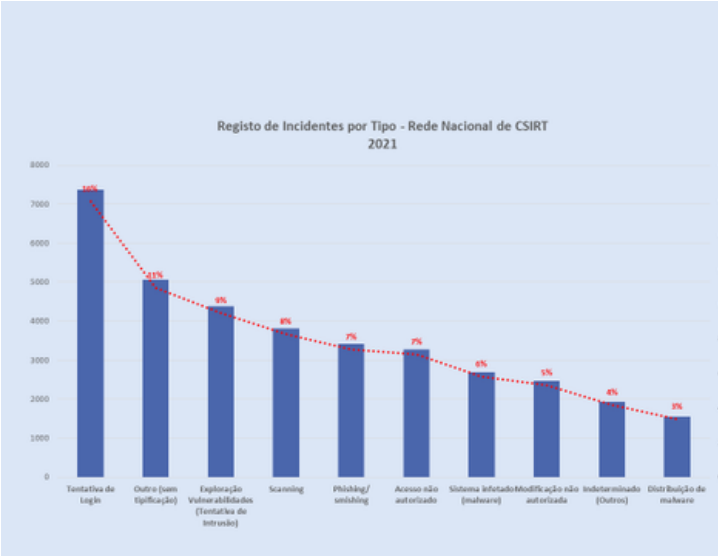
ANÁLISE E AVALIAÇÃO DA SITUAÇÃO DO CIBERESPAÇO PORTUGUÊS

Riscos e Conflitos

INCIDENTES REGISTADOS

Tendência de aumento do volume de incidentes de cibersegurança e de cibercrimes no ciberespaço de interesse nacional em 2021 e 2022.





CIBERAMEAÇAS DOMINANTES EM PT

1. Phishing (e-mail)/ smishing (SMS)/ vishing (telefone);
2. Fraude/burla online;
3. Ransomware;
4. Comprometimento de contas, ou tentativa; e
5. Exploração de vulnerabilidades (em crescimento a nível internacional).

AMEAÇAS
ANÁLISE GLOBAL

Os agentes de ameaça mais relevantes no ciberespaço:

Nível Crítico:

- Cibercriminosos;
- Phishing/smishing/vishing, ransomware e fraudes/burlas online
- Atores estatais;

ataques de phishing e spear phishing, comprometimento de contas, exploração de vulnerabilidades para a realização de intrusões

Nível Preocupante

- Ameaça interna negligente;

colaboradores que inadvertidamente comprometem a sua organização

- Cyber-offenders;

assédio ou destruição de informação

- Hacktivistas.

afirmações ideológicas no ciberespaço, através, por exemplo, de defacements

PERCEÇÃO DE RISCO E TENDÊNCIAS: ANÁLISE GLOBAL

A perceção de risco de ocorrência de incidente de cibersegurança aumentou em 2021

- Incremento de ameaças híbridas (combinam meios militares e não-militares), os ataques a cadeias de fornecimento, a exploração de vulnerabilidades e a proliferação de ransomware (tendências internacionais com impacto no ciberespaço português)
- Propensão para uma maior intervenção de atores estatais
- Persistência do uso das fragilidades do fator humano
- Ataques de ransomware, violações de dados relativas a credenciais de acesso, e exploração de vulnerabilidades

Tecnologias móveis a serem cada vez mais utilizadas como alvos de ataque

AMEAÇAS E TENDÊNCIAS

No inquérito anual à comunidade de entidades com protocolo com o CNCS:

- 98% dos inquiridos tem a perceção de risco de sofrer um incidente de cibersegurança

Apesar do incremento da perceção de risco:

- 48% dos inquiridos acredita que o ciberespaço de interesse nacional está mais capacitado.

Tipos de ciberameaças percecionados como os mais relevantes pelo mercado:

- Phishing
- Ransomware (em crescimento de perceção!)
- Engenharia social

Os **agentes de ameaça** percecionados como os mais relevantes são:

- Cibercriminosos
- Hacktivistas
- Atores estatais (CNCS).

O **tipo de agentes de ameaça** efetivamente mais relevantes são:

- Cibercriminosos
- Atores estatais
- Ameaça interna negligente

OLHAR PARA O FUTURO

PROTEÇÃO. COMPROMISSO. RESILIÊNCIA.

Prospetivas para o ciberespaço de interesse nacional:

- Contexto internacional propenso à ação de governos e entidades governamentais
- Persistência da exploração das fragilidades do fator humano
- Aumento de casos de ransomware
- Violações de dados para uso de credenciais de acesso
- Aumento de exploração de vulnerabilidades
- Relevância das tecnologias móveis e da Internet das Coisas como potenciais superfícies de ataque

EMPRESAS
MATURIDADE DIGITAL

Para gerir um negócio, na atual envolvente do mundo digital, não basta adquirirmos e usarmos as tecnologias, e esperar que elas façam o resto por nós.

As tecnologias são a base do futuro, mas as empresas só lá chegam se estiverem dispostas acompanhar o ritmo da evolução do seu mercado, a mudar processos, mentalidades e procedimentos enquadrados numa cultura de melhoria continua.

É com base neste contexto que tanto se fala na transformação digital:

UMA NOVA FORMA DE ESTAR NOS NEGÓCIOS, UM NOVO ENQUADRAMENTO EMPRESARIAL E UMA NOVA FORMA DE INTEGRAR AS EQUIPAS.

EMPRESAS
MATURIDADE DIGITAL

A transformação digital não é um fim em si mesma, mas antes um caminho a percorrer – um caminho que desagua na maturidade digital.

A **maturidade digital** é o grau de melhoria que as empresas atingem nas operações e na satisfação dos clientes graças à automação de processos.

- Apoios às empresas localizadas em território português, inseridos sobretudo no Portugal 2020 e no Plano de Recuperação e Resiliência (PRR).

- A certificação de maturidade digital está acessível a qualquer organização, do setor privado ou público, que se pode certificar nas dimensões que considerar mais relevantes e/ou prioritárias para o seu negócio.

Significado da Maturidade Digital para o Negócio

Construção de:

1. Uma cultura digital, de processos ágeis e adaptáveis;
2. Relações fortes e sólidas com os stakeholders.

Uma empresa digitalmente madura é uma empresa que está na frente do mercado.

- Maior eficiência nos processos da sua operação e negócios
- Melhor conhecimento dos seus Clientes
- Maior eficiência de planeamento de recursos
- Maior notoriedade da marca
- Melhor comunicação com o mercado
- Melhoria da relação e interação com:

1. **Clientes** (procura da satisfação plena na relação);
2. **Parceiros e fornecedores** (redução de reclamação através da mitigação de labirintos burocráticos)
3. **Colaboradores** (implementação de ferramentas de melhoria de gestão de RH; potencial de redução de tarefas repetitivas ou cujo valor não é imediatamente percetível).

OBRIGADO!

Proteja a sua empresa!

Contacte-nos.

Olívio Pereira: olivio.pereira@tecnologiasimaginadas.com
Carlos Silva: carlos.silva@tecnologiasimaginadas.com
Tecnologias Imaginadas: +351 212 592 207