https://www.educamaisbrasil.com.br/educacao/noticias/qual-e-a-estrutura-de-um-artigo-cientifico-abnt (Texto com estrutura de artigo)
https://www.educamaisbrasil.com.br/educacao/noticias/qual-e-a-estrutura-de-um-artigo-cientifico-abnt

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 possóiveis 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

- **C**ontextualização sobre a importância dos dados na era digital.
- **C**rescente ameaça cibernética e necessidade de proteção.
- **A**presentação do papel dos antivírus na segurança digital.

2. Fundamentos dos Antivírus

- **E**xplicação sobre o que são antivírus e como funcionam.
- **E**volução dos antivírus ao longo do tempo.
- **D**iferença entre antivírus tradicionais e soluções de segurança mais abrangentes.

3. Principais Ameaças Cibernéticas

- **D**escrição das principais ameaças que os antivírus ajudam a combater (vírus, malware, ransomware, etc.).
- **E**statísticas recentes sobre o aumento de ataques cibernéticos.

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 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 maisr apidamente, 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, oa 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

- **R**ecapitulação do papel dos antivírus na proteção de dados.
- **P**erspectivas futuras para a segurança cibernética.

8. Referências

- **C**ite 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!