IPVX
CONSULTORIA E FORMAÇÃO

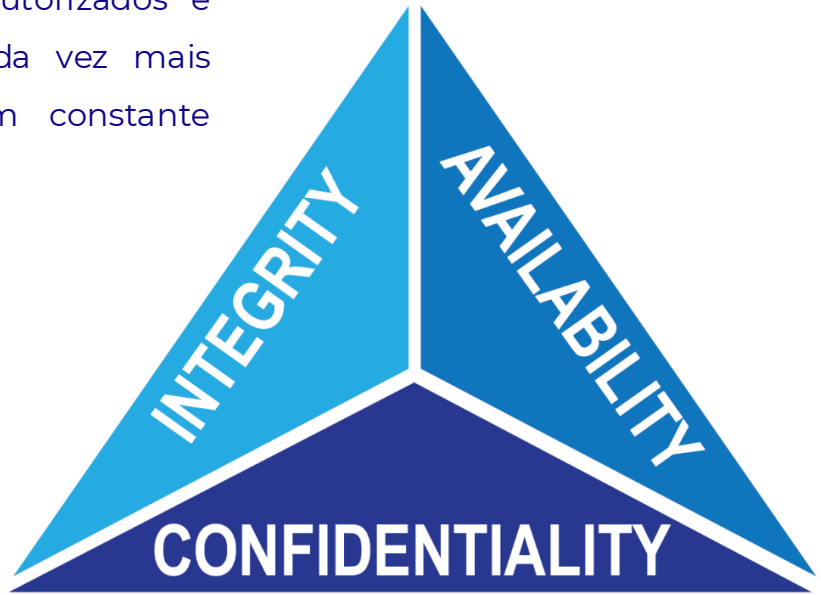
Introdução a CyberSegurança

Josuél Chifuanda

0/ DEFINIÇÕES E PRINCÍPIOS

A cibersegurança é o conjunto de práticas, tecnologias, processos e controles projetados para proteger sistemas, redes, dispositivos e dados contra ataques cibernéticos, acessos não autorizados e danos. Essa área é essencial em um mundo cada vez mais conectado, onde ameaças cibernéticas estão em constante evolução.

- Confidencialidade
- Integridade
- Disponibilidade
- Autenticidade
- Não-repúdio



CONFIDENCIALIDADE

1/ CONFIDENCIALIDADE

A confidencialidade é um dos pilares fundamentais da cybersegurança, sendo parte integrante do modelo CIA (Confidencialidade, Integridade e Disponibilidade).

Seu principal objetivo é proteger as informações contra acessos não autorizados, garantindo que apenas as pessoas, sistemas ou processos devidamente autorizados possam visualizar ou manipular os dados.

1/ CONFIDENCIALIDADE

Controle de Acesso: Limita quem pode acessar informações ou recursos específicos. É implementado por meio de:

Autenticação: Verifica a identidade de um usuário ou sistema (ex.: senhas, biometria, tokens). Autorização: Concede ou restringe acesso com base em políticas de segurança e privilégios.

Classificação de Dados: As informações são classificadas com base na sua sensibilidade (ex.: Público, Restrito, Confidencial, Secreto) e protegidas conforme o nível de criticidade.

Criptografia: Converte dados em um formato ilegível para usuários não autorizados. A descriptografia só é possível com uma chave ou credencial válida.

Segregação de Dados: Garante que os dados armazenados ou processados sejam separados de forma lógica ou física, impedindo que usuários acessem informações de outros.

Transmissão Segura Protege os dados em trânsito usando protocolos como HTTPS, VPN, SSL/TLS ou IPsec, prevenindo interceptações (man-in-themiddle).

1/ ASPECTOS FUNDAMENTAIS DA CONFIDENCIALIDADE

Transmissão Segura: Protege os dados em trânsito usando protocolos como HTTPS, VPN, SSL/TLS ou IPsec, prevenindo interceptações (man-in-the-middle).

Prevenção de Vazamentos de Informação (Data Loss Prevention - DLP) Sistemas que monitoram e controlam a movimentação de dados para impedir que informações confidenciais sejam enviadas para locais não autorizados

1/ AMEAÇAS A CONFIDENCIALIDADE

Ataques de Interceptação: Quando dados são capturados durante a transmissão (ex.: ataques man-in-the-middle, sniffing de rede).

Exposição Acidental de Dados: Ocorre quando usuários ou sistemas compartilham informações sem tomar precauções adequadas.

Acesso Não Autorizado: Inclui invasões a sistemas ou uso inadequado de credenciais comprometidas. Malware e Spyware Softwares maliciosos que capturam informações sensíveis, como keyloggers ou trojans.

Boas Práticas para Manter a Confidencialidade:

• Políticas de Senhas: Use senhas fortes, únicas e mude-as regularmente. Considere autenticação multifator (MFA).

• Educação e Conscientização: Treine usuários para reconhecer ameaças, como phishing, e aplicar práticas seguras.

• Classificação de Dados: Estabeleça critérios claros para rotular e proteger informações confidenciais.

Monitoramento Contínuo: Utilize ferramentas de segurança para identificar tentativas de acesso não autorizado.

• Restrição de Privilégios: Aplique o princípio do menor privilégio, limitando o acesso aos dados estritamente necessário.

1/ EXEMPLOS PRÁTICO DE CONFIDENCIALIDADE

Imagine que uma empresa de saúde armazena dados médicos dos pacientes. Para proteger a confidencialidade:

Controle de Acesso: Apenas médicos e enfermeiros autorizados podem acessar informações dos pacientes.

Criptografia: Dados sensíveis, como diagnósticos, são criptografados no armazenamento e durante a transmissão.

DLP: Ferramentas monitoram o envio de arquivos, impedindo que dados médicos sejam compartilhados com terceiros sem autorização.

INTEGRIDADE

2/ INTEGRIDADE

É um dos três pilares fundamentais do modelo CIA (Confidencialidade, Integridade e Disponibilidade) na cibersegurança.

Refere-se à garantia de que os dados ou sistemas não sejam alterados, corrompidos ou manipulados de forma não autorizada, preservando sua precisão, consistência e confiabilidade ao longo de seu ciclo de vida.

2/ ASPETOS FUNDAMENTAIS DA INTEGRIDADE

Proteção Contra Alterações Não Autorizadas: Assegura que os dados sejam modificados apenas por indivíduos ou processos devidamente autorizados.

Deteção de Modificações Indevidas: Utiliza mecanismos para identificar mudanças não autorizadas em dados, como logs, hashes ou sistemas de auditoria.

Manutenção de Precisão e Consistência: Garante que os dados permaneçam exatos e consistentes, tanto no armazenamento quanto durante a transmissão.

Recuperação de Dados Corrompidos: Em casos de corrupção ou modificação acidental, os sistemas devem permitir a restauração dos dados ao seu estado original.

2/ MECANISMOS PARA GARANTIR A INTEGRIDADE

Assinaturas Digitais: Utilizam criptografia para verificar a autenticidade e integridade de documentos ou transações, garantindo que os dados não foram alterados.

Hashes Criptográficos: Geração de um valor único (como um código) para um conjunto de dados. Se os dados forem modificados, o hash correspondente também será alterado.

Exemplos de algoritmos: MD5, SHA-256. Controles de Acesso: Impedem que usuários não autorizados modifiquem arquivos ou sistemas.

Logs de Auditoria: Registram todas as mudanças realizadas nos sistemas ou dados, permitindo rastrear qualquer alteração não autorizada.

Redundância e Backups: Sistemas redundantes e cópias de segurança garantem que dados originais possam ser restaurados caso sejam corrompidos.

Checksums e Controles de Erro Verificam a integridade de dados durante a transmissão, corrigindo erros que possam ocorrer no envio.

2/ AMEAÇAS À INTEGRIDADE

Modificação Maliciosa: Ataques que alteram dados intencionalmente para causar danos ou obter vantagens, como:

- Alteração de registros financeiros.
- Modificação de informações críticas em bancos de dados.

Corrupção de Dados: Pode ocorrer por erros no armazenamento, falhas de hardware ou software, ou ataques de malware.

Ataques Man-in-the-Middle (MitM): Ocorrem durante a transmissão de dados, onde um invasor intercepta e altera informações antes de chegar ao destino.

Erro Humano: Alterações acidentais realizadas por usuários legítimos sem intenção maliciosa.

2/ EXEMPLOS PRÁTICO DE INTIGRIDADE

Cenário Bancário: Imagine que um cliente faz uma transferência bancária de $100. A integridade garante que o valor transferido permaneça inalterado durante o processo, e o sistema registra exatamente $100, sem alterações.

Sistemas de Saúde: Dados médicos de pacientes, como histórico clínico ou prescrições, não podem ser alterados indevidamente, pois isso pode levar a diagnósticos ou tratamentos incorretos.

DISPONIBILIDADE

3/ DISPONIBILIDADE

A disponibilidade é o terceiro pilar fundamental do modelo CIA (Confidencialidade, Integridade e Disponibilidade) na cibersegurança. Seu principal objetivo é garantir que as informações, sistemas e recursos estejam acessíveis para os usuários autorizados sempre que necessário, evitando interrupções que possam comprometer as operações.

3/ ASPETOS FUNDAMENTAIS DA DISPONIBILIDADE

A disponibilidade é essencial para a continuidade das operações em qualquer sistema ou organização. Seus principais aspetos incluem:

Redundância: Implementação de sistemas e recursos duplicados para evitar falhas em caso de problemas. Recuperação de Desastres: Planos e mecanismos para restaurar sistemas rapidamente após incidentes.

Tolerância a Falhas: Uso de tecnologias que permitem ao sistema continuar operando, mesmo diante de falhas.

Monitoramento Contínuo: Supervisão ativa para identificar e resolver problemas antes que afetem os serviços.

Proteção Contra Ataques: Defesa contra ameaças como DDoS, que podem comprometer a acessibilidade dos sistemas.

A combinação desses fatores assegura que os serviços permaneçam disponíveis, mesmo em cenários adversos.

3/ AMEAÇAS A DISPONIBILIDADE

A disponibilidade pode ser comprometida por diversos tipos de ameaças, que incluem:

- **Ataques DDoS (Distributed Denial of Service):** Sobrecarga dos sistemas por meio de um grande volume de requisições maliciosas, tornando-os indisponíveis para usuários legítimos.
- **Falhas de Hardware:** Problemas em servidores, discos rígidos ou outros equipamentos essenciais podem causar interrupções.
- **Desastres Naturais:** Incidentes como inundações, terremotos ou incêndios podem danificar a infraestrutura física.
- **Erros Humanos:** Configurações incorretas, exclusões acidentais ou negligência podem impactar a operação do sistema
- **Malware:** Softwares maliciosos, como ransomwares, podem bloquear o acesso ao sistema ou destruir dados importantes.

Essas ameaças reforçam a necessidade de estratégias robustas para garantir que os sistemas permaneçam acessíveis mesmo diante de adversidades

3/ BOAS PRÁTICAS PARA GARANTIR A DISPONIBILIDADE

Redundância de Sistemas: Implante servidores e equipamentos de rede redundantes para evitar interrupções em caso de falhas.

Monitoramento Proativo: Utilize ferramentas de monitoramento em tempo real para identificar problemas antes que afetem os usuários.

Plano de Recuperação de Desastres (DRP): Elabore e teste regularmente um plano para restaurar serviços rapidamente após incidentes.

Manutenção Preventiva: Realize inspeções e atualizações periódicas para evitar falhas devido ao desgaste de equipamentos ou vulnerabilidades de software.

Proteção contra Ataques DDoS: Implante soluções robustas para mitigar ataques de negação de serviço e manter os sistemas operacionais.

Balanceamento de Carga: Distribua o tráfego entre servidores para evitar sobrecarga e garantir desempenho consistente.

CYBER AMEAÇAS

4/ O QUE É UMA AMEAÇA CIBERNÉTICA ?

O que é uma ameaça Cibernética ? Uma ameaça cibernética refere-se a qualquer potencial perigo ou ataque que possa comprometer a segurança de sistemas computacionais, redes, dispositivos e dados. Refere-se à ampla gama de atividades maliciosas que podem danificar ou interromper um sistema de computador, uma rede ou as informações nele contidas.

Malware: Programas maliciosos, como vírus, worms e trojans, que infectam sistemas e podem roubar dados ou causar danos.

Phishing: Técnicas de engenharia social que enganam usuários para que forneçam informações sensíveis, como senhas e dados bancários.

Ataques DDoS (Distributed Denial of Service): Ataques que sobrecarregam servidores ou redes, tornando-os indisponíveis para usuários legítimos.

Ransomware: Tipo de malware que criptografa dados e exige um resgate para liberar o acesso.

Injeção de SQL: Ataques que exploram vulnerabilidades em bases de dados para roubar ou alterar informações.

4/ O QUE É UMA AMEAÇA CIBERNÉTICA ?

Exploração de vulnerabilidades: Ameaças que aproveitam falhas de segurança conhecidas em softwares e sistemas para obter acesso não autorizado.

4/ FONTES DE AMEAÇAS CIBERNÉTICAS

Ameaças cibernéticas podem surgir de diversos pontos, com diferentes motivações e métodos. Governos Nacionais: Ataques patrocinados por estados com o objetivo de espionagem ou desestabilização.

Terroristas: Ataques para causar pânico ou interromper serviços essenciais.

Agentes Secretos Industriais: Espionagem corporativa para roubo de dados e propriedade intelectual.

Hackers: Indivíduos ou grupos que invadem sistemas para roubo de dados ou exploração de vulnerabilidades.

Insiders da Organização: Colaboradores com acesso privilegiado que podem causar danos.

4/ NÍVEL DO ÍNDICE DE AMEAÇA À CYBERSEGURANÇA

Nível do Índice de Ameaça à Segurança Cibernética As ameaças cibernéticas são avaliadas diariamente pela CTU (unidade de combate a ameaças) e associadas a um nível de índice de ameaças. Os níveis do índice de ameaça são:

- **Nível 1:** Protegido Ameaças mínimas ou inexistentes, com baixo risco.
- **Nível 2:** Elevado Ameaças possíveis ou em andamento, mas sem impacto significativo imediato.
- **Nível 3:** Alto Ameaças reais e iminentes, com risco substancial de impacto.
- **Nível 4:** Crítico Ameaças graves, com alto risco de comprometer sistemas ou dados essenciais.

CYBERATAQUES

5/ TIPOS DE CYBERATAQUES

Ameaça persistente avançada (APT): Um ataque de rede no qual uma pessoa não autorizada obtém acesso a rede e permanece lá sem ser detetada por um longo período de tempo.

Backdoor: Método para ignorar a autenticação normal e obter acesso no sistema operacional ou aplicativo

Buffer Overflow: Um exploit que tira vantagem do programa que está esperando pela entrada de um usuário.

Man-in-the-middle: Este ataque intercepta e retransmite mensagens entre duas partes que estão se comunicando diretamente uma com a outra.

Script entre sites (XSS): Um ataque de injeção de código que permite que um invasor execute JavaScript malicioso no navegador de outro usuário.

Ataque de negação de serviço (DOS): Qualquer ataque em que os invasores tentam impedir que usuários autorizados acessem o serviço.

Injeção SQL: Uma vulnerabilidade muito comum explorada em aplicativos da web que permite que hackers mal-intencionados roubem e alterem dados no banco de dados do site.

5/ IMPACTOS DOS CYBERATAQUES

Um ataque cibernético bem-sucedido pode causar danos significativos a organizações, sistemas e à confiança do consumidor. Alguns dos impactos potenciais incluem:

- **Perda financeira:** Custos associados a danos diretos, como roubo de dados, interrupções nas operações e gastos com recuperação e mitigação.
- **Danos à reputação:** A percepção negativa por parte dos consumidores e parceiros pode reduzir a confiança na marca, resultando em perda de clientes e market share.
- **Consequências jurídicas:** Multas e sanções decorrentes do não cumprimento de regulamentações de segurança e privacidade de dados, além de possíveis processos legais.

CÓDIGOS MALICIOSOS

6/ CÓDIGOS MALICIOSO

Códigos maliciosos (malware) são programas ou scripts desenvolvidos com o intuito de prejudicar ou comprometer a segurança de um sistema ou rede. Esses códigos podem ser distribuídos por diferentes meios, como e-mails, downloads ou sites comprometidos, e podem afetar dispositivos pessoais, sistemas corporativos e servidores. Alguns tipos comuns de códigos maliciosos incluem:

Vírus: Programas que se propagam ao infectar arquivos legítimos e se replicar.

Worms: Malwares que se espalham automaticamente através de redes, sem a necessidade de interação do usuário.

Trojan Horses (Cavalos de Troia): Programas que se disfarçam como softwares legítimos, mas, quando executados, permitem que um atacante ganhe controle sobre o sistema.

Ransomware: Software que criptografa os dados de uma vítima e exige um resgate para a liberação. • Spyware: Malwares que espionam e coletam informações d

6/ CÓDIGOS MALICIOSO

Spyware: Malwares que espionam e coletam informações do usuário sem seu consentimento. Esses códigos maliciosos podem causar danos variados, desde roubo de dados até comprometer a integridade e a disponibilidade dos sistemas.

Botnet: é uma rede de dispositivos infectados por malware, conhecidos como "bots" ou "zumbis". Os cibercriminosos usam botnets para controlar remotamente esses dispositivos e realizar ataques em grande escala, como ataques DDoS (negação de serviço distribuída), ou para enviar spam.

Keylogger: é um tipo de malware que registra todas as teclas pressionadas pelo usuário. Ele pode ser usado para capturar informações confidenciais, como senhas, números de cartão de crédito ou outras informações pessoais.

Rootkit: é um conjunto de ferramentas maliciosas projetadas para obter acesso privilegiado a um sistema e ocultar a presença de outros malwares. Rootkits podem ser difíceis de detectar e eliminar.

VULNERABILIDADES

7/ O QUE É UMA VULNERABILIDADE ?

Em segurança cibernética, vulnerabilidade se refere a uma falha em um sistema que pode torná-lo suscetível a ataques. Uma vulnerabilidade é composta por três elementos principais:

- **Falha no sistema:** Um erro ou defeito no design, implementação ou configuração de um sistema que cria uma brecha de segurança.
- **Acesso do invasor:** O invasor deve ter a capacidade de acessar o sistema para explorar a falha. Isso pode ser feito por meio de credenciais roubadas, um ataque direto ou outras formas de acesso não autorizado.
- **Capacidade de explorar a falha:** O invasor deve ter os recursos ou o conhecimento necessários para tirar proveito da falha e realizar um ataque, como a execução de código malicioso ou o acesso a dados confidenciais.

Esses três elementos combinados tornam a vulnerabilidade uma ameaça em potencial à segurança de um sistema.

7/ CLASSIFICAÇÃO DE VULNERABILIDADES ?

As vulnerabilidades podem ser classificadas com base no tipo de ativo que elas afetam. As principais classificações incluem:

Hardware: Vulnerabilidades em dispositivos físicos, como servidores, roteadores e terminais, que podem ser exploradas para comprometer a segurança do sistema.

Programas: Defeitos ou falhas em software, como bugs ou erros de código, que podem ser explorados por atacantes para obter acesso não autorizado ou causar danos.

Rede: Falhas nos protocolos de comunicação, na configuração de rede ou em dispositivos de rede, que podem ser exploradas para interceptar ou modificar dados.

Humanas: Vulnerabilidades associadas a erros humanos ou comportamentos indevidos, como falta de treinamento em segurança ou uso inadequado de sistemas.

Local físico: Deficiências no ambiente físico, como falta de segurança nas instalações, que podem permitir acesso físico não autorizado a equipamentos ou dados sensíveis.

Organizacional: Falhas em processos, políticas e controles internos de segurança, que podem ser exploradas por atacantes para comprometer a segurança de uma organização.

7/ CLASSIFICAÇÃO DE VULNERABILIDADES ?

As vulnerabilidades em sistemas de segurança cibernética podem ser originadas por diversos fatores, frequentemente relacionados à falta de práticas adequadas de proteção e monitoramento. Entre as causas mais comuns estão:

Faltando patches: A ausência de atualizações regulares e patches de segurança essenciais permite que falhas conhecidas permaneçam exploráveis, expondo o sistema a riscos significativos.

Credenciais de texto não criptografado: Quando as credenciais de acesso são armazenadas ou transmitidas em texto simples, sem criptografia, tornam-se vulneráveis à interceptação, facilitando o acesso não autorizado a sistemas e dados sensíveis.

Usando canais não criptografados: A utilização de canais de comunicação sem criptografia deixa os dados expostos, tornando os suscetíveis a ataques, como o "man-in-the-middle", em que os dados são interceptados e manipulados por terceiros

Emanação de RF: Dispositivos que emitem sinais de radiofrequência (RF) podem, inadvertidamente, vazar informações sensíveis, criando uma vulnerabilidade que pode ser explorada por atacantes para interceptar comunicações sem fio ou acessar dados privados.

IPVX
CONSULTORIA E FORMAÇÃO

OBRIGADO!!

Josuél Chifuanda