DOMMIFY

MOVING BEYOND

NEWSLETTER CIBERSEGURANÇA

Uma oferta Dommify

Edição Nº1

CYBERSECURITY

Podes ser um patrocinador ! Este espaço é para ti :)

Se tens artigos que gostarias de partilhar com a equipa, envia para pedro.trindade@dommify.com

BEM-VINDOS À NOSSA PRIMEIRA NEWSLETTER!

PREZADO COLABORADOR

Sabemos que o trabalho é tanto que às vezes parece que estamos a tentar fazer backup de uma internet inteira numa disquete...Mas não te preocupes, porque resumimos algumas das nossas formações mais importantes para ti. Agora só precisas de 5 minutos para te pores a par e protegeres-te das ameaças digitais!

YAY....LEIS!!!

A segurança da informação é um tema crucial, especialmente em setores de domótica e automação industrial, onde a integridade e a disponibilidade dos sistemas são vitais para o funcionamento contínuo das operações. Nesta edição, abordaremos os principais pontos sobre a segurança da informação e as obrigações legais de cibersegurança de acordo com o Decreto-Lei n.º 65/2021.

BUCKLE UP !!

Nesta edição, vamos explorar os objetivos da segurança, identificar as principais ameaças, entender o regime jurídico vigente, apresentar medidas e boas práticas recomendadas, e analisar a cibersegurança em números. Vamos lá?

OBJETIVOS DA SEGURANÇA DA INFORMAÇÃO

A segurança da informação visa assegurar:

- **Confidencialidade**: Apenas pessoas autorizadas têm acesso à informação.
- **Integridade**: A informação não é alterada de maneira maliciosa ou negligente.
- **Disponibilidade**: O negócio não é interrompido por ações maliciosas ou negligentes.

PRINCIPAIS AMEAÇAS E VULNERABILIDADES

Ameaças podem ser ações ou eventos capazes de induzir alterações indesejadas em ativos. Estas ameaças podem ser:

- Físicas de origem natural: Catástrofes naturais.
- Físicas de origem acidental: Avarias e rupturas.
- Lógicas de origem intencional: Cibercrimes, como phishing, malware, e ransomware.

A vulnerabilidade é a susceptibilidade de um ativo a ações que comprometam sua segurança, influenciada pela probabilidade de ocorrência e de sucesso da ameaça.

> **ABRACE A VIGILÂNCIA CIBERNÉTICA, PORQUE DENTRO DELA ESTÁ A CHAVE PARA NUNCA MAIS USAR "SENHA123"**

REGIME JURÍDICO DA SEGURANÇA DO CIBERESPAÇO

Conforme o Decreto-Lei n.º 65/2021, todas as entidades devem:

- Inventário de Ativos: Elaborar e manter atualizado um inventário de todos os ativos essenciais.
- Plano de Segurança: Implementar medidas técnicas e organizativas adequadas para gerir os riscos que afetam a segurança das redes e sistemas de informação.
- Análise dos Riscos: Realizar análises periódicas dos riscos para identificar, quantificar e estabelecer prioridades para mitigação.
- Notificação de Incidentes: Notificar incidentes de segurança ao Centro Nacional de Cibersegurança (CNCS).

MEDIDAS DE SEGURANÇA E BOAS PRÁTICAS

MEDIDAS DISSUASORAS

Registos de Atividades
Objetivo: Desencorajar comportamentos inadequados ou maliciosos ao manter um registo detalhado de todas as atividades realizadas no sistema.

MEDIDAS PREVENTIVAS

Barreiras Físicas e Lógicas, Controle de Acessos
Objetivo: Prevenir acessos não autorizados e proteger a integridade dos sistemas e dados.

MEDIDAS PALIATIVAS

Isolamento de Ameaças, Aplicação de Patches
Objetivo: Minimizar os danos em caso de uma violação de segurança ou vulnerabilidade identificada.

MEDIDAS DE RECUPERAÇÃO

Planos de Recuperação, Seguros
Objetivo: Garantir a rápida recuperação e continuidade das operações após um incidente de segurança.

MEDIDAS DISSUADORAS

Como Funciona:

- Monitorização Contínua: Registar todas as ações executadas pelos usuários e sistemas em tempo real.
- Auditoria Regular: Rever logs periodicamente para identificar padrões suspeitos ou atividades anómalas.
- Transparência: Informar os utilizadores sobre a existência de registos de atividades pode dissuadir comportamentos impróprios.

Benefícios:

- Detecção Rápida: Possibilita a identificação imediata de atividades suspeitas.
- Responsabilização: Atribui ações específicas a utilizadores específicos, facilitando a responsabilidade.

MEDIDAS PREVENTIVAS

Barreiras Físicas:

- Segurança Física: Controle de acesso aos locais onde os servidores e outros dispositivos críticos estão localizados.
- Proteção de Infraestrutura: Utilização de câmeras de vigilância, fechaduras eletrônicas e guardas de segurança.

Barreiras Lógicas:

- Firewalls: Implementação de firewalls para controlar o tráfego de rede e bloquear acessos não autorizados.
- Sistemas de Detecção de Intrusão (IDS): Monitorar e analisar o tráfego de rede em busca de atividades suspeitas.

Controle de Acessos:

- Autenticação Forte: Utilização de autenticação multifator (MFA) para garantir que somente usuários autorizados possam acessar sistemas críticos.
- Políticas de Senha: Implementação de políticas rigorosas de senha, exigindo complexidade e mudanças periódicas.

Benefícios:

- Redução de Riscos: Minimizam a probabilidade de acessos não autorizados.
- Proteção Proativa: Estabelecem defesas robustas contra possíveis ataques.

MEDIDAS PALIATIVAS

Isolamento de Ameaças:

- Quarentena de Sistemas: Isolar rapidamente sistemas comprometidos para evitar a propagação da ameaça.
- Segmentação de Rede: Dividir a rede em segmentos menores para limitar o impacto de um ataque.

Aplicação de Patches:

- Atualizações Regulares: Implementar atualizações de software e patches de segurança assim que forem disponibilizados pelos fornecedores.
- Gestão de Vulnerabilidades: Utilizar ferramentas para identificar e corrigir vulnerabilidades conhecidas nos sistemas.

Benefícios:

- Mitigação de Danos: Reduzem o impacto de incidentes de segurança em andamento.
- Correção Rápida: Implementam soluções para vulnerabilidades conhecidas, prevenindo futuros ataques.

MEDIDAS DE RECUPERAÇÃO

Planos de Recuperação:

- Plano de Recuperação de Desastres (DRP): Documentação detalhada de procedimentos para restaurar sistemas críticos e dados após um incidente.
- Testes Regulares: Realizar testes periódicos do DRP para garantir sua eficácia e atualidade.

Seguros:

- Seguros Cibernéticos: Contratar seguros específicos para cobrir os custos associados a incidentes cibernéticos, como violações de dados e interrupções operacionais.
- Avaliação de Riscos: Colaborar com seguradoras para avaliar riscos e definir coberturas adequadas.

Benefícios:

- Continuidade de Negócios: Asseguram que a empresa possa retornar às operações normais rapidamente após um incidente.
- Proteção Financeira: Mitigam os impactos financeiros de incidentes de segurança, cobrindo custos de recuperação e danos.

CIBERSEGURANÇA EM NUMEROS

Aumento de incidentes

Em 2021, houve um aumento de **23%** nos incidentes de cibersegurança em comparação com 2020

Prevalência de Phishing

O phishing e o smishing foram responsáveis por **43%** dos incidentes reportados ao CERT.PT em 2020

Volume de Ataques

Portugal registou uma média semanal de 871 ataques cibernéticos por organização em 2021

Roubo de Identidade

77% dos utilizadores de internet em Portugal estão preocupados com o roubo de identidade, onde alguém se faz passar por eles usando seus dados pessoais

Infeções por Malware

74% dos incidentes reportados envolveram a infecção de dispositivos com software malicioso

Notificação de Incidentes

Mais de dois terços dos incidentes registrados pelo CERT.PT em 2020 ocorreram em entidades privadas

TIMING DE AVISOS E RELATÓRIOS

Notificação ao CNCS

As entidades devem notificar o Centro Nacional de Cibersegurança (CNCS) sobre qualquer incidente de segurança relevante no prazo de 24 horas após a detecção do incidente

Elaboração de Relatórios

A elaboração e submissão do relatório anual sobre o estado de cibersegurança da entidade deve ser feita até o dia 31 de janeiro de cada ano