

Artigo sobre Antivírus - EP II RC

Armando Augusto Marchini Vidal,
Marcos Vilela Rezende Júnior

Dezembro 2023

1 Conversas com IAs

1.1 19/12

Pergunta:

Defina, de forma breve, os seguintes assuntos:

- TCP/UDP
- Camada de Redes
- Camada de Enlace
- Segurança
- Segurança de redes

Resposta:

Claro, aqui estão as definições breves para os termos que você mencionou:

- **TCP/UDP:** TCP (Protocolo de Controle de Transmissão) e UDP (Protocolo de Datagrama do Usuário) são partes da suíte de protocolos da internet. O TCP é um protocolo orientado à conexão que garante a entrega completa e correta dos dados, enquanto o UDP é um protocolo sem conexão que não oferece garantias de entrega
- **Camada de Redes:** É a camada 3 no Modelo OSI, responsável pelas conexões entre redes diferentes. Ela permite a conexão e transferência de pacotes de dados entre diferentes redes. O Protocolo de Internet (IP) é um dos principais protocolos usados nesta camada
- **Camada de Enlace:** É a camada mais baixa no conjunto de protocolos de Internet, responsável pela comunicação confinada ao enlace (link) ao qual um computador (host) está fisicamente conectado

- **Segurança:** Refere-se à proteção contra perigo ou ameaça potencial, ou ausência de risco, ou à certeza e inexistência de dúvidas. É um termo utilizado de maneira específica em diversas áreas, como segurança social, segurança cidadã, segurança informática, segurança alimentar, segurança rodoviária, entre outras

- **Segurança de redes:** É qualquer atividade projetada para proteger o acesso, o uso e a integridade da rede corporativa e dos dados. Inclui tecnologias de hardware e software, tem como alvo uma variedade de ameaças e impede que as ameaças entrem ou se espalhem na rede

Pergunta:

Quais temas dentro de segurança de redes podem ser pesquisados a parte para criação de um artigo?

Resposta:

Existem vários temas interessantes dentro da segurança de redes que você pode explorar para a criação de um artigo. Aqui estão algumas sugestões:

1. **Invasão de sistemas empresariais:** Este tema pode abordar as técnicas utilizadas pelos invasores, os tipos de sistemas mais visados e as medidas preventivas que podem ser adotadas
2. **Quebra de sigilo de dados:** Você pode discutir sobre os métodos utilizados para quebrar o sigilo de dados e como as empresas podem proteger suas informações
3. **Ataques cibernéticos:** Este é um tema amplo que pode incluir tipos de ataques, impactos

desses ataques e estratégias de defesa

4. **Prejuízos causados por ataques hackers:**
Aqui, você pode explorar os impactos financeiros e operacionais que os ataques hackers podem causar nas organizações
5. **Medidas voltadas para a defesa dos dados:**
Este tema pode abordar as várias técnicas e ferramentas utilizadas para proteger os dados de ataques
6. **Integridade e o valor das informações:**
Você pode discutir a importância da integridade dos dados e como ela afeta o valor das informações

Lembre-se, é importante escolher um tema que seja de seu interesse e que tenha bastante material disponível para pesquisa. Boa sorte com seu artigo!

Pergunta:

Destrinche os temas 5 e 6 apresentados na resposta anterior, mostrando um breve resumo sobre eles e também aponte possíveis sub temas dentro de cada para uma pesquisa mais aprofundada

Resposta:

Claro, aqui estão os detalhes sobre os temas 5 e 6:

5. Medidas voltadas para a defesa dos dados

A segurança da informação é uma série de ações estratégicas adotadas para controlar e evitar riscos de roubo, danos e perdas de dados, dispositivos, servidores, sistemas e redes. As medidas de proteção de dados envolvem a realização periódica de backup dos arquivos, manutenção de sistemas operacionais atualizados, recomendação de não instalação de softwares e arquivos desconhecidos, e uso de antivírus. Aqui estão alguns subtemas que você pode explorar:

- **Backup de dados:** Como os backups regulares podem ajudar a proteger os dados.
- **Atualizações de sistema operacional:** A importância de manter os sistemas operacionais atualizados para a segurança dos dados.

- **Softwares desconhecidos:** Os riscos associados à instalação de softwares desconhecidos.

- **Antivírus:** O papel dos antivírus na proteção dos dados.

6. Integridade e o valor das informações

A integridade dos dados é uma característica essencial da segurança da informação, garantindo que as informações não sofreram alterações não autorizadas ou impróprias. A falta de integridade das informações pode gerar ineficiência, resultando em mais custos para a mesma receita e, consequentemente, menor margem de lucro. Aqui estão alguns subtemas que você pode explorar:

- **Verificação de erros e validação:** Como esses métodos podem ajudar a garantir a integridade dos dados.

- **Impacto da falta de integridade dos dados:** Como a falta de integridade dos dados pode afetar a eficiência e a lucratividade de uma empresa.

- **Integridade referencial em bancos de dados:** O papel da integridade referencial na manutenção da integridade dos dados em bancos de dados relacionais.

- **Proteção contra alterações não autorizadas:** Medidas que podem ser tomadas para proteger os dados contra alterações não autorizadas.

Espero que isso ajude na sua pesquisa!

Pergunta:

Estou planejando fazer um artigo com o tema Antivírus: O papel dos antivírus na proteção dos dados

Resposta:

Excelente escolha de tema! A proteção de dados é uma preocupação crucial nos dias de hoje, e os antivírus desempenham um papel fundamental nesse cenário. Aqui estão algumas sugestões para estruturar e desenvolver o seu artigo:

1. Introdução

A importância dos dados na era digital.

Na era digital, a relevância dos dados vai além da mera comodidade. Eles são o pilar fundamental para a eficiência e inovação em diversos setores da sociedade. No contexto empresarial, a análise de dados tornou-se uma peça-chave na formulação de decisões estratégicas. As empresas dependem da coleta e interpretação eficiente de dados para entender melhor o mercado, antecipar tendências, otimizar operações e criar estratégias competitivas.

Por outro lado, os indivíduos também passaram a depositar sua confiança em plataformas digitais para documentar suas atividades diárias. Seja por meio de redes sociais, aplicativos de saúde ou serviços de armazenamento em nuvem, as pessoas geram e compartilham uma quantidade massiva de dados pessoais online. Esses dados podem incluir desde preferências de compra até informações sensíveis de saúde e localização.

A conectividade global oferece uma acessibilidade incrível, mas ao mesmo tempo intensifica os riscos associados ao manuseio dos dados. A perda ou comprometimento de dados sensíveis não apenas ameaça a privacidade individual, mas também pode acarretar consequências financeiras e sociais devastadoras. A exposição indevida de informações pessoais pode levar a fraudes financeiras, roubo de identidade e outros crimes cibernéticos.

A sociedade tem se tornado cada vez mais dependente da tecnologia digital, e com isso a necessidade de proteção e segurança dos dados torna-se imperativa. Empresas e indivíduos precisam implementar medidas rigorosas de segurança cibernética para mitigar os riscos associados à coleta, armazenamento e transmissão de dados.

Crescente ameaça cibernética e necessidade de proteção.

O constante avanço das tecnologias digitais traz consigo não apenas inovações benéficas, mas também uma escalada nas ameaças cibernéticas. Os ataques, cada vez mais sofisticados, variam desde esquemas de

phishing astutos até intrusões em larga escala, como o ransomware. Essas investidas não apenas comprometem dados cruciais, mas também têm o potencial de paralisar operações empresariais, resultando em danos financeiros significativos e impactos irreversíveis nas reputações das organizações afetadas. Em um contexto de crescente interconectividade digital, a proteção cibernética transcende a mera precaução, tornando-se uma necessidade imperativa. À medida que a tecnologia continua a evoluir, a adaptação constante e a inovação em segurança cibernética são indispensáveis para enfrentar e superar as ameaças em constante evolução que permeiam o ambiente digital contemporâneo.

O papel dos antivírus na segurança digital.

Os antivírus constituem a primeira linha de defesa na guerra contra ameaças digitais. Essas ferramentas especializadas utilizam algoritmos sofisticados e bancos de dados em constante atualização para reconhecer padrões de comportamento malicioso. Ao realizar varreduras contínuas em sistemas e arquivos em busca de sinais de ameaças, os antivírus desempenham um papel crucial na identificação e remoção de vírus, malware e outras formas de software indesejado. Além disso, muitos antivírus agora incorporam recursos de proteção em tempo real, oferecendo uma camada adicional de segurança contra ataques em constante evolução. Em um cenário digital cada vez mais complexo e dinâmico, a presença e eficácia dessas ferramentas são fundamentais para garantir a integridade e a segurança dos sistemas digitais.

2. Fundamentos dos Antivírus

O que são antivírus e como funcionam.

Os antivírus desempenham um papel crucial na salvaguarda da integridade e segurança dos sistemas computacionais, sendo concebidos com a finalidade específica de identificar, prevenir e erradicar software malicioso, como vírus, worms, trojans e spywares, que representam ameaças potenciais à confidencialidade e

integridade dos dados. O funcionamento dessas ferramentas é intrinsecamente vinculado à capacidade de detecção de padrões característicos dessas ameaças, fazendo uso de uma variedade de métodos e técnicas.

A análise heurística, por exemplo, constitui uma abordagem que capacita os antivírus a identificarem comportamentos suspeitos, mesmo na ausência de uma exposição prévia a uma ameaça específica. Além disso, a busca por assinaturas digitais associadas a códigos maliciosos representa uma técnica convencional e eficaz para a identificação e neutralização de ameaças já conhecidas.

Evolução dos Antivírus ao Longo do Tempo

Ao longo das últimas décadas, testemunhamos uma evolução substancial no campo dos antivírus, impulsionada pela necessidade de adaptação contínua diante de ameaças em constante mutação. Inicialmente concebidos de forma mais simplificada, esses programas centravam-se primariamente na detecção de vírus reconhecidos, sendo atualizados por meio de assinaturas. No entanto, face à crescente complexidade das ameaças, os antivírus evoluíram consideravelmente, incorporando tecnologias avançadas, tais como análise comportamental, sandboxing e aprendizado de máquina. A presença generalizada de inteligência artificial e aprendizado profundo representa, atualmente, características comuns em antivírus modernos, potencializando uma detecção mais eficiente e ágil de ameaças emergentes.

Antivírus Tradicionais versus Soluções Abrangentes

Os antivírus tradicionais, embora desempenhem um papel fundamental, frequentemente concentram-se exclusivamente na identificação e remoção de malware. Em contrapartida, as soluções de segurança mais abrangentes expandem significativamente seu escopo, visando lidar com uma gama mais ampla de ameaças. Para além da detecção de malware, essas soluções incorporam funcionalidades como firewalls para monitoramento e controle do tráfego de rede, proteção contra phishing para prevenir ataques

de engenharia social, controle parental destinado a resguardar os membros mais jovens da família e implementação de criptografia para assegurar a confidencialidade dos dados. A integração de tecnologias avançadas, como machine learning e inteligência artificial, confere a essas soluções uma abordagem proativa na identificação e mitigação de ameaças de natureza complexa. Em suma, a constante evolução dessas ferramentas reflete a busca incessante por salvaguardar a segurança cibernética em um cenário digital dinâmico e desafiador.

3. Ameaças Cibernéticas Principais

As principais ameaças combatidas pelos antivírus.

Os antivírus desempenham um papel crucial na defesa contra uma miríade de ameaças cibernéticas que evoluem constantemente. Ao longo dos anos, as técnicas dos cibercriminosos tornaram-se mais sofisticadas, exigindo que os programas antivírus evoluam para acompanhar essa evolução. Conversamos com ChatGPT e o Bing para obtermos as principais ameaças combatidas pelos antivírus. O GPT nos proporcionou uma lista mais robusta, da qual destacamos:

- **Malware:** Vírus, worms, trojans e spyware continuam a ser ameaças persistentes. Malwares são programas maliciosos que buscam explorar vulnerabilidades em sistemas para roubo de dados, interrupção de operações e até mesmo para controle remoto de dispositivos.
- **Ransomware:** Uma ameaça particularmente devastadora, o ransomware criptografa os arquivos de uma vítima, exigindo o pagamento de um resgate em troca da chave de descriptografia. Essa forma de ataque tem causado prejuízos significativos a empresas e indivíduos.
- **Phishing:** Táticas de engenharia social, como e-mails fraudulentos, sites falsos e mensagens

de texto enganosas, são usadas para obter informações confidenciais, como senhas e dados bancários, explorando a confiança das vítimas.

- **Ataques de dia zero:** Explorando vulnerabilidades previamente desconhecidas em softwares, os ataques de dia zero podem ocorrer antes que os desenvolvedores tenham tido a oportunidade de criar uma correção. Os antivírus desempenham um papel crucial na detecção precoce desses ataques.
- **Botnets:** Redes de dispositivos infectados que são controlados remotamente por hackers, muitas vezes para realizar ataques distribuídos de negação de serviço (DDoS) ou para distribuição de spam.

Estatísticas Recentes sobre Ataques Cibernéticos.

O cenário de ameaças cibernéticas tem evoluído rapidamente, com um aumento constante no número e na sofisticação dos ataques. Novamente fomos a nossas IAs para consultar informações. Podemos dizer que as estatísticas recentes revelam uma realidade alarmante para a segurança das redes de computadores:

- **Golpes no WhatsApp no Brasil:** Mais de 3 milhões de golpes foram registrados apenas no aplicativo de mensagens WhatsApp no Brasil. Isso demonstra como os criminosos estão explorando plataformas populares para atingir um grande número de usuários.
- **Ransomware em Ascensão:** Em 2021, os ataques de ransomware (que envolvem o sequestro de dados e a exigência de resgate) totalizaram US\$102,3 milhões por mês. Esses ataques afetaram empresas, organizações governamentais e até mesmo indivíduos, causando prejuízos significativos.
- **Aumento dos Ataques Cibernéticos no Brasil:** No primeiro semestre de 2022, houve 31,5 bilhões de tentativas de ataques cibernéticos direcionadas a empresas no Brasil. Esse número

representa um aumento alarmante de 94% em relação ao ano anterior. As organizações precisam estar preparadas para enfrentar essas ameaças constantes. No segundo trimestre de 2022, os ataques cibernéticos no Brasil aumentaram 46% em comparação com o mesmo período do ano anterior. Isso destaca a urgência de medidas preventivas e de proteção digital.

- **Ataques Cibernéticos em 2023:** Somente em 2023, o Brasil já sofreu 23 bilhões de ataques cibernéticos. Entre eles, os golpes de vírus bancários tiveram um crescimento de 20%. Esses ataques podem resultar em roubo de informações financeiras e comprometimento da privacidade dos usuários.

Em resposta a essas ameaças em constante evolução, a comunidade de segurança cibernética continua a desenvolver e aprimorar estratégias de defesa, incluindo a implementação de soluções antivírus avançadas, conscientização do usuário e práticas de segurança robustas em redes de computadores.

4. Funcionalidades dos Antivírus

Dentre as funcionalidades de um antivírus podemos citar: Análise em tempo real, Detecção heurística, Atualizações automáticas de definições, Proteção contra phishing e ameaças online e Firewall integrado. Para entrar em mais detalhes, pedimos para que o Copilot do Bing e o ChatGPT selecionassem as mais importantes. Como resultado temos, respectivamente, Análise em tempo real e Atualizações automáticas de definições. Esses tópicos foram escolhidos com base na eficácia de aplicação e preparação de um antivírus.

Análise em tempo real

O antivírus monitora constantemente as atividades do sistema em execução, identificando e respondendo a ameaças. Temos como características:

- **Monitoramento contínuo:** Todos os arquivos, processos e atividades do sistema são verificados.

- **Heurística e assinaturas:** Combinação de técnicas como análise de comportamento com definições conhecidas de ameaças para identificar padrões.
- **Verificação de arquivos em acesso:** Verificação do conteúdo de arquivos abertos, executados, copiados ou modificados.
- **Proteção contra exploits:** Monitoramento de atividades que indicam tentativas de explorar vulnerabilidades do sistema.
- **Bloqueio em tempo real:** Ao detectar uma ameaça, o antivírus pode bloquear, quarentenar ou remover o arquivo/processo malicioso.
- **Atualizações automáticas:** Definições de vírus e outras ameaças são mantidas atualizadas automaticamente pelo antivírus.
- **Mínimo impacto no desempenho:** Antivírus projetado para ter o mínimo impacto no desempenho e nos processos do computador do usuário.

Atualizações automáticas de definições

O antivírus se mantém atualizado para as informações mais recentes sobre as ameaças cibernéticas por esse processo. Ele garante a eficácia do antivírus e possui os seguintes aspectos:

- **Definições de vírus e malware:** Bancos de dados com informações para identificar ameaças (assinatura de código, comportamentos, entre outros) para combatê-las.
- **Atualizações regulares e automáticas:** Essas atualizações ocorrem regularmente e garantem que o antivírus esteja sempre atualizado com informações sobre ameaças que surgem a todo momento.
- **Reações a ameaças emergentes:** Com o surgimento de novas ameaças, fornecedores de antivírus devem desenvolver definições para identificação delas.

- **Assinaturas digitais e técnicas de detecção:** Assinaturas digitais de malware conhecido, técnicas de detecção heurística e comportamentais e outras estratégias estão incluídas nas definições de cada atualização.
- **Automatização de processo:** A atualização automática, sem interferência do usuário, é essencial para que o antivírus verifique a disponibilidade de atualizações e baixe-as.
- **Conexão com a internet:** Essas atualizações automáticas requerem conexão com a internet para permitir atualizações para definições mais recentes.

5. Impacto dos Antivírus na Performance

Formas de Impacto

Diversos fatores podem ser observados em um antivírus que impactam direta ou indiretamente no desempenho de um sistema. Alguns dos pontos principais que devem ser observados são:

- **A Variação de Desempenho:** É preciso notar qual o tamanho do impacto de cada antivírus na performance de um sistema. Enquanto alguns antivírus são focados no baixo impacto, outros consomem mais recursos para uma maior proteção. Testes feitos por terceiros podem ser encontrados online.
- **Os Recursos do Sistema:** Os recursos consumidos pelo antivírus podem incluir a CPU, a memória RAM e o armazenamento. A complexidade de realização de suas funções de verificação e proteção determinam o quanto de cada um desses recursos será consumido.
- **As Configurações do Antivírus:** Alguns antivírus podem oferecer opções de configuração que permitem ao usuário ajustar o equilíbrio entre segurança e desempenho.

- **Varreduras Agendadas:** Uma das formas de contornar o problema de consumo de recursos (e por consequência o impacto no desempenho) é através das varreduras agendadas. Elas podem ser feitas em momentos de baixa atividade do usuário para competir menos pelos recursos do sistema. De forma contrária, se estas varreduras forem feitas em momentos de alto uso por parte do usuário, o consumo e a competição pelos recursos será maior.
- **Atualizações e Verificações em Tempo Real:** Atualizações em tempo real, assim como verificações constantes de arquivos em execução, tem um impacto direto no desempenho, especialmente para sistemas antigos e/ou com recursos limitados.
- **Hardware e Tecnologia:** De forma geral, como visto pelo item anterior, sistemas mais antigos e com maior limitação de recursos irão sofrer mais com o uso de antivírus, tendo um impacto de desempenho muito mais visível.

É possível ressaltar alguns antivírus que possuem impacto em desempenho, apesar de baixo. Por exemplo: o F-Secure (suportado apenas pelo Windows) venceu prêmios de Melhor Proteção e Melhor Desempenho da AV-TEST em diversos anos e pode ser considerado como uma das melhores opções; e também o Panda Dome Antivirus que possui alta eficiência em proteção e uma execução na nuvem, que otimiza o desempenho.

Por outro lado, também é possível notar impactos positivos no desempenho desses sistemas com a utilização de antivírus. Apresentando soluções como por exemplo a otimização de tarefas ou limpeza de memória, os computadores podem iniciar mais rapidamente, funcionar sem muitos problemas e, obviamente, remover vírus que impactam seu desempenho, mesmo que estes tenham infectado o sistema antes da instalação do antivírus.

Discussão sobre o equilíbrio entre proteção e desempenho.

Para encontrar um equilíbrio entre o impacto no desempenho do sistema e a proteção garantida pelo antivírus, os principais fatores a serem levados em consideração são:

- **Necessidades Individuais:** A priorização do usuário entre a segurança do sistema e seu desempenho. Isso é um fator que varia de pessoa a pessoa.
- **Tipo de Uso do Computador:** Tarefas intensivas que demandam muito do sistema podem exigir um antivírus com impacto mínimo.

Esses fatores devem ser considerados na escolha de um público-alvo para a empresa dona do antivírus, visto que o escopo pode variar muito e, com isso, a necessidade e a priorização.

Dentre as formas de evitar esses problemas, temos (entre soluções que podem ser aplicadas de forma geral):

- **Configurações Ajustáveis:** Para conseguir abranger um número maior de necessidades, uma alta personalização de configurações permite que o usuário decida a relação entre proteção/impacto de forma mais livre.
- **Atualizações Incrementais:** Baixando apenas novas definições de ameaça, ao invés de todo o banco de dados, um antivírus pode diminuir seu impacto enquanto garante proteção contra ameaças desconhecidas.

6. Estudo de Caso

Dentre os testes de desempenho de sistemas com e sem antivírus, podemos destacar e analisar o teste de performance feito pela AV-Comparatives. Esse teste avalia o impacto do software antivírus no desempenho do sistema. Em 2015, ano que será analisado, os testes foram realizados em uma máquina com um processador Intel Core i7, 8GB de RAM

e discos SSD, sob um sistema Windows 10 Home 64-Bit atualizado. Os produtos de segurança foram avaliados com as configurações padrão e com uma conexão ativa à Internet. Foram realizadas as seguintes atividades/testes: cópia de arquivos, arquivamento/desarquivamento, instalação de aplicativos, lançamento de aplicativos, download de arquivos, navegação na web e PC Mark 10 Professional Testing Suite.

Comparação de diferentes soluções antivírus no mercado.

Tendo como objeto de estudo o antivírus F-Secure, temos os seguintes resultados:

- Cópia de arquivos: 0,9 segundos a mais do que o sistema sem antivírus (média de 11,8 segundos)
- Arquivamento/desarquivamento: 0,8 segundos a mais do que o sistema sem antivírus (média de 23,8 segundos)
- Instalação de aplicativos: 0,7 segundos a mais do que o sistema sem antivírus (média de 29,4 segundos)
- Lançamento de aplicativos: 0,3 segundos a mais do que o sistema sem antivírus (média de 6,6 segundos)
- Download de arquivos: 0,1 segundos a mais do que o sistema sem antivírus (média de 10,1 segundos)
- Navegação na web: 0,1 segundos a mais do que o sistema sem antivírus (média de 10,1 segundos)
- PC Mark 10: 0,1% a menos do que o sistema sem antivírus (média de 100%)

O F-Secure (no ano de 2015 em que a análise foi feita) ficou em segundo lugar nas comparações entre os 19 softwares, perdendo apenas para o ESET Smart Security 9.0 que teve uma interferência praticamente nula no sistema. Dentre as medidas usadas, o F-Secure se destacou principalmente nas atividades de arquivos (cópias, arquivamento/desarquivamento) e instalação

de aplicativos, tendo um impacto menor que a maioria de seus concorrentes. O F-Secure, nessa análise, se mostrou um dos produtos mais leves e eficientes do mercado, com um baixíssimo impacto de desempenho no Windows 10. Isso o torna uma ótima opção para a busca de antivírus e o mostra como um excelente exemplo de eficiência no que foi estudado ao longo do artigo.

7. Conclusão

- Recapitulação do papel dos antivírus na proteção de dados.
- Perspectivas futuras para a segurança cibernética.

8. Referências

- Cite estudos, relatórios e fontes confiáveis para fundamentar as informações apresentadas.

Lembre-se de adaptar o conteúdo de acordo com a extensão e os requisitos específicos do seu artigo. Além disso, atualize as informações para refletir as últimas tendências e desenvolvimentos na área de segurança cibernética e antivírus. Boa sorte com o seu artigo!