APOSTILA DE SEGURANÇA DA INFORMAÇÃO

CONCEITOS DE SEGURANÇA DA INFORMAÇÃO

2020

Sumário

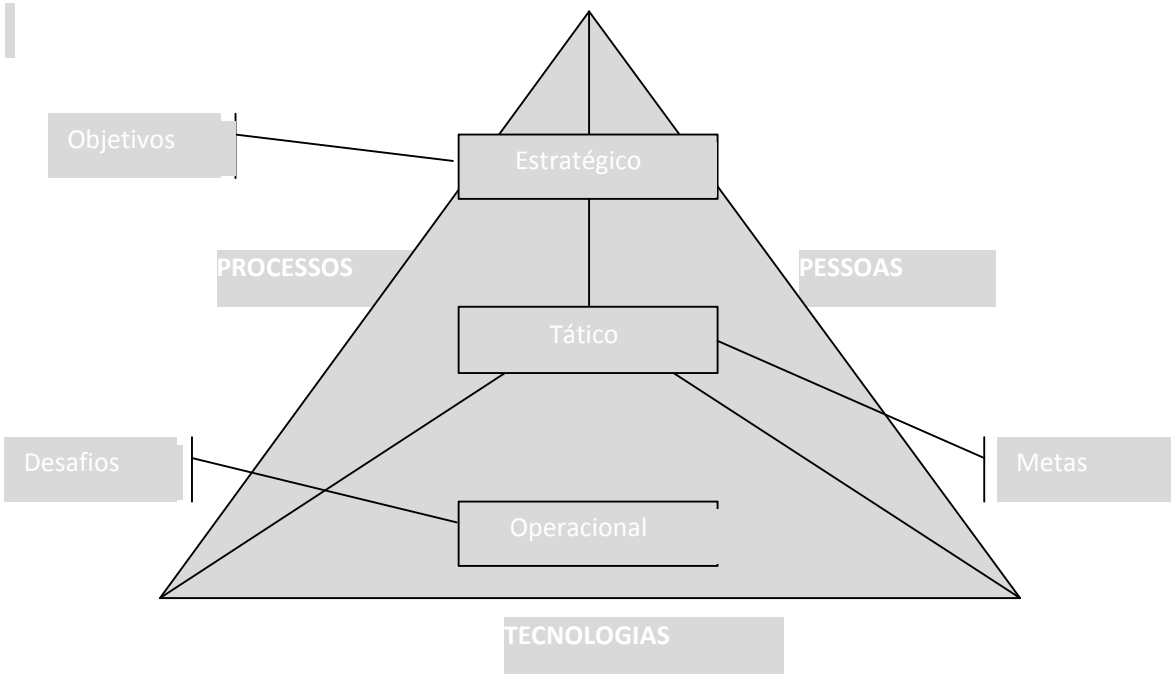
Introdução

Avanços na tecnologia computacional tem criado uma repentina busca por pessoas para ajudar a monitorar e proteger dados e informações que pessoas utilizam para completarem seu trabalho. Estes avanços também colocam tecnologias nas mãos das pessoas que frequentemente não tem experiência e conhecimento para proteger isso. Como um computador de segurança profissional, você tem uma responsabilidade primária de proteger e resguardar a informação que sua organização utiliza. A área de Segurança está em crescimento na indústria do computador, e a necessidade por pessoas qualificadas está aumentando rapidamente. Sua perseguição de segurança + certificado é uma ótima primeira etapa neste processo.

A presente apostila de forma bem simples tentará compartilhar informações pertinentes à segurança da informação dentre os vários aspectos de segurança computacional. Este trabalho introduz o básico da segurança computacional e provê vários conceitos e orientações que poderão ser utilizados para entendermos os riscos que as organizações encaram e as etapas que você deve seguir como regra para minimizar estes riscos.

A importância da Informação

A informação é o dado com uma interpretação lógica ou natural dada a ele por seu usuário. A informação tem um valor altamente significativo e pode representar grande poder para quem a possui. A informação contém valor, pois está integrada com os processos, pessoas e tecnologias. A próxima figura demonstra, do ponto de vista estratégico, o relacionamento dos processos, tecnologias e pessoas.



Vivemos em uma sociedade eu se baseia em informações e que exibe uma crescente propensão para coletar e armazenar informações e o uso efetivo da informação permite que uma organização aumente a eficiência de suas operações.

A informação é um ativo que, como qualquer outro ativo importante para os negócios, tem um valor para a organização e consequentemente necessita ser adequadamente protegida (NBR 17999, 2003). Na sociedade da informação, a informação é o principal patrimônio da empresa e está sob constante risco. A informação representa a inteligência competitiva dos negócios e é reconhecida como ativo crítico para a continuidade operacional e saúde da empresa. A informação e o conhecimento serão os diferenciais das empresas e dos

profissionais que pretendem destacar-se no mercado e manter a sua competitividade.

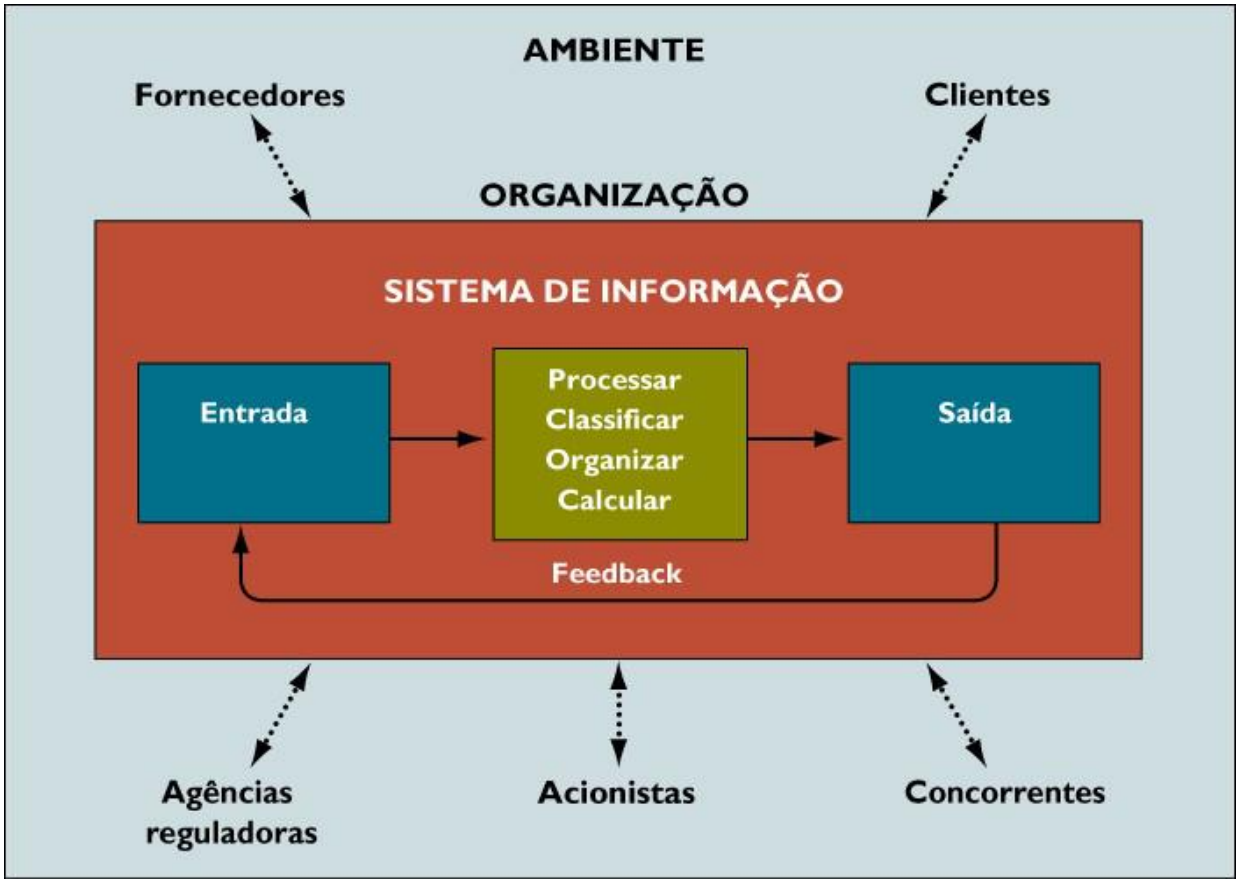
As empresas já perceberam que o domínio da tecnologia como aliado

para o controle da informação é vital. O controle da informação é um fator de sucesso crítico para os negócios e sempre teve fundamental importância para as corporações do ponto de vista estratégico e empresarial. Dispor da informação correta, na hora adequada, significa tomar uma decisão de forma ágil e eficiente. Com a evolução dos dados e sistemas, a informação ganhou mobilidade, inteligência e real capacidade de gestão. A informação é substrato da inteligência competitiva; deve ser administrada em seus particulares, diferenciada e salvaguardada.

Sistema de Informação

Um sistema de informação pode ser definido tecnicamente como um conjunto de componentes inter-relacionados que coleta (ou recupera), processa, armazena e distribui informações destinadas a apoiar a tomada de decisões, a coordenação e o controle de uma organização. Além de dar suporte à tomada de decisões, à coordenação e ao controle, esses sistemas também auxiliam os gerentes e trabalhadores a analisar problemas, visualizar assuntos complexos e criar novos produtos.

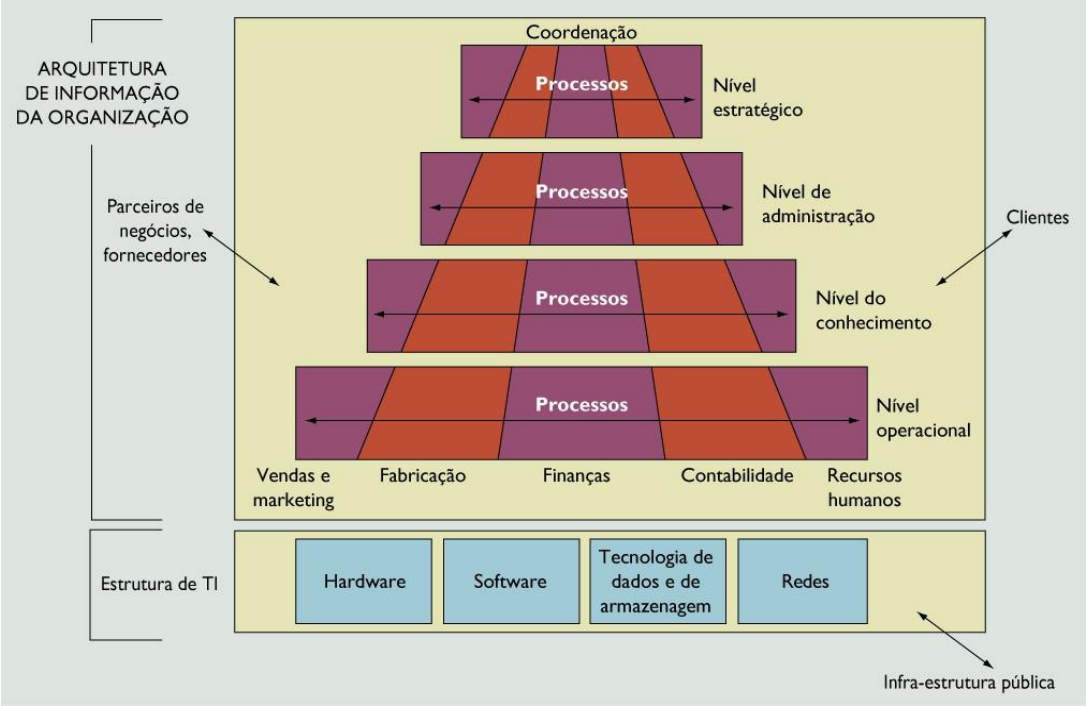
Os sistemas de informação contêm informações sobre pessoas, locais e coisas significativas para a organização ou para o ambiente que a cerca. Três atividades em um sistema de informação produzem as informações de que as organizações necessitam para tomar decisões, controlar operações, analisar problemas e criar novos produtos ou serviços. Essas atividades são a entrada, o processamento e a saída (veja a próxima figura).



A entrada captura ou coleta dados brutos de dentro da organização ou de seu ambiente externo. O processamento converte esses dados brutos em uma forma mais significativa. A saída transfere as informações processadas às pessoas que as utilizarão ou às atividades em que serão empregadas. Os sistemas de informação também requerem um feedback, que é a entrada que volta a determinados membros da organização para ajudá-los a avaliar ou corrigir o estágio de entrada.

Os sistemas de informação são partes integrantes das organizações. Na verdade, para algumas empresas, como as que fazem avaliação de crédito, sem sistema de informação não haveria negócios.

Os administradores de hoje devem saber como estruturar e coordenar as diversas tecnologias de informação e aplicações de sistemas empresariais para atender às necessidades de informação de cada nível da organização e às necessidades da organização como um todo.



Informação, competitividade e estratégia

Segundo (Rezende e Abreu, 2000), a informação desempenha papéis importantes tanto na definição quanto na execução de uma estratégia. A informação auxilia os executivos a identificar tanto as ameaças quanto as oportunidades para a empresa e cria o cenário para uma resposta competitiva mais eficaz. A informação funciona também como um recurso essencial para a definição de estratégias alternativas. A informação é essencial para a criação de uma organização flexível na qual existe um constante aprendizado.

As organizações estão modificando-se profundamente, invertendo suas pirâmides organizacionais, criando unidades de negócios autônomas, descentralizando decisões e constituindo parcerias. A garantia de sua integração e da manutenção de parâmetros comuns de atuação é dada pela informação, que flui entre suas várias partes.

A eficácia de uma empresa pode ser definida pela relação entre resultados obtidos e resultados pretendidos. Para que uma empresa possa adotar políticas estratégicas eficazes, é necessário que estas sejam baseadas em informação, que passa a ser a principal matéria-prima de qualquer organização.

Da perspectiva de uma empresa, o sistema de informação é uma solução organizacional e administrativa baseada na tecnologia de informação para enfrentar um desafio proposto pelo ambiente (Laundon e Laudon, 2004). Desta

forma, os sistemas de informação são essenciais para qualquer organização (veja a próxima figura). Ter o controle sobre este ambiente é essencial para a qualidade dos serviços prestados pela empresa.

A informação certa comunicada a pessoas certas é de importância vital para a empresa. Para a tomada de decisões, é necessários um cuidado detalhado com a integridade, precisão, atualidade, interpretabilidade e valor geral da informação.

Classificação das Informações

Nem toda informação é crucial ou essencial a ponto de merecer cuidados especiais. Por outro lado, determinada informação pode ser tão vital que o custo de sua integridade, qualquer que seja, ainda será menor que o custo de não dispor dela adequadamente. Em (Wadlow, 2000; Abreu, 2001; Boran, 1996) é exposto, a necessidade de classificação da informação em níveis de prioridade, respeitando a necessidade de cada empresa assim como a importância da classe de informação para a manutenção das atividades da empresa:

- **Pública** – informação que pode vir a público sem maiores consequências danosas ao funcionamento normal da empresa, e cuja integridade não é vital;
- **Interna** – o acesso a esse tipo de informação deve ser evitado, embora as consequências do uso não autorizado não sejam por demais sérias. Sua integridade é importante, mesmo que não seja vital;
- **Confidencial** – informação restrita aos limites da empresa, cuja divulgação ou perda pode levar a desequilíbrio operacional, e eventualmente, perdas financeiras, ou de confiabilidade perante o cliente externo, além de permitir vantagem expressiva ao concorrente;
- **Secreta** – informação crítica para as atividades da empresa, cuja integridade deve ser preservada a qualquer custo e cujo acesso deve ser restrito a um número bastante reduzido de pessoas. A manipulação desse tipo de informação é vital para a companhia.

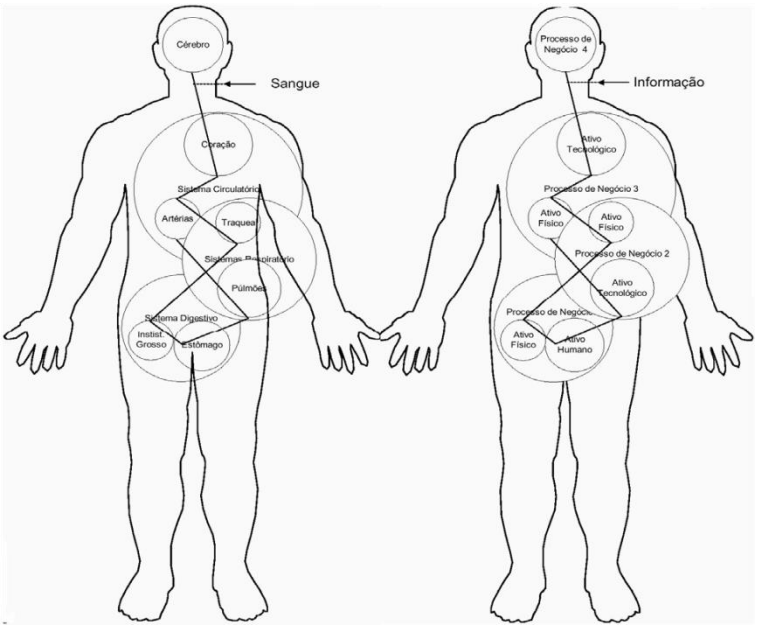
Entretanto, independentemente da relevância ou tipo da informação, a gestão dos dados organizacionais é estratégica, pois possibilita o apoio para a tomada de decisões em qualquer âmbito institucional. Algumas informações são centrais para organização e a divulgação parcial ou total destas pode alavancar um número de repercussões cuja complexidade pode ser pouco ou nada administrável pela organização com consequências possivelmente nefastas.

O conceito de engenharia da informação – que é um conjunto empresarial de disciplinas automatizadas, dirigindo ao fornecimento da informação correta para a pessoa certa no tempo exato (Martin, 1991; Feliciano Neto, Furlan e Higo, 1988) – já demonstrava a importância da segurança da informação para as instituições.

Conforme (Crosby, 1992), a qualidade dos processos custa dinheiro, mas a falta dela custa muito mais. Estabelecendo uma analogia, a segurança custa dinheiro mas a sua ausência poderá custar muito mais.

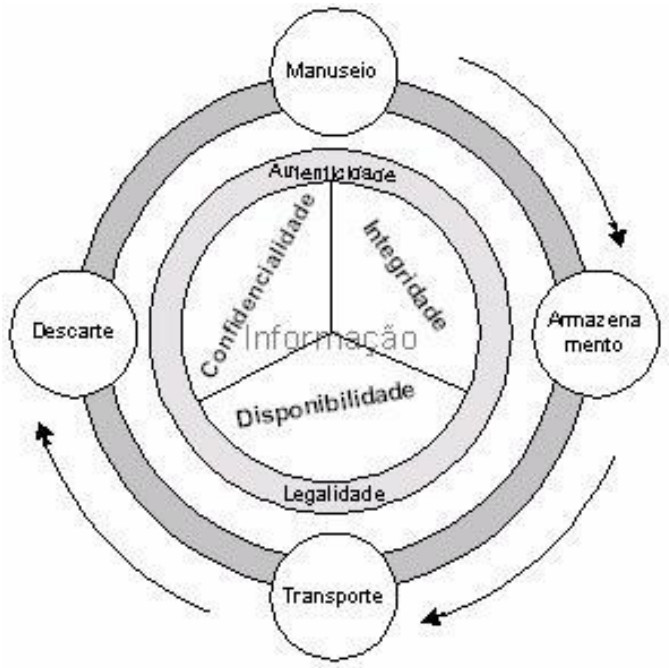
Ciclo de Vida da Informação

O Ciclo de Vida é composto e identificado pelos momentos vividos pela informação que a colocam em risco. Os momentos são vivenciados justamente quando os ativos físicos, tecnológicos e humanos fazem uso da informação, sustentando processos que, pos sua vez, mantêm a operação da empresa. A próxima figura demonstra uma relação entre o corpo humano e o negócio de uma empresa.



Os órgãos (analogamente, ativos físicos, tecnológicos e humanos), se utilizam sangue (analogamente, informação), para pôr em funcionamento os sistemas digestivo, respiratório, etc. (analogamente, processos de negócio), para consequentemente, manter a consciência e a vida do indivíduo (analogamente, a continuidade do negócio).

Correspondendo às situações em que a informação é exposta a ameaças que colocam em risco suas propriedades, atingindo a sua segurança, a próxima figura revela todos os 4 momentos do ciclo de vida que são merecedores de atenção.



- **Manuseio** – Momento em que a informação é criada e manipulada, seja ao folhear um maço de papéis, ao digitar informações recém-geradas em uma aplicação Internet, ou, ainda, ao utilizar sua senha de acesso para autenticação, por exemplo.
- **Armazenamento** – Momento em que a informação é armazenada, seja em um banco de dados compartilhado, em uma anotação de papel posteriormente postada em um arquivo de ferro, ou, ainda em uma mídia de disquete depositada na gaveta da mesa de trabalho, por exemplo.
- **Transporte** – Momento em que a informação é transportada, seja ao encaminhar informações por correio eletrônico, ao postar um documento via aparelho de fax, ou, ainda, ao falar ao telefone uma informação confidencial, por exemplo.
- **Descarte** – Momento em que a informação é descartada, seja ao depositar na lixeira da empresa um material impresso, seja ao eliminar um arquivo eletrônico em seu computador de mesa, ou ainda, ao descartar um CDROM usado que apresentou falha na leitura.

Conceitos gerais de segurança da Informação

O termo '**segurança da informação**' agrega uma extensa disposição de atividades em uma organização. Isto inclui produtos e processos para prevenir acessos não autorizados, modificação, e exclusão de informação, conhecimento, dados e fatos.(1)

Esta área também envolve a proteção de recursos prevenindo-os de serem corrompidos em situações de ataques que podem estar além do controle de pessoas responsáveis pela segurança da informação.(2)

A partir perspectiva de um profissional em computação, você está lidando com questões que são muito maiores do que meros sistemas de proteção de vírus de computador. Você está protegendo valiosos ativos de uma organização de pessoas que está muito motivada a obter e usar estes ativos, sendo que algumas destas pessoas podem ainda estar dentro de sua organização. Felizmente, a maioria deles estará fora. (3)

Infelizmente, este trabalho não é muito fácil de fazer. Informações sobre fraquezas e vulnerabilidades em vários sistemas comerciais são bem conhecidas e documentadas. Seus adversários podem usar sistemas de pesquisa para encontrar vulnerabilidades em qualquer produto virtual ou em sistemas operacionais. Eles podem aprender como tirar proveito das susceptíveis fraquezas que existem no sistema.(4)

Segurança da informação inclui três áreas de foco primário. Estas áreas endereçam diferentes partes da segurança de um computador. Um plano de segurança de computador efetivo deve avaliar os riscos e criar estratégias e métodos que as endereçam.

Esta sessão foca nestas três áreas:(5)

I. Segurança física
II. Segurança Operacional
III. Gerenciamento e políticas

Cada uma destas áreas é vital para assegurar a segurança em uma organização. Você pode pensar sobre isto como um banco de três pernas. Se qualquer uma das três pernas do banco quebrar, você irá cair e se machucar. Você deve olhar pelo negócio em geral e levantar todas as questões que o negócio

encara e que diz respeito a segurança da informação. Figura 1.1 mostra como estes componentes de segurança de computador interagem para prover um ambiente razoavelmente seguro.(6)

Parte do seu trabalho é fazer recomendações para gerenciamento de necessidades e deficiências, tomar ações para minimizar os riscos e exposição de sua informação e sistemas, estabilidade, manter e defender a segurança dos sistemas cujo você trabalha. Esta não é uma tarefa pequena, e você deve fazer cada elemento de modo que pode ter uma chance razoável de manter a segurança de sua organização.(6)

Triângulo de Segurança

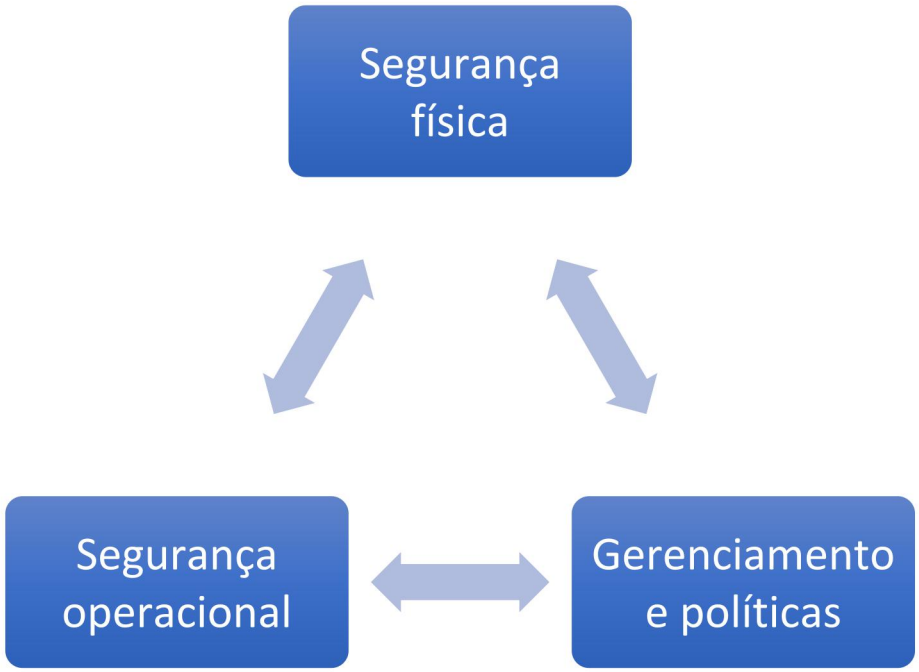


Figura 1 - Tríade de Segurança da informação -Referencia - (6)

Segurança física

Segurança física envolve a proteção de seus ativos e informação de acessos físicos de pessoas não autorizadas. Estas ameaças muitas vezes apresentam-se como técnicos de serviço, porteiros, clientes, fornecedores ou até mesmo funcionários. Eles podem furtar seu equipamento, danificar, ou pegar documentos de escritórios, latas de lixo ou arquivamento de gabinetes. Suas motivações podem ser tão simples como uma ganância ou tão complexa como um desejo de roubar seus segredos de comércio para vender para um concorrente como um ato de vingança.(6)

Segurança física é relativamente fácil de realizar. Você assegura facilidades pelo controle de acesso ao escritório, triturando documentos desnecessários, instalando sistemas de segurança e limitando acesso às áreas sensíveis do negócio. A maioria dos edifícios de escritórios fornecem perímetros e passagem de segurança durante o tempo em que o local não está ocupado.(7)

O primeiro componente da segurança física envolve fazer uma localização física do que é um alvo menos tentador. Se o escritório ou edifício em que você

está é aberto a toda equipe, obter acesso para dentro do negócio no prédio é fácil. Você deve impedir as pessoas de verem sua organização como um alvo tentador. Bloqueando portas e instalando vigilância ou sistemas de alarmes que podem fazer uma localização física até de um alvo menos desejável. Bastantes alvos escancarados envolvendo menos riscos por parte das pessoas envolvidas estão disponíveis. Tente fazer que seu escritório não interesse a ninguém.(3)

O segundo componente da segurança física envolve de uma penetração ou furto. Você quer saber o que está quebrado, o que está perdido e como esta perda ocorreu. Sistemas passivos de videoteipes são uma boa maneira de fazer isso. A maioria dos ambientes de varejo rotineiramente gravam áreas-chave do negócio para identificar como furtos ocorreram e como os fizeram. Estas gravações são admissíveis como evidências em muitas cortes judiciais. A aplicação da lei deve ser envolvida tanto quando ocorre uma infiltração ou um furto.

O terceiro da segurança física envolve consiste em recuperação a partir de um furto ou perda de um sistema ou informação crítica. Como a organização irá recuperar a partir de uma perda e retornar ao estado normal de negócio? Se um vândalo destruir a sua sala de servidores, em quanto tempo sua organização poderia levar para voltar a operação e produção total?

Segurança operacional

Segurança operacional trata de como sua organização faz as coisas. Isto inclui computadores, networks e sistemas de comunicação tão bem como o gerenciamento da informação. Segurança operacional engloba uma grande área, e como um profissional de segurança você será envolvido nesta área.

Ativos da segurança operacional incluem controle de acesso, autenticação e topologias de segurança após a instalação de rede estar completa. Ativos operacionais incluem o dia a dia da operação de redes, conexões de outras redes, planos de backup e planos de restauração. Em suma, segurança operacional engloba tudo o que não é relacionado a projeto ou segurança física em sua rede. As questões que você trata em uma capacidade operacional podem parecer exageradas de primeira vista. Muitas das áreas que você irá abordar são vulnerabilidades, fraqueza ou políticas de segurança inadequadas nos sistemas que você usa, por exemplo.

I. Programar uma política de expiração de senha inteligente, você poderia solicitar aos usuários a trocar suas senhas a cada 30 ou 60 dias.

II. Solicitar a rotação de senha.

III. Solicitar senhas complexas

IV. Controlar a quantidade de logins (tentativas e sucessos)

Sua rede corporativa, quando conectada a internet, se torna uma vulnerabilidade em potencial. Você pode instalar hardwares e softwares para melhorar a segurança, mas o gerenciamento pode decidir se estas medidas custam muito mais para implementar. Novamente, operacionalmente podem existir coisas pequenas que você pode fazer para isto.

Gestão e políticas

Gestão e políticas fornecem direção, regras e procedimentos para implementação de um ambiente de segurança. Políticas, para ser eficaz, deve ter apoio integral e intransigente da equipe de gestão da organização. Orientações da gestão fornecem iniciativas de segurança na raiz de onde necessitam ser eficaz. Profissionais de segurança da informação podem recomendar políticas, mas eles precisam do apoio da gestão para implementá-las. Não há nada pior do que uma segurança autoproclamada “czar” sem o apoio da gestão.

As questões que devem ser decididas em nível de gestão e de política afetam toda a empresa e podem ter grande impacto na produtividade, moral e cultura corporativa. Políticas também estabilizam pretensões sobre ativos de segurança relatados. Estas políticas devem ser tratadas de uma forma não diferente de férias, licença médica ou rescisão de uma organização. Muitas pessoas podem dizer exatamente quantos dias de férias eles tiram por ano; contudo, muitos não sabem dizer quais são as políticas de segurança ou algumas informações de tratamento.

O número de chaves de políticas é necessário para assegurar a rede. A lista abaixo identifica algumas áreas que requerem pensamento e planejamento:

1. Políticas de Administração

Políticas administrativas apresentam sugestões e expectativas para atualizações, monitoramento, backups e auditorias. Administradores de sistemas e manutenção de usuários usam disso para conduzir o negócio. As políticas devem delinear claramente quantas vezes e quando as atualizações aparecem, quando e como ocorre monitoramento, análises e de registro.

As políticas devem ser específicas o suficiente para ajudar a manter o pessoal administrativo focado no negócio para executar os sistemas e redes. Ao mesmo tempo, têm de ser suficientemente flexível para permitir a emergências e imprevistas em certas circunstâncias.

2. Requisitos de projeto

Requisitos de projeto delinear são as capacidades que do sistema devem ter. Estes requisitos são normalmente parte do projeto inicial e afetam muito as soluções que você pode usar. Muitos vendedores irão responder a cada lance e assegurar-lhe que eles são seguros. Você pode usar os requisitos para beneficiar fornecedores explicar e propor soluções. Esta política deve ser muito específica sobre requisitos de segurança. Se seu projeto não inclui a segurança como parte integrante da implementação, pode apostar que a sua rede tem vulnerabilidades.

3. Planos de recuperação de desastres

Planos de recuperação de desastres (DRP) são uma das maiores dores de cabeça que os profissionais de TI enfrentam. A DRP é cara para desenvolver, caro para testar e caro para manter atualizada. A maioria das grandes empresas investem enormes quantias em DRP incluindo backup ou hot sites. Um hot site é uma facilidade que é projetada para fornecer disponibilidade imediata em caso de falha de um sistema ou rede.

A probabilidade que uma organização realmente necessite de um hot site é relativamente pequena e pode parecer sem importância, até o momento em que você realmente necessite de um.

O DRP leva em consideração praticamente todos os tipos de ocorrência ou possíveis falhas. Ela pode ser tão simples como se um único sistema fosse falhar, ou tão complicado como a necessidade de recuperar uma grande empresa multinacional de um desastre cataclísmico.

4. Políticas de Informação

Políticas de informação referem-se aos vários aspectos da segurança da informação. Isso inclui acesso, classificação de marcação e de armazenamento para transmissão e destruição de informações confidenciais. O desenvolvimento de políticas de informação é fundamental para a segurança.

5. Políticas de Segurança

Políticas de segurança definem como a configuração dos sistemas e rede de ser. Isso inclui a instalação de conexões de software, hardware e rede. Políticas de segurança também definir como identificação e autorização (I & A) ocorre, e quem determina o controle de acesso, auditoria e rede conectividade. Criptografia e software antivírus são normalmente cobertos nestas políticas. As políticas de segurança também estabelecer procedimentos e métodos utilizados de expiração de senha conta, seleção, tentativas de logon e áreas afins.

6. Políticas de Uso

Políticas de uso agregam como a informação e os recursos são utilizados. Você precisa explicar aos usuários como eles podem usar os recursos organizacionais e para que finalidades. Essas políticas estabelecer a lei sobre o uso de computador. Uso políticas incluem declarações sobre a privacidade, a propriedade e consequências de atos impróprios. Suas políticas de uso devem explicar claramente as expectativas de uso sobre a Internet e e-mail.

7. Gestão de políticas de usuário

Gestão de políticas de identifica as várias ações que devem ocorrer no curso normal das atividades dos funcionários. Estas políticas devem abordar como novos empregados são adicionados ao sistema. A política deve abordar a formação e orientação, instalação de equipamentos, e bem como sua configuração. Transferência de trabalhadores é uma parte normal de uma empresa. Se um empregado é transferido para um novo emprego, os privilégios e acesso que tinha da antiga posição podem ser inadequados para a nova posição. O estabelecimento de um novo acesso e novos direitos permite que o empregado continue a trabalhar. Se você se esquecer de revogar os privilégios anteriores, este usuário pode ter acesso a mais informações do que eles precisam. Com o tempo, isso pode resultar numa situação chamada privilégio de fluência. O usuário pode adquirir privilégios administrativos do sistema por acidente. Funcionários demitidos representam uma ameaça à segurança da informação. Em alguns casos, um funcionário demitido pode pedir para ter acesso ao banco de listas de clientes, contas, ou outras informações confidenciais. É imperativo que os empregados que deixam a empresa terem suas contas desativadas ou excluídas, e o acesso desligado. Você ficaria surpreso com quantas vezes a administradores de sistemas não sabem

sobre mudanças de pessoal. Seu gerenciamento de políticas de usuários deve indicar rapidamente e notificar o departamento de TI sobre rescisões de funcionários e quando ela ocorre.

Definições

I. Segurança da informação.
II. Incidente de segurança.
III. Ativo.
IV. Ameaça.
V. Vulnerabilidade.
VI. Risco.
VII. Ataque.
VIII. Impacto.

1. Definição de segurança da informação

Segurança da Informação compreende a proteção das informações, sistemas, recursos e demais ativos contra desastres, erros (intencionais ou não) e manipulação não autorizada, objetivando a redução da probabilidade e do impacto de incidentes de segurança.

Segundo a norma ABNT NBR ISO/IEC 27002:2005, a segurança da informação é a proteção da informação de vários tipos de ameaças para garantir a continuidade do negócio, minimizando os riscos e maximizando o retorno sobre os investimentos e as oportunidades de negócio.

2. Como É Obtida A Segurança Da Informação

A segurança da informação é obtida como resultado da implementação de um conjunto de controles, compreendendo políticas, processos, procedimentos, estruturas organizacionais e funções de hardware e software. Em particular, os controles necessitam ser estabelecidos, implementados, monitorados, analisados e continuamente melhorados, com o intuito de atender aos objetivos do negócio e de segurança da organização. A identificação de controles adequados requer um planejamento detalhado.

Outras definições:

1. Incidente de segurança

corresponde a qualquer evento adverso relacionado à segurança; por exemplo, ataques de negação de serviços (Denial of Service – DoS), roubo de informações, vazamento e obtenção de acesso não autorizado a informações.

2. Ativo

qualquer coisa que tenha valor para a organização e para os seus negócios. Alguns exemplos: banco de dados, softwares, equipamentos (computadores, note- books), servidores, elementos de redes (roteadores, switches, entre outros), pessoas, processos e serviços.

3. Ameaça

qualquer evento que explore vulnerabilidades. Causa potencial de um inci- dente indesejado, que pode resultar em dano para um sistema ou organização (vide item 2.18 ABNT NBR ISO/IEC 27002:2007).

4. Vulnerabilidade

qualquer fraqueza que possa ser explorada e comprometer a segurança de sistemas ou informações. Fragilidade de um ativo ou grupo de ativos que pode ser explorada por uma ou mais ameaças (vide item 2.17 ABNT NBR ISO/IEC 27002:2007). Vulnerabilidades são falhas que permitem o surgimento de deficiências na segurança geral do computador ou da rede. Configurações incorretas no computador ou na segurança também permitem a criação de vulnerabilidades. A partir desta falha, as ameaças exploram as vulnerabilidades, que, quando concretizadas, resultam em danos para o computador, para a organização ou para os dados pessoais.

5. Risco

combinação da probabilidade (chance da ameaça se concretizar) de um evento ocorrer e de suas consequências para a organização. Algo que pode ocorrer e seus efeitos nos objetivos da organização.

6. Ataque

qualquer ação que comprometa a segurança de uma organização.

7. Impacto

consequência avaliada de um evento em particular.

Infraestrutura organizacional para a segurança da informação

Seção 6 da norma ABNT NBR ISO/IEC 27002:2005 –

Organizando a segurança da informação.

I. Importância da infraestrutura.

II. Atribuição de responsabilidades.

III. Coordenação da segurança da informação.

Neste tópico serão apresentados os aspectos relevantes para o estabelecimento de uma infraestrutura de apoio à segurança da informação nas organizações. Em especial serão tratadas a razão da importância da infraestrutura, a relevância da atribuição de responsabilidades e questões relacionadas à coordenação.(8)

8. Importância da infraestrutura

Fornece todas as condições para a gestão da segurança da informação na organização. Uma recomendação é definir uma estrutura de gerenciamento para controlar a elabo- ração e implantação da segurança da informação.

Para garantir a segurança da informação em determinada organização, deve-se atentar para a necessidade do estabelecimento de uma infraestrutura que propicie o seu gerenciamento. Inicialmente, é válido definir uma estrutura de gerenciamento própria para o controle da implantação da segurança da informação. (8)

Em particular, se for o caso, é relevante a contratação de consultoria especializada com o propósito de elaborá-la e implantá-la na organização. (8)

9. Atribuição de responsabilidades

I. Deve-se atribuir responsabilidades de acordo com a política de segurança.

II. Funcionários podem delegar tarefas de segurança da informação, mas não podem delegar responsabilidades.

III. Se necessário, é preciso instituir o cargo de gestor de segurança da informação.

Preocupações:

I. Áreas de responsabilidade.

Responsabilidades dos funcionários.

Processos a serem implementados.

Atribuir responsabilidades é uma atividade considerada crucial para a segurança da informação, devendo ser realizada de acordo com a política de segurança da informação da organização. (8)

Funcionários (ou pessoas em determinados cargos) que possuam responsabilidades definidas formalmente na política de segurança podem delegar atividades relacionadas diretamente à segurança da informação, todavia não se eximindo das responsabilidades. Sendo assim,

é relevante que, nos casos de delegação, os funcionários que delegam a atividade avaliem se esta está sendo realizada conforme a política de segurança, legislação e normas vigentes. (8)

Para cada ativo e procedimento de segurança da informação, é importante atribuir responsabilidades a um funcionário (ou cargo). Em outras palavras, o funcionário (ou cargo) deverá efetuar a gestão do ativo ou procedimento segundo determinação da política de segurança.

Dependendo do tamanho e das vulnerabilidades da organização, pode-se estabelecer o cargo de gestor da segurança da informação, que responde, em primeira instância, pela segurança global da organização e ainda auxilia no desenvolvimento da política de segurança e define a estratégia para a sua divulgação, exigindo seu cumprimento por todos. Ao gestor, cabe estar sempre atualizado em relação aos problemas, riscos e soluções de segurança; selecionar os mecanismos de segurança mais adequados aos problemas de segurança específicos da organização; e verificar a adequação da política de segurança, mecanismos e procedimentos de segurança da informação adotados. (8)

Coordenação da segurança da informação

Compreende a colaboração entre partes, como dirigentes, funcionários, auditores, consultores etc.

O Objetivos da coordenação são os seguintes:

I. Aprovar metodologias e procedimentos de segurança da informação.

II. Assegurar a conformidade com a política de segurança.

III. Coordenar a implantação de controles.

IV. Educar para a segurança da informação.

Para a efetividade da segurança da informação em uma organização, seus dirigentes devem montar uma equipe multidisciplinar (dirigentes e funcionários de vários departamentos, por exemplo) para coordenar as atividades necessárias. Se necessário, pode-se também instituir um comitê específico. (8)

Em particular, recomenda-se que a coordenação atue nas seguintes atividades:

I. Avaliar e aprovar metodologias e procedimentos necessários à segurança da informação;

II. Controlar todos os procedimentos, com o intuito de assegurar a conformidade com a política de segurança da organização;

III. Coordenar a implantação de controles de segurança da informação, tais como medidas contra acessos não autorizados;

IV. Divulgar adequadamente para toda a organização os procedimentos, os controles e a política de segurança. Lembre-se sempre de que a conscientização das pessoas pode ser considerada tão relevante quanto o uso de outros mecanismos de segurança baseados em tecnologia. (8)

Tratamento de ativos

Seção7 da norma ABNT NBRISO/ IEC27002:2005– Gestãodeativos.

I. Proteção de ativos.
II. Inventário de ativos.
III. Proprietário de ativo.

Uma vez que os ativos são elementos essenciais para o negócio das organizações, este tópico apresenta os aspectos primordiais a serem considerados. Serão apresentadas as preocupações com a proteção dos ativos e dos procedimentos recomendados, para fins de gestão de ativos e recuperação após desastres: inventário e designação de proprietário para cada ativo da organização. (8)

Proteção dos ativos

Ativos são elementos essenciais ao negócio da organização.

Ativos devem ser inventariados.

Todo ativo deve ter um responsável por manter sua segurança.

Os ativos da organização são elementos importantes para o negócio; sendo assim, sua proteção adequada deve ser estabelecida e mantida. (8)

Exemplos:

I. Equipamentos;
II. Bases de dados;
III. Serviços de iluminação;
IV. Acordos;
V. Procedimentos de suporte técnico;
VI. Trilhas de auditoria;
VII. Aplicativos;
VIII. Sistemas de informação;
IX. Pessoas;
X. Imagem comercial da organização.

Para tal proteção, são recomendados dois procedimentos: **inventariar** os ativos e **associar a cada um deles um proprietário**, responsável pela manutenção de sua segurança. (8)

A seguir, serão apresentados mais detalhes a respeito de cada procedimento.

Inventário de ativos

O inventário é essencial para recuperação após desastres e compreende:

I. Identificar ativos.

II. Catalogar ativos.

III. Manter o catálogo.

No inventário de ativos, deve-se estruturar e manter os ativos devidamente identificados. Na identificação, as informações relevantes tipicamente são: o tipo do ativo, configuração, sua criticidade para os negócios da organização, localização, informações sobre o tratamento de backups e licenças. Ainda no inventário, deve-se identificar o proprietário de cada ativo e a classificação da informação, quando cabível. (8)

Em casos de recuperação após desastres, o inventário de ativos representa um dos itens essenciais para sua efetividade. E, para a gestão de riscos, o inventário é uma premissa.

Proprietário de ativo

Aquele que é o responsável autorizado sobre o(s) ativo(s).

Proprietário não é dono do ativo!

Atividades:

I. Garantir a classificação dos ativos.

II. Definir e analisar, periodicamente, as restrições de acesso aos ativos.

O proprietário de um ativo é o responsável pela manutenção da sua segurança, efetuando, então, atividades como:

I. Garantir a classificação adequada dos ativos;

II. Definir e analisar, periodicamente, as restrições de acesso ao ativo.

São exemplos de proprietários de ativos o gerente de RH (Recursos Humanos) da organização, responsável por documentos específicos, e o desenvolvedor responsável por sua estação de trabalho. Vale ressaltar que, se necessário e cabível, pode-se atribuir ao gestor da segurança da informação a responsabilidade por determinados ativos,

principalmente aqueles diretamente relacionados à segurança da informação, como a própria política de segurança. (8)

Exemplo: Inventário do ativo “base de dados”.

Tipo: dados.

Criticidade para os negócios: alta.

Localização: sala de servidores da organização.

Tratamento de backup: incremental e diário.

Proprietário: administrador do banco de dados.

Este exemplo apresenta algumas **informações a respeito do ativo** “base de dados” de uma organização. Pode-se observar que:

O tipo considerado é “dados”. A classificação de ativos pode variar de uma organização para outra; todavia, tipicamente pode-se categorizar em hardware, software, dados, documentação etc.

A criticidade do ativo é considerada alta, visto que os dados são essenciais ao negócio da organização. Pode-se associar a criticidade atribuída segundo as categorias utilizadas na análise/avaliação de riscos para a organização. Para exemplificar, pode-se classificar ativos como de alta, moderada ou baixa criticidade.

A localização do ativo é a sala de servidores da organização, visto que se trata de uma base de dados armazenada em um banco de dados.

O tratamento de backup aplicado ao ativo é incremental e diário. Para todos os ativos é relevante indicar a política de backup para fins de gestão de incidentes, em particular. Para fins de conhecimento, a política pode determinar, de acordo com o grau de criticidade do ativo, o backup completo ou incremental e seu período (mensal, quinzenal, semanal ou diário, por exemplo).

O responsável pela segurança do ativo. No caso, o administrador do banco de dados da organização.

Modelo de ataques de segurança da informação

Há quatro modelos de ataque possíveis:

1. Interrupção

quando um ativo é destruído ou torna-se indisponível (ou inutilizável), caracterizando um ataque contra a disponibilidade. Por exemplo, a destruição de um disco rígido.

2. Interceptação

quando um ativo é acessado por uma parte não autorizada (pessoa, programa ou computador), caracterizando um ataque contra a confidencialidade. Por exemplo, cópia não autorizada de arquivos ou programas.

3. Modificação

quando um ativo é acessado por uma parte não autorizada (pessoa, programa ou computador) e ainda alterado, caracterizando um ataque contra a integridade. Por exemplo, mudar os valores em um arquivo de dados.

4. Fabricação

quando uma parte não autorizada (pessoa, programa ou computador) insere objetos falsificados em um ativo, caracterizando um ataque contra a autentici- dade. Por exemplo, a adição de registros em um arquivo.

Na Figura 2, observamos o fluxo normal da informação de uma origem para um destino (a). Na sequência, o esquema apresenta cada um dos modelos de ataques possíveis: uma interrupção (b), interceptação (c), modificação (d) e fabricação (e).

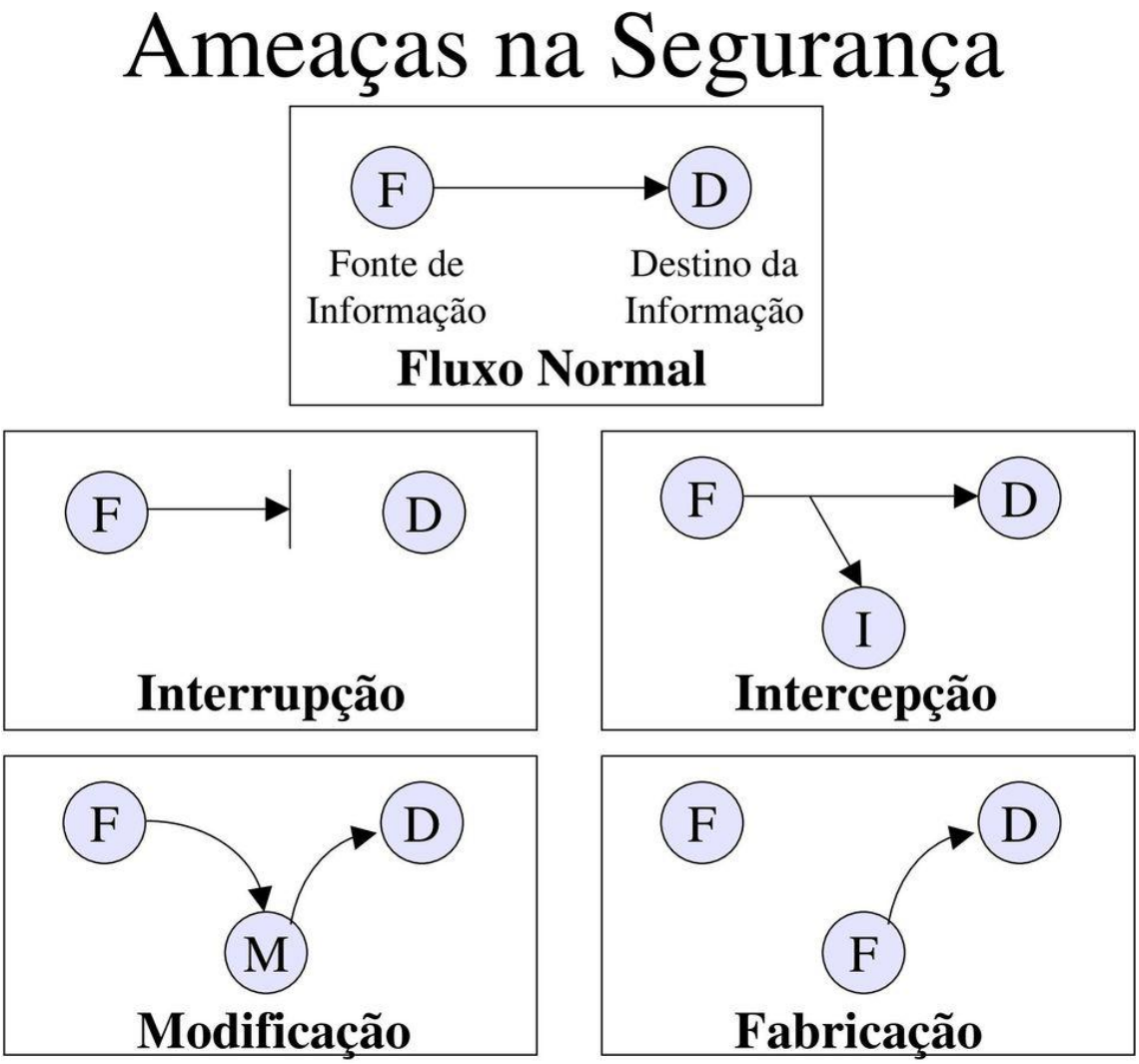


Figura 2 - Tipos de Ataques de Segurança da informação- Referencia (9)

1. Ataques ativos:

Resultam na alteração ou destruição dos dados.

O ataque é um ato deliberado de tentar se desviar dos controles de segurança com o objetivo de explorar as vulnerabilidades. Existem as seguintes formas de ataque:

envolvem modificação de dados, criação de objetos falsificados ou negação de serviço, e possuem propriedades opostas às dos ataques passivos. São ataques de difícil prevenção, por causa da necessidade de proteção completa de todas as facilidades de comunicação e processamento, durante o tempo todo. Sendo assim, é possível detectá-los e aplicar uma medida para recuperação de prejuízos causados.

2. Ataques passivos

São os ataques baseados em escutas e monitoramento de transmissões, com o intuito de obter informações que estão sendo transmitidas. A escuta de uma conversa telefônica é um exemplo desta categoria.

Ataques desta categoria são difíceis de detectar porque não envolvem alterações de dados; todavia, são possíveis de prevenir com a utilização de criptografia.

Arquitetura de segurança

3. Proteção de dados contra modificações não autorizadas.

Proteger os dados contra perda / roubo / furto.

Proteção de dados contra a divulgação não autorizada.

Garantir a identidade do remetente correto dos dados.

Garantir a identidade correta do destinatário dos dados.

A arquitetura de segurança proposta pelo modelo ISA (interconexão de sistemas abertos) definido na norma ISO 7498-2 estabelece os seguintes objetivos ou requisitos de segurança:

Proteção de dados contra modificações não autorizadas.

Proteger os dados contra perda / furto / roubo.

Proteção de dados contra a divulgação não autorizada.

Garantir a identidade do remetente correto dos dados.

Garantir a identidade correta do destinatário dos dados.

Serviços de segurança

1. Objetivos:

Aumento da segurança.

Utilização de mecanismos de segurança.

2. Categorias de serviços de segurança.

Os objetivos do projeto de uma topologia de segurança têm de lidar com questões de confidencialidade, integridade, disponibilidade e responsabilidade. Abordar essas quatro questões como parte inicial de seu projeto de rede ajudará a garantir maior segurança.(15)

Você vai ver muitas vezes a confidencialidade, integridade, disponibilidade referidos como a CIA da segurança de rede. O componente de prestação de contas é igualmente importante. Os objetivos do projeto devem ainda identificar quem é responsável e por quais aspectos de segurança do computador.

As próximas seções apresentam os quatro componentes que precisam ser abordados nos objetivos do projeto para melhorar a segurança da rede e informação.

1. Confidencialidade

O objetivo da confidencialidade é evitar ou minimizar o acesso não autorizado e divulgação de dados e informações. Em muitos casos, as leis e regulamentos exigem confidencialidade de informação específica. Registros da Segurança social, folha de pagamento e registros dos empregados, registros médicos e informações corporativas são bens de alto valor. Esta informação pode, eventualmente, criar questões de responsabilidade ou constrangimento se cair em mãos erradas. Nos últimos anos, tem ocorrido uma série de casos em que a conta bancária e números de cartão de crédito foram publicados na internet. Os custos destes tipos de violação de sigilo excedem em muito as perdas reais do uso indevido dessas informações.

Se as questões de confidencialidade são abordadas no início da fase de projeto, os passos que devem ser tomados para minimizar esta exposição se tornará claro.

2. Integridade

O objetivo da integridade é certificar-se de que os dados que estão sendo trabalhados realmente estão corretos. A integridade das informações é fundamental para uma topologia da segurança. As organizações trabalham e tomam decisões com base nos dados que eles têm disponível.

disponível. Se esta informação não é precisa ou é adulterada por uma pessoa não autorizadas, as consequências podem ser devastadoras.

Tomemos o caso de um distrito escolar que perdeu toda a folha de pagamento e registros dos empregados para os funcionários do distrito. Quando o problema foi descoberto, o distrito escolar não tinha escolha a não ser enviar aplicativos e formulários a todos os funcionários pedindo-lhes quanto tempo eles tinham trabalhado no distrito escolar e quanto eles recebiam.

Como é que uma organização sabe que a informação que eles estão usando para tomar decisões está precisa e não foi adulterada ou alterada? Em alguns casos, seria quase melhor ter a informação destruída do que tê-la imprecisa. As pessoas assumem que a informação que eles estão usando é precisa. O que deve ter sido adulterado?

3. Disponibilidade

A meta de disponibilidade é para proteger os dados e prevenir a sua perda. Dados que não podem ser acessados são de pouco valor. Se um acidente ou ataque que ocorre derruba um servidor de chaves ou banco de dados, essa informação não estará disponível para as pessoas que precisam dela. Isso pode causar estragos em uma organização. Seu trabalho é fornecer o máximo de disponibilidade para seus usuários, garantindo a integridade e confidencialidade.(3)

A parte mais difícil do processo é determinar que o equilíbrio destes três aspectos deve ser mantido para garantir a segurança aceitável para a informação e os recursos da organização.

4. Responsabilidade

O objetivo final e muitas vezes esquecido do projeto é preocupação com a responsabilidade. Muitos dos recursos utilizados por uma organização são compartilhados entre vários departamentos ou individuais. Se um erro ou incidente acontece, que é responsável por corrigi-lo? Quem determina se a informação está correta ou não?

É uma boa ideia tornar claro sobre quem possui os dados ou é responsável por certificar-se do que é preciso. Você também quer ser capaz de rastrear e monitorar as alterações de dados para detectar e reparar os dados em caso de perda ou danos. A maioria dos sistemas rastream e armazenam os logs de

atividades do sistema e manipulação de dados, além de também fornece relatórios sobre problemas.

Segurança da informação e terceiros

I. A razão do tratamento diferenciado.
II. Possíveis riscos.
III. Tratamento dos clientes.
IV. Acordos específicos.
V. Gerência de serviços de terceiros.

É relevante estabelecer procedimentos adequados antes de disponibilizar acessos por parte de terceiros. Neste tópico, serão tratados o porquê do tratamento diferenciado dos terceiros e possíveis riscos envolvidos; como tratar com os clientes a respeito da manutenção de acordos específicos para o contexto e os procedimentos recomendados para a gerência de serviços terceirizados.

A razão do tratamento diferenciado

Deve-se manter a segurança de recursos e informações acessíveis a terceiros.

Acessíveis = processados, transmitidos ou gerenciados.

Considerar:

I. Possíveis riscos.
II. Acordos específicos.

Deve-se considerar um tratamento diferenciado para os recursos e informações que sejam processados, transmitidos ou gerenciados por partes externas, por exemplo, empresas prestadoras de serviço, com o objetivo de permitir tais acessos em conformidade com a política de segurança da informação vigente na organização.

Para tanto, é relevante efetuar uma análise dos potenciais riscos envolvidos e as possíveis medidas de segurança adequadas ao tratar com partes externas. Em especial, as medidas de segurança e demais critérios específicos quanto à segurança da informação devem ser definidos em acordo entre as partes.

Possíveis riscos

É preciso identificar, analisar e avaliar os riscos, e implementar medidas de segurança antes de disponibilizar o acesso a terceiros. Devem ser considerados:

I. Recursos de processamento.

II. Valor da informação.

III. Pessoas envolvidas.

IV. Práticas e procedimentos para o tratamento de incidentes de segurança.

V. Requisitos legais, regulamentares e contratuais.

No tratamento da segurança da informação em relação a terceiros, há potenciais riscos específicos. Sendo assim, é importante analisar e avaliar os riscos envolvidos diretamente com os acessos externos, aplicando as medidas de segurança adequadas antes de disponibilizar o acesso.

A seguir, são apresentados alguns dos principais aspectos a considerar para o contexto:

I. Identificar os recursos aos quais terceiros podem ter acesso;

II. Indicar o tipo de acesso a cada recurso;

III. Conhecer o valor e a criticidade das informações disponibilizadas a terceiros;

IV. Aplicar medidas de segurança condizentes aos riscos para cada informação acessada por terceiros;

V. Considerar as pessoas que poderão acessar a informação no lado dos terceiros;

VI. Implantar práticas e procedimentos para o tratamento de incidentes de segurança;

VII. Considerar os requisitos legais, contratuais e regulamentares aplicáveis ao contexto.

1. Exemplo de regras para tratamento de terceiros:

“Não é permitida a revelação de identificação, autenticação e autorização de uso pessoal ou uso de recursos autorizados por intermédio de tais itens por parte de terceiros.”

“Não é permitido o fornecimento de informações a terceiros a respeito dos serviços disponibilizados na organização, exceto os de natureza pública ou mediante autorização de equipe/gestor competente.”

Neste exemplo, são apresentadas regras de tratamento das informações e serviços por parte de terceiros, cujo objetivo é demonstrar a aplicação de procedimentos formais com vistas à segurança da informação.

Tratamento dos clientes

Deve-se identificar todos os requisitos de segurança antes de disponibilizar o acesso aos clientes. Preocupações:

I. Proteção dos ativos.
II. Descrição detalhada do produto/serviço a ser fornecido.
III. Políticas de controle de acesso.
IV. Responsabilidades legais.

Ao tratar com clientes, a organização deve identificar, antecipadamente, todos os requisitos de segurança diretamente relacionados ao acesso externo a ativos e informações. Sendo assim, recomenda-se:

2. Proteger os ativos e indicar ações corretivas em casos de comprometimento;

I. Descrever, em detalhes, o produto/serviço a ser fornecido;
II. Considerar as políticas de controle de acesso vigentes;
III. Indicar as responsabilidades legais da organização e do cliente.

Acordos de confidencialidade específicos

Deve-se considerar a segurança da informação ao estabelecer acordos com terceiros. Considerar, pelo menos:

I. Política de segurança.
II. Medidas de segurança aplicadas ao ativo envolvido.
III. Treinamento de funcionários.
IV. Atribuição de responsabilidades.
V. Processo para gestão de mudanças.
VI. Classificação da informação disponibilizada.

Nos acordos, os requisitos de segurança devem ser contemplados a fim de assegurar o conhecimento e cumprimento deles por parte de terceiros.

3. Nos acordos deverá considerar:

I. A política de segurança da informação vigente;
II. O uso de medidas de segurança para a proteção de ativos;

III. Treinamento e conscientização das pessoas em termos da segurança da informação e suas responsabilidades;

IV. Processo claro de gerência de mudanças;

V. Políticas de controle de acesso;

VI. Direito de efetuar auditoria;

VII. Requisitos para a continuidade de serviços;

VIII. Responsabilidades legais, contratuais e regulamentares aplicáveis.

Inclusive, devem ser definidos acordos de confidencialidade, de modo que os requisitos de segurança contemplados expressem as necessidades da organização quanto ao valor das informações para o negócio.

Esses acordos protegem a informação, ao passo que determinam as responsabilidades dos envolvidos quanto à proteção, uso e divulgação das informações da organização. Sendo assim, os acordos de confidencialidade podem ser estabelecidos entre a organização e terceiros, e entre a organização e seus funcionários.

Em organizações nas quais a gestão da segurança da informação for terceirizada, os acordos devem estabelecer detalhes a respeito do modo como os terceiros garantirão a segurança atendendo a obrigações legais e aos requisitos do negócio.

Gerência de serviços de terceiros

Serviços disponibilizados e acordos com terceiros devem ser monitorados. Boas práticas:

4. Considerar a segurança da informação ao elaborar acordos de entrega de serviços.

I. Disponibilizar soluções técnicas para monitoramento.

II. Monitorar e analisar serviços entregues e logs.

III. Gerenciar mudanças nos serviços.

Os serviços terceirizados em determinada organização devem ser gerenciados com o propósito de garantir adequação aos requisitos de segurança da informação e aos negócios. Sendo assim, os acordos estabelecidos entre a organização e terceiros devem ser gerenciados e controlados adequadamente. Práticas apropriadas:

Deve-se considerar medidas de segurança, níveis de serviço e requisitos de entrega de serviços ao elaborar os acordos de entrega de serviços terceirizados. Tais acordos devem ser verificados para que os requisitos de segurança acordados sejam cumpridos;

I. É relevante dispor de soluções técnicas e recursos suficientes para monitorar os acordos e requisitos de segurança estabelecidos;

II. Deve-se monitorar e analisar regularmente serviços e logs fornecidos por terceiros;

III. Deve-se gerenciar as mudanças em termos de serviços terceirizados, considerando melhorias possíveis, atualizações de políticas, estabelecimento de novos controles de segurança e uso de novas tecnologias, por exemplo.

Exemplo:

1 Cláusula contratual – Segurança da informação.

"A CONTRATADA obriga-se a utilizar programas de proteção e segurança da informação que busquem evitar qualquer acesso não autorizado aos seus sistemas, seja em relação aos que eventualmente estejam sob sua responsabilidade direta, seja através de link com os demais sistemas da CONTRATANTE ou, ainda, por utilização de e-mail."

Objetivos da Segurança da Informação

As metas de segurança da informação são muito simples. Estes objetivos definem uma estrutura para o desenvolvimento e manutenção de um plano de segurança. Eles são fáceis de expressar, mas difícil de realizar. Estes objetivos são os seguintes:

1. Prevenção

Prevenção refere-se a prevenir que violações do computador ou informações ocorram. Violações de segurança são também referidos como incidentes. Quando ocorre um incidente, o resultado de um colapso pode estar nos procedimentos de segurança. Incidentes de todas as formas e tamanhos. Incidentes simples incluem coisas como a perda de uma senha ou deixar um terminal conectado durante a noite. Eles podem também ser completamente envolvidos e resultarem no envolvimento do pessoal de locais de aplicação da lei ou federais. Se um grupo de hackers atacar e derrubar o site, você consideraria isso um grande incidente. Na teoria,

seus procedimentos e políticas de segurança o fariam invulnerável a um ataque. Infelizmente, este não é geralmente o que acontece. Melhorando suas políticas de prevenção, menor será a probabilidade de sucesso de um ataque.

2. Detecção

Detecção refere-se à identificação de eventos quando eles ocorrem. Detecção é um problema muito difícil em muitas situações. Um ataque em seu sistema pode ocorrer durante um longo período de tempo antes que seja bem sucedido. Detecção de um incidente envolve a identificação dos ativos sob ataque, como ocorreu, e por quem. O processo de detecção pode envolver uma variedade de ferramentas importantes ou um simples exame dos arquivos de log do sistema. Atividades de detecção devem ser partes contínuas de suas políticas de segurança da informação e procedimentos.

3. Resposta

Resposta se refere ao desenvolvimento de estratégias e técnicas para lidar com um ataque ou perda. Desenvolvimento de uma resposta adequada a um

incidente envolve vários fatores. Se o incidente foi uma sonda, o atacante pode reunir informações de inteligência sobre a rede ou sistemas. Estes tipos de ataques podem ser aleatórios ou direcionados. Eles geralmente causam poucos danos. Invariavelmente, porém, um ataque será bem sucedido. Quando isso acontece, será útil ter um plano bem pensado e testado para responder, restaurar a operação, e neutralizar a ameaça. É sempre melhor ter um conjunto de procedimentos e métodos na mão para se recuperar de um incidente do que tentar "criar" uma resposta e acertar precisamente.

Essas metas são uma parte importante de estabelecer padrões para uma organização. Você não pode permitir que essas políticas ou metas tornem-se insignificantes. Se você faz, você e sua organização estão se preparando para uma surpresa. Infelizmente, a surpresa não será agradável, e pode ter muito custo para corrigir.

O Processo de Segurança

Você precisa pensar sobre este negócio de segurança inteiro como uma combinação de processos, procedimentos e políticas. A segurança da informação envolve fatores humanos e técnicos. Os fatores humanos são abordados pelas políticas que são aplicadas na organização. Os componentes de tecnologia incluem as ferramentas que você instala em sistemas com os quais você trabalha. Tem várias partes neste processo, e cada um é descrito nas seções seguintes.

1. Software antivírus

Os vírus de computador é uma das tendências mais irritantes que acontecem hoje. Parece que quase toda semana alguém inventa um novo vírus para danificar sistemas. Alguns desses vírus não fazem nada mais do que dar-lhe um grande “Te peguei”, outros destroem sistemas, redes de contaminar e causar estragos em sistemas de computador. (10)

O negócio de fornecimento de software para usuários de computador para protegê-los tem de tornar-se grande na indústria. Existem vários fornecedores muito bons e bem estabelecidos de software antivírus.

Métodos de proteção de novos vírus entram em cena quase tão rápido quanto os novos vírus. Software antivírus examina a memória do computador, arquivos do disco, e de entrada e saída de e-mail. O software utiliza normalmente um arquivo de definição de vírus que é atualizada regularmente pelo fabricante.

Felizmente, esses arquivos de definição de vírus são normalmente atualizados a cada duas semanas ou mais. Se esses arquivos são mantidos atualizados, o sistema do computador vai ser relativamente seguro. Infelizmente, a maioria das pessoas não os mantém atualizados. Usuários vão reclamar que um novo vírus foi detectado. Após o exame, você vai descobrir que, na maioria dos casos, o seu arquivo de definição de vírus do mês está desatualizado. Como você pode ver, o sistema pode ser derrubado se os arquivos de definição não são atualizados regularmente.(5)

Controle de acesso

O processo de estabelecimento de controle de acesso é crítico. Controle de acesso define como os usuários e os sistemas se comunicam. O controle de acesso protege a informação de acesso não autorizado. Três modelos básicos são utilizados para explicar o controle de acesso. Vamos olhar para cada um nas seguintes seções.(11)

2. Controle de Acesso Obrigatório

O Controle de acesso obrigatório (MAC) é um modelo estático que usa um conjunto predefinido de privilégios de acesso a arquivos no sistema. Os administradores de sistema estabelecer esses parâmetros e os associa a uma conta, arquivos ou recursos. O modelo MAC pode ser muito restritivo. Em um modelo de MAC, administradores estabelecem o acesso. Os administradores também são as únicas pessoas que podem alterar o acesso. Os usuários não podem compartilhar recursos de forma dinâmica, a menos que a estática de relacionamento já existe.(11)

3. Controle de Acesso Discricionário

O modelo de Controle de acesso discricionário (DAC) permite que o proprietário de um recurso estabeleça privilégios para as informações que possuem. O modelo DAC seria permitir que um usuário compartilhasse um arquivo ou usar um arquivo que alguém tenha compartilhado. O modelo DAC estabelece uma lista de controle de acesso (ACL) que identifica os usuários que têm autorização para essa informação. Isso permite que o proprietário conceda ou revogue o acesso a indivíduos ou grupos de indivíduos dependendo da situação.

Este modelo é de natureza dinâmica e permite que a informação seja compartilhada facilmente entre os usuários.(11)

4. Controle de Acesso Baseado em Hierarquia

Função baseada de controle de acesso modelo (RBAC) permite que um usuário a agir de uma determinada maneira predeterminada com base no cargo que o usuário ocupa na organização. Os usuários podem ser atribuídos a sistema de certos papéis. O utilizador pode executar certa função ou direito baseado no papel que eles são atribuídos. Um exemplo disso pode ser uma função chamada "vendedor". O vendedor pode acessar apenas as informações que são estabelecidas para esse papel. Eles podem ser capazes de acessar estas informações a partir de qualquer estação da rede, com base estritamente na função. (11)

O modelo RBAC é muito comum em funções administrativas em uma rede. Para fazer backup de arquivos de dados em computadores, privilégios limitados são necessários. Estes privilégios são atribuídos a uma pessoa chamada de operador de backup. O backup operador só tem acesso aos direitos ou privilégios predefinidos para esse papel.

Autenticação

Autenticação prova que o usuário ou o sistema é realmente quem eles dizem ser. Uma das partes mais críticas do sistema de segurança é a autenticação. Este é parte de um processo que é também referida como de identificação e autenticação (I A). O processo de identificação começa quando um ID de usuário ou nome é digitada em uma tela de login. (12)

A autenticação é realizada por desafiar a afirmação sobre quem está acessando o recurso. Sem autenticação, ninguém pode pretender ser qualquer um. (12)

Sistemas de autenticação ou métodos baseiam-se em um ou mais de entre eles três fatores:

5. Algo que você sabe - uma senha ou PIN

6. Algo que você tem - um cartão inteligente ou um dispositivo de identificação

7. Algo que você é - suas impressões digitais ou padrão da retina

Sistemas também autenticam um ao outro usando métodos semelhantes. Frequentemente sistemas vão passar informações privadas entre si para estabelecer a identidade. Uma vez que a autenticação ocorreu, dois sistemas podem comunicar-se nas formas previstas no projeto. Existem vários métodos comuns de autenticação. Cada um deles tem vantagens e desvantagens que devem ser consideradas quando se avalia a autenticação de sistemas ou métodos. (12)

Nome de usuário / senha

Um nome de usuário e senha são identificadores únicos para um processo de logon. Quando usuários se sentar na frente de um computador, a primeira coisa que um sistema de segurança exige é que eles estabelecem quem são. (12)

A identificação é tipicamente confirmada através de um processo de logon. A maioria dos sistemas operacionais usa um ID de usuário e senha para fazer isso. (12)

O processo de início de sessão identifica a operação do sistema e, possivelmente, a rede, que você é quem você diz ser a figura 3 ilustra esse processo de logon e senha.

Note que o sistema operacional compara esta informação com a informação armazenada do processador de segurança e aceita ou nega a tentativa de logon.

O sistema operacional pode estabelecer privilégios ou permissões com base em armazenados dados sobre esse ID particular. (12)

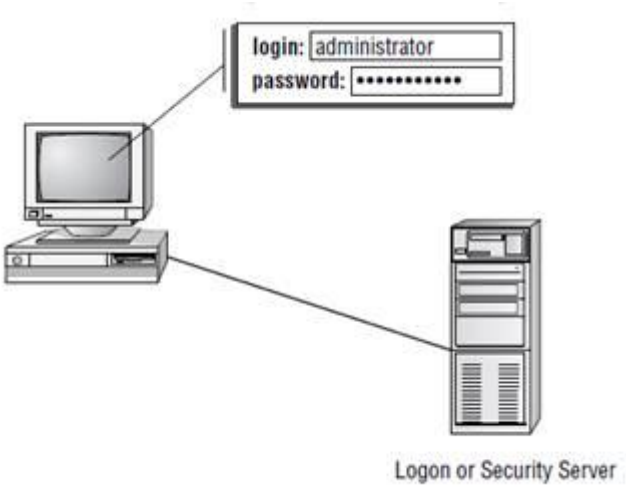


Figura 3 - Processo de Logon ocorrendo em uma estação de trabalho – Referencia (13)

Challenge Handshake Authentication Protocol (CHAP)

CHAP é um protocolo que solicita um sistema para verificar a identidade.

CHAP não usa um ID de usuário / mecanismo de senha. Em vez disso, o iniciador envia um pedido de início de sessão a partir do cliente para o servidor. O servidor envia uma solicitação para o cliente. A solicitação é criptografada e enviado de volta para o servidor. O servidor compara o valor do cliente e se os resultados de informação, os subsídios de servidores e autorização. Se a resposta falhar, a sessão de falha e a fase de solicitação começa de novo a figura 4 ilustra o procedimento CHAP. Este método handshake envolve três passos e é normalmente automática entre sistemas.

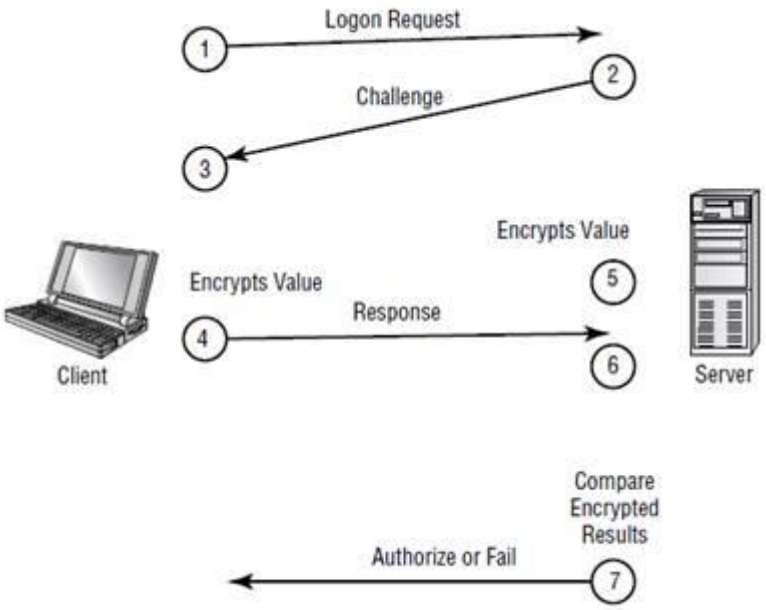


Figura 4 - Autenticação CHAP - Referencia (7)

Certificados

Certificados são outra forma comum de autenticação. Um servidor ou certificado autoridade pode emitir um certificado que será aceito pela solicitação do sistema. Os certificados podem ser tanto dispositivos de acesso físico, tais como cartões inteligentes, ou certificados eletrônicos que são usados como parte do processo de logon. Uma maneira simples de pensar neles é o crachá para acesso as salas na escola. A figura 5 ilustra um certificado sendo entregues a partir do servidor para o cliente uma vez a autenticação foi estabelecida. Se você tem um passe livre, você pode passear pelos corredores da escola. Se o seu passe é inválido, o monitor de corredor pode enviar para o escritório do diretor.

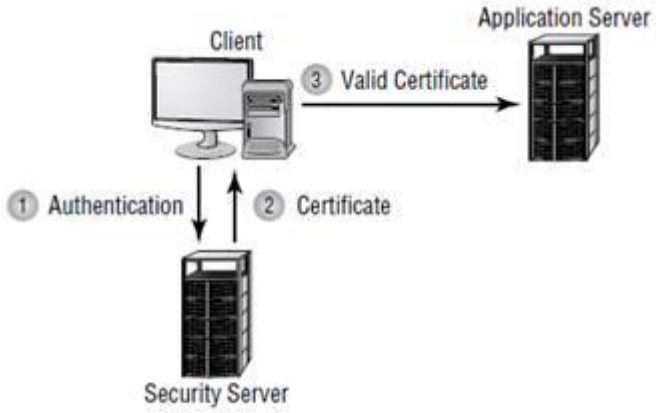


Figura 5 - Certificado sendo emitido uma vez que a identificação foi verificada – Referencia (5)

8. Tokens de segurança

Tokens de segurança são semelhantes aos certificados. Tokens de segurança contêm os direitos e privilégios de acesso do portador como parte do token. Muitos sistemas operacionais geram um token que é aplicado a cada ação tomada no sistema de computador. Se o seu token não lhe conceder acesso a determinadas informações, que a informação vai ou não ser exibida, ou o seu acesso será negado. O sistema de autenticação cria um token cada vez que um usuário começa uma sessão. Em a realização de uma sessão, o token é destruído. A figura 6 mostra uma segurança token que contém a identificação de logon e privilégios de acesso.

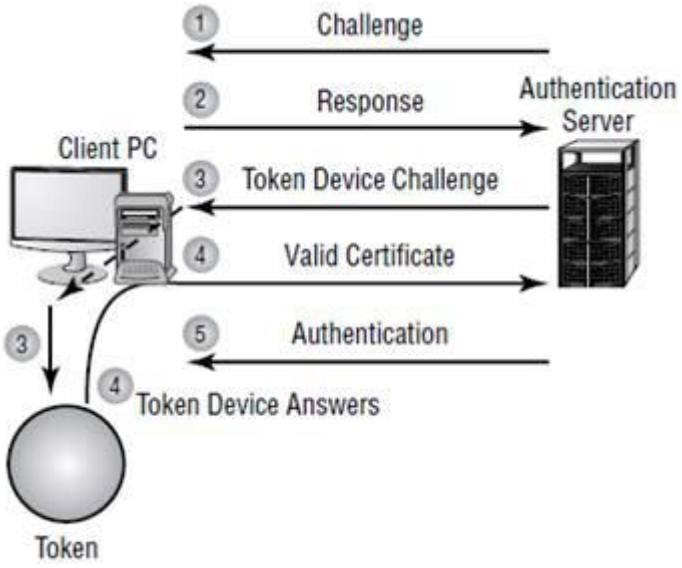


Figura 6 - Token de Autenticação de Segurança – Referencia (10)

Kerberos

Kerberos é um protocolo de autenticação relativamente novo. Originalmente concebido pelo MIT, Kerberos está se tornando muito popular como um método de autenticação. (7)

Kerberos permite a um único login em uma rede distribuída. O processo de autenticação Kerberos usa um Centro de distribuição de Chaves para orquestrar todo o processo. O KDC autentica o princípio. Princípios podem ser usuários, programas ou sistemas. O KDC proporciona um bilhete para o princípio. Uma vez que este bilhete é emitido, ele pode ser usado para autenticar relação a outros princípios. Isso ocorre automaticamente quando um pedido ou serviço é realizado por outro princípio. Kerberos está crescendo em popularidade e provavelmente vai se tornar comum padrão em ambientes de rede ao longo dos próximos anos. A única significativa fraqueza de Kerberos é que o KDC é um ponto único de falha. Se o KDC vai para baixo, o processo de autenticação irá parar. Figura 1.7 mostra o processo de autenticação Kerberos e o bilhete que está sendo apresentado para sistemas que são autorizadas pelo KDC. (7)

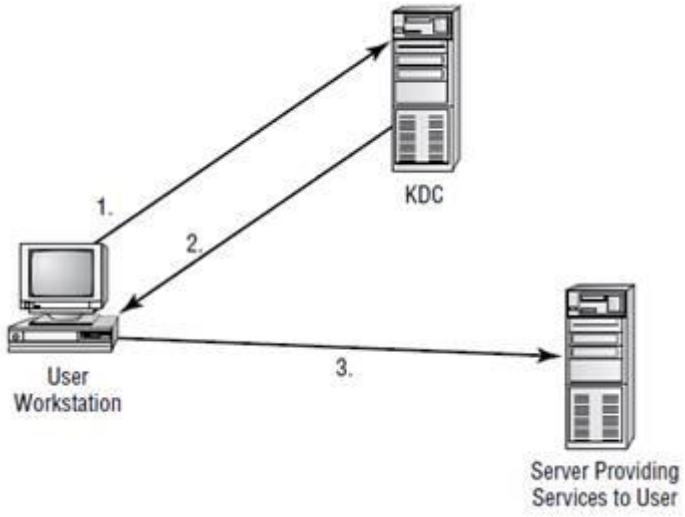


Figura 7 - Processo de Autenticação Kerberos – Referência. (7)

Processo de segurança Multi-Fator

Quando dois ou mais destes métodos de acesso são incluídos como uma parte do processo de autenticação, você está implementando um sistema multi-fator. Há sistemas que utilizam cartões inteligentes e senhas é referido como um fator de dois sistemas de autenticação. Autenticação de dois fatores é mostrada na figura 8. Este exemplo requer tanto um cartão inteligente e um processo senha de logon.

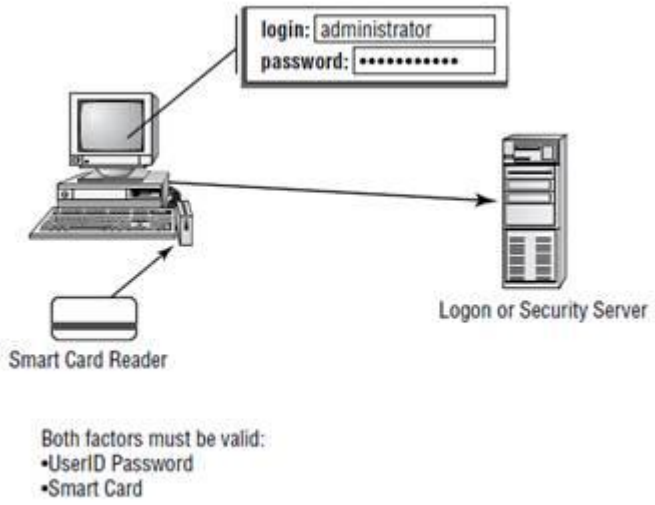


Figura 8 - Dois fatores de Autenticação – Referencia (6)

Smart Cards

Um cartão inteligente é um tipo de crachá ou cartão que pode permitir o acesso a múltiplos recursos, incluindo edifícios, estacionamentos e computadores.

Cada zona ou computador terá um leitor em que você pode inserir o cartão ou ser digitalizado. Este cartão contém informações sobre a sua identidade, acesso e privilégios. Figura 8 mostra um usuário inserir um cartão inteligente em um leitor, e ele verifica a identidade. O leitor está ligado à estação de trabalho e valida contra o sistema de segurança. Isto aumenta a segurança do processo de autenticação, porque você deve estar na posse física do cartão inteligente para usar os recursos. É claro que, se o cartão se torna perdido ou roubado, a pessoa que encontrar o cartão terá acesso aos recursos permitidos pelo cartão inteligente.(6)

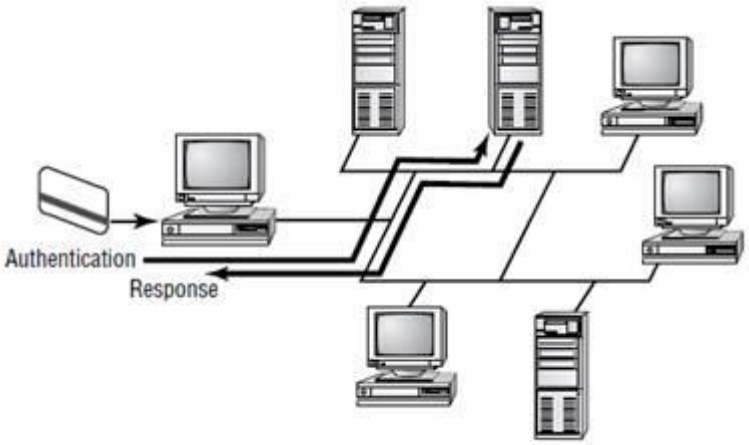


Figura 9 - Processo de Autenticação de Cartão Inteligente – Referencia (6)

Biometria

Dispositivos biométricos usam características físicas para identificar o usuário. Eles são cada vez mais comuns no ambiente de negócios. Os sistemas biométricos incluem scanners de mão, scanners de retina, e scanners que, em breve, possivelmente serão de DNA. E para ter acesso aos recursos, você deve passar por um processo de triagem física. No caso de um scanner de mão, o que podem existir são impressões digitais, cicatrizes e marcas reais na sua mão. Scanners de retina comparam padrão da retina de seu olho a um padrão armazenado na retina para verificar a sua identidade. Scanners de DNA examinarão uma parcela única de sua estrutura de DNA, a fim de verificar se você é quem você diz que é. (6)

Questões práticas

Você pode configurar vários parâmetros e padrões diferentes para forçar as pessoas em sua organização para se conformar. Ao estabelecer esses parâmetros, é muito importante que você considere a capacidade das pessoas que trabalharão com essas políticas. (6)

Se você estiver trabalhando em um ambiente onde as pessoas não têm experiência com computadores, você pode passar um bom tempo ajudando as pessoas se lembram e recuperar senhas. Muitas organizações tiveram que reavaliar suas diretrizes de segurança depois que eles já passaram por grandes custos e comprimentos para implementarem sistemas de alta segurança. (6)

Multi-fator de autenticação e segurança

O proprietário da empresa deve tornar-se cada vez mais preocupado com a segurança do computador e a displicência dos usuários. Ela relata que os usuários devem regularmente sair do escritório no final do dia, sem a assinatura de fora de suas contas. A empresa está tentando ganhar um contrato de trabalho com o governo, que vai exigir que tomem medidas adicionais de segurança.

O que você sugere para o proprietário?

A melhor sugestão seria a de considerar a implementação de um fator multi-sistema de autenticação. Este sistema pode consistir em um cartão inteligente a um logon/processo senha. Leitores de cartões inteligentes podem ser configurados para exigir que o cartão deva permanecer inserido no leitor enquanto o usuário está logado. Se o cartão inteligente for removido, por exemplo, no final do dia, a estação de trabalho do usuário seria automaticamente deslogada. Ao exigir um logon/senha, você pode ainda proporcionar uma segurança mais razoável se o smart card for roubado. Esta solução fornece uma segurança razoável, e não de forma significativa aumenta os custos de segurança. O governo provavelmente irá requerer o controle de acesso adicional, tais como alarmes de perímetro e de controle de acesso físico a áreas sensíveis. Estas medidas, no entanto, não vão forçar os usuários a sair quando saem de suas estações de trabalho.

Serviços e Protocolos

Muitos serviços e protocolos estão disponíveis para os usuários de computador utilizar. Protocolos de correios Web, e outros estão disponíveis para facilitar a comunicação entre os sistemas. Cada protocolo ou serviço que existe de um computador a rede abrirá vulnerabilidades, aumentando os problemas potenciais de segurança. Todos os dias alguém encontra uma nova vulnerabilidade comumente usados em serviços e protocolos de sistemas de computação e de rede.

Protocolos e serviços comuns

Se o ambiente é como a maioria, você terá de oferecer vários protocolos para seus usuários. Alguns dos protocolos mais comuns que você deve oferecer incluem e-mail, a Web, acesso à Internet, e alguns protocolos de controle. Ofertar estes serviços é normal em um ambiente habilitado para Internet:

E-mail

A maioria dos clientes deseja ativar sistemas de correio eletrônico para uso em uma organização. Isso significa que o seu plano de segurança deve incluir suporte para e-mail de tráfego. Isso inclui correio de entrada e saída. Várias portas são usadas no processo de e-mail.

Web

Muitas empresas estão a implementar estratégias baseadas na web para comunicações. Estas estratégias incluem um produto baseado em servidor, e um baseado em cliente do produto (um navegador). Navegadores podem se comunicar

com os serviços usando várias portas. Essas portas permitem que a informação seja enviada e recebida pelo cliente ou servidor.

Telnet é um serviço que permite que os usuários remotos acessem usando um sistema de emulação de terminal. Telnet é cada vez menos comum hoje em dia, mas é ainda usado em larga escala. Conexões Telnet geralmente são inseguros e desprotegido.

Protocolo de Transferência de Arquivo (FTP) é um protocolo de transferência de arquivos usado extensivamente na Internet. Sessões de FTP não são criptografadas. Muitos protocolos FTP implementados não criptografam o logon ou senhas no início da sessão.

Protocolo de rede de nova transferência (NNTP) permitem aos empregados acessar servidores de notícias na Internet. Isto é, conseguir enviar e receber mensagens para os servidores que armazenam para USENET encaminhar as mensagens. Existem mais de 14.000 fóruns em uso para Usenet. Estes fóruns são chamados newsgroups.

Sistema de Nome de Domínio (DNS) é usado para resolver nomes de sistemas para endereços da Internet. É um serviço muito comum e em uso na maioria das redes. Se você tem um site para anunciar seus produtos ou serviços, o DNS permite que você diga a usuários externos em que o servidor está localizado. DNS traduz endereços da web, como www.sybex.com, para endereços TCP/IP, tais como 192.168.0.110.

Protocolo de Controle de Mensagem (ICMP) O Protocolo de Controle de Mensagem fornece ferramentas de mensagens de rede, como Ping. O Ping é um utilitário que permite verificar se um sistema está acessível ou não. O ICMP torna muitos aspectos da comunicação mais fácil no ambiente da Internet.

Protocolos e Serviços não essenciais

Muitas redes suportam muitos protocolos e serviços de informação de acesso. Protocolos não essenciais devem ser desativados ou desligados. Isto inclui serviços e protocolos que são inerentemente inseguros. Abaixo está uma lista parcial de serviços que não devem ser oferecidos na rede:

Serviços NetBios
UNIX RPC
NFS
Serviços X
Serviços R, tais como rlogin e rexec
Telnet
FTP
TFTP (Protocolo de Transferência de Arquivo Trivial)
Netmeeting
Sistemas de controle remoto
SNMP (Protocolo Simples de Gerenciamento de Rede)

Esses protocolos não são recomendados porque eles enviam senhas sem criptografia através da rede, possuem pouca ou nenhuma capacidade de segurança, ou expõe o sistema a vulnerabilidades por causa da própria natureza das atividades que desempenham. (14)

Topologias de Segurança

A topologia de segurança de sua rede define o projeto da rede e implementação de uma perspectiva de segurança. Ao contrário de uma topologia de rede, estamos mais preocupados com os métodos de acesso, segurança e tecnologias a Topologia de Segurança abrange quatro áreas principais de preocupação:

1. Objetivos do projeto
2. Zonas de segurança
3. Tecnologias
4. Requisitos de Negócio
5. Metas do projeto

Zonas de Segurança

O termo zona de segurança descreve métodos de projeto que isolam sistemas de outros sistemas ou redes. Ao discutir as zonas de segurança em uma rede, é útil pensar sobre eles como quartos.

Você pode ter alguns quartos em sua casa ou escritório que qualquer um pode entrar. Você terá outras salas onde o acesso é limitado a indivíduos específicos para fins específicos. Estabelecer as zonas de segurança é um processo similar em uma rede. As zonas de segurança permitem que você isolar os sistemas de usuários não autorizados. As seções seguintes apresentam os aspectos chave da criação e concepção de zonas de segurança.(11)

6. Visão geral de Redes

Ao longo do tempo, as redes se tornaram um assunto complexo. Elas podem até mesmo parecerem ter vida própria. É comum que uma rede tenha ligações entre departamentos, empresas, países e de acesso público usando privado comunicações e caminhos através da Internet. Todos em uma rede não

precisam ter acesso a todos os ativos na rede. Você pode isolar cada rede usando hardware e software. Um roteador é um bom exemplo de uma solução de hardware. Você pode configurar algumas máquinas na rede para estar em um determinado intervalo de endereços e outros para estar em diferentes faixas de endereço. Esta separação faz com que as duas redes fiquem invisíveis uma para outra, a menos que um haja um roteador conectando-as. Algumas das opções mais recentes de switches de dados também permitem criar partições de redes em menores ou zonas privadas.

Aqui estão as quatro zonas de segurança mais comuns que você vai encontrar:

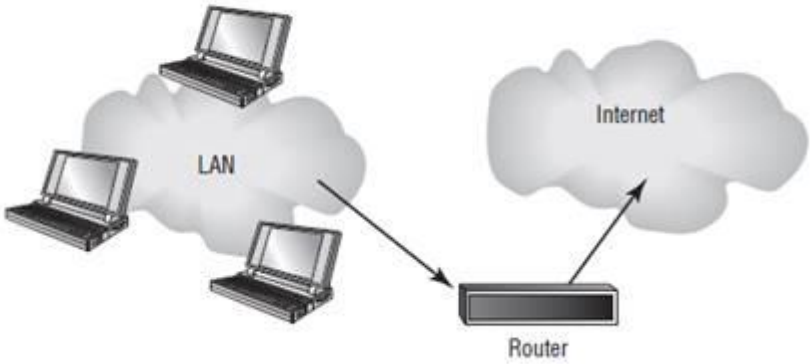
I. Internet
II. Intranet
III. Extranet
IV. DMZ

Implementando Intranets, Extranets e DMZs você pode criar um ambiente razoavelmente seguro para sua organização.

Internet

A Internet é uma rede global que conecta computadores e redes em conjunto. A Internet pode ser usada por qualquer pessoa que tenha acesso a um portal de Internet ou um provedor de serviços de Internet. A Internet é um ambiente que você deve assumir o envolvimento de um nível de baixa confiança das pessoas que a utilizam. Você deve assumir que o visitante de seu website pode ter más intenções. Eles também podem ser pessoas que querem comprar o seu produto ou contratar sua empresa.(10)

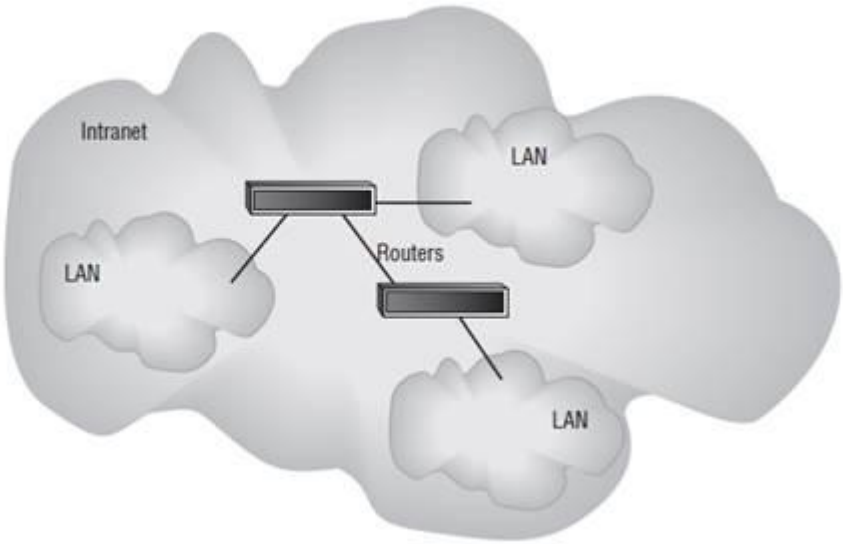
FIGURE 1.10 A typical LAN connection to the Internet



Intranet

Intranets são redes privadas implementadas e mantidas por uma empresa individual ou organização. O acesso à intranet está limitado a sistemas dentro da Intranet. Intranets utilizam as mesmas tecnologias usadas pela Internet. Intranets podem ser ligadas à Internet, mas não estão disponíveis para acesso aos usuários que não estão autorizados a fazer parte da Intranet. O acesso a Intranet é concedido a usuários confiáveis dentro da rede corporativa ou para usuários em locais remotos. A figura 1.11 mostra uma rede Intranet.

FIGURE 1.11 An Intranet network



Extranet

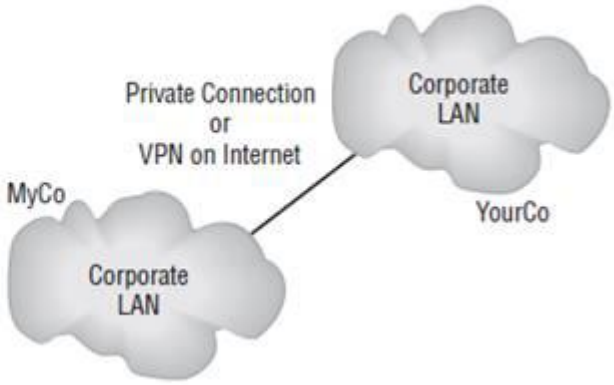
Extranets são extensões das Intranets que incluem conexões de fora para parceiros.

Uma Extranet permite você se conectar a um parceiro por uma rede privada ou

uma conexão usando um canal de comunicação seguro através da Internet.

Conexões extranet envolvem conexões que estão entre organizações confiáveis. Uma Extranet é ilustrada na Figura 1.12. Note-se que esta rede fornece uma conexão entre as duas organizações. Esta conexão pode ser feita através da Internet. Se assim for, estas redes usariam um protocolo de Tunneling para realizar uma ligação segura.

FIGURE 1.12 A typical Extranet between two organizations

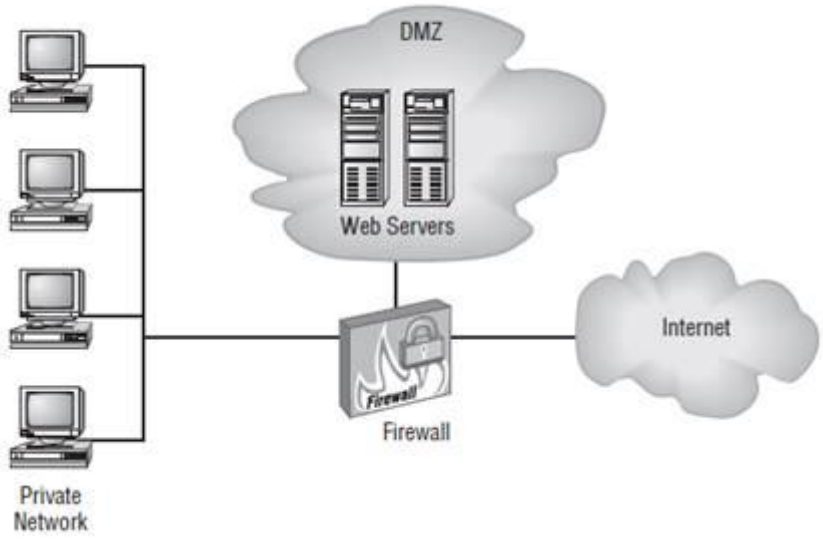


DMZ

A Zona Desmilitarizada (DMZ) é uma área onde você pode colocar um servidor público para ser acessado por pessoas que você não pode confiar. Ao isolar

um servidor em uma DMZ, você pode ocultar ou remover o acesso a outras áreas de sua rede. Você ainda pode acessar o servidor usando sua rede, mas outros não são capazes de acessar outros recursos da rede. Isso pode ser realizado usando firewalls para isolar a rede. A suposição ao estabelecer uma DMZ é que a pessoa que acessa o recurso não é necessariamente alguém que você confie com outras informações. A figura 1.13 mostra um servidor colocado em uma DMZ. Note-se que o resto da rede não está visível para os usuários externos. Isso diminui a ameaça de invasão no interior rede.

FIGURE 1.13 A typical DMZ



BACKUP

1. Backup Completo ou Full

Backup completo ou full é simplesmente fazer a cópia completa de todos os arquivos, pastas ou volumes para destinos estabelecidos como servidores, sistemas de discos ou fitas como tapes LTO e autoloaders. Embora esse tipo de backup forneça a melhor proteção contra a perda de dados, a maioria das organizações que utiliza backup em fita só utiliza esse expediente periodicamente, principalmente devido a demora para realizar o processo.

Backup Full

2. Atributo - Archive

Archive é um atributo que indica se o arquivo foi modificado desde o último backup, quando o archive é modificado, indica que não teve backup da versão mais nova, caso os backups sejam o Normal ou o Incremental, o Archive volta ao estado desmarcado.

TIPO	Arquivos com cópia de backup	Desmarca o atributo archive
Normal ou Completo	Arquivos e Pastas Selecionadas	Sim
Cópia	Arquivos e Pastas Selecionadas	Não
Diferencial	Arquivos e Pastas Selecionados que foram modificados após o último backup normal ou incremental	Não
Incremental	Arquivos e Pastas Selecionados que foram	Sim

	modificados após o último backup normal ou incremental	
Diariamente	Arquivos e Pastas Selecionados que foram modificados ao longo do dia	Não

3. Saiba mais sobre as diferenças entre backup em fita e disco.

A principal vantagem em realizar o backup full é ter uma cópia idêntica do ambiente de produção, o que facilita ao gestor de TI localizar arquivos ou pastas que porventura necessitem ser restaurados. Por outro lado, fazer a cópia completa dos dados indiscriminadamente sem nenhum tipo de verificação sempre consumirá mais espaço que o necessário, pois todas as informações serão copiadas, inclusive as que já estão armazenadas e não foram alteradas.

4. Backup incremental

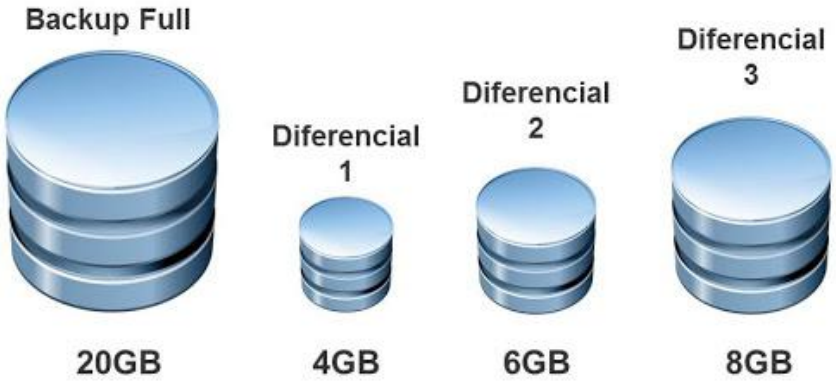
O backup incremental surgiu para sanar algumas deficiências encontradas ao realizar o backup full, como a de sempre copiar todos os dados a cada operação, mesmo que nenhuma alteração tenha sido realizada.

Além dos recursos desnecessariamente consumidos para manter diversas cópias completas dos dados, o crescimento explosivo na criação de conteúdo aumentou muito o tempo gasto para manter o backup sempre atualizado.

O primeiro passo para instituir um sistema de backup incremental é a realização da cópia completa dos dados. Assim que essa cópia for realizada, a cada nova instrução de backup o sistema verificará quais arquivos foram alterados desde o último evento e, havendo alteração, só copiará os que forem mais atuais.

Esse processo gera um fragmento de backup a cada operação, menor que a cópia completa dos dados.

As principais vantagens em usar softwares com recursos do backup incremental é que esse processo é mais rápido que o backup completo e, por gravar somente arquivos alterados, ocupa menos espaço. Por outro lado, a principal desvantagem dos backups incrementais está na demora para restauração, pois para que haja a recuperação de arquivos é necessário restaurar o último backup full e seus respectivos fragmentos incrementais subsequentes. Isso implica correr riscos, pois caso apenas um dos arquivos incrementais apresente problemas, toda a restauração estará comprometida.



5. Backup Diferencial

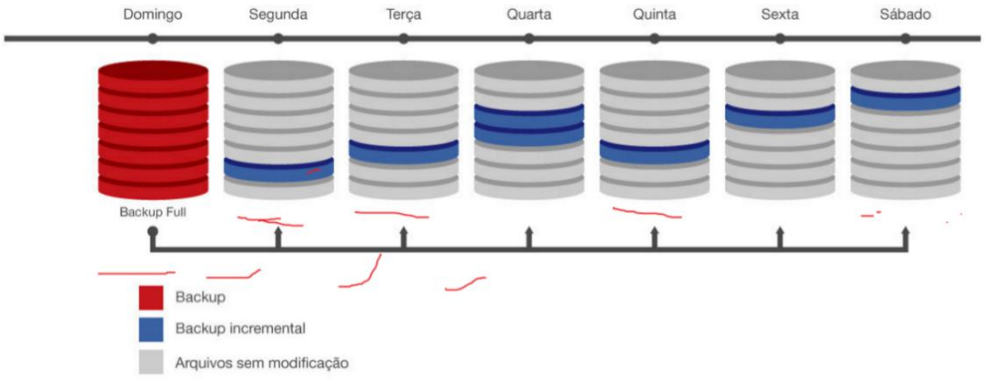
Para minimizar esse risco da perda de dados, o backup diferencial alia o conceito de economia e velocidade do backup incremental, porém com uma diferença fundamental:

Após realizar o primeiro backup completo, cada backup diferencial compara o conteúdo a ser copiado com o último backup full e copia todas as alterações realizadas.

Isso significa que uma maior quantidade de dados será gravada a cada novo backup diferencial, pois o último fragmento sempre conterá todas as diferenças entre o backup original e o volume de dados atualizado.

Esse processo é mais prático quando comparado ao incremental, pois só exigirá o backup completo e o último fragmento de backup para restauração de dados.

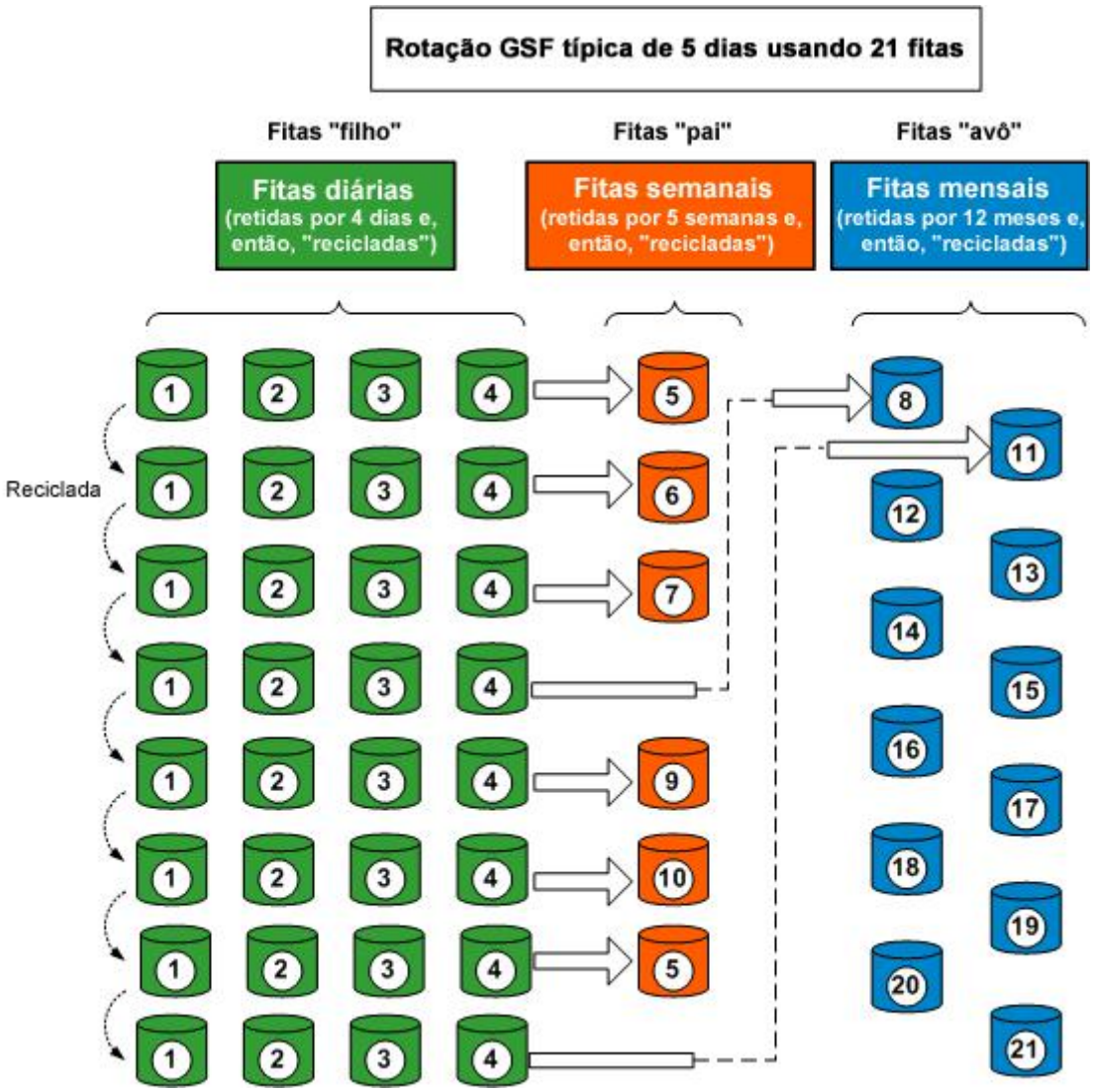
O problema desse método é que dependendo do incremento de dados da empresa, cada processo poderá gerar arquivos de backup diferenciais maiores e maiores, superando inclusive o tamanho do primeiro backup completo. Como na cópia incremental apenas as últimas modificações são registradas, a velocidade do processo é maior, pois apenas os dados alterados no último backup incremental são gravados.



6. Método de rotacionamento de fitas

MÉTODO AVÔ-PAI-FILHO

Avô-pai-filho de backup é um esquema de rotação comum para a mídia de backup, em que há três ou mais ciclos de backup, como diária, semanal e mensal. Os apoios diários são rodados diariamente usando um sistema FIFO como acima. Os backups semanais são igualmente girados em uma base semanal, e o backup mensal em uma base mensal. Além disso, trimestral, semestral e / ou backups anuais também poderia ser mantido separadamente. Muitas vezes, alguns desses backups são removidos do site para fins de custódia e recuperação de desastres.



RAID

RAID foi originalmente denominado de **"*Redundant Array of Inexpensive Drives*"** (Conjunto Redundante de Discos Baratos). Com o tempo, numa tentativa

de dissociar o conceito de "discos baratos", a indústria reviu o acrônimo para **"*Redundant Array of Independent Disks*"** (Conjunto Redundante de Discos Independentes).

RAID é um meio de se criar um subsistema de armazenamento composto por vários discos individuais, com a finalidade de ganhar segurança -- por meio da redundância de dados -- e desempenho. Popularmente, RAID seriam dois ou mais discos (por exemplo, HD ou disco rígido e até SSD) trabalhando simultaneamente para um mesmo fim, por exemplo, citando o exemplo de RAID 1 logo abaixo, serviria como um espelhamento simples, rápido e confiável entre dois discos, para se fazer uma cópia idêntica de um disco em outro.

O RAID oferece segurança e confiabilidade por meio da adição de redundância. Se um disco falhar, o outro continua funcionando normalmente e o usuário nem percebe diferença. O administrador é avisado pelo sistema e substitui o disco que falhou. Apesar disso, o RAID não protege contra falhas de energia ou erros de operação ou contra a falha simultânea dos dois discos. Falhas de energia, código errado de núcleo ou erros operacionais podem danificar os dados de forma irrecuperável. Por este motivo, mesmo usando-se o RAID não se dispensa a tradicional cópia de backup.

1. RAID 0 (Striping)

RAID-0.

No *striping*, ou distribuição, os dados são subdivididos em segmentos consecutivos (*stripes*, ou faixas) que são escritos sequencialmente através de cada um dos discos de um *array*, ou conjunto.

Cada segmento tem um tamanho definido em blocos. A distribuição, ou ***striping***, oferece melhor desempenho comparado a discos individuais, se o tamanho de cada segmento for ajustado de acordo com a aplicação que utilizará o conjunto, ou *array*.

Há problemas de confiabilidade e desempenho. RAID-0 não terá desempenho desejado com sistemas operacionais que não oferecem suporte a busca combinada de setores.

Uma desvantagem desta organização é que a confiança se torna geometricamente pior. Um disco SLED com um tempo médio de vida de 20.000 horas será 4 vezes mais seguro do que 4 discos funcionando em paralelo com

RAID 0 (admitindo-se que a capacidade de armazenamento somada dos quatro discos for igual ao do disco SLED). Como não existe redundância, não há confiabilidade neste tipo de organização.

Vantagens:

acesso rápido as informações

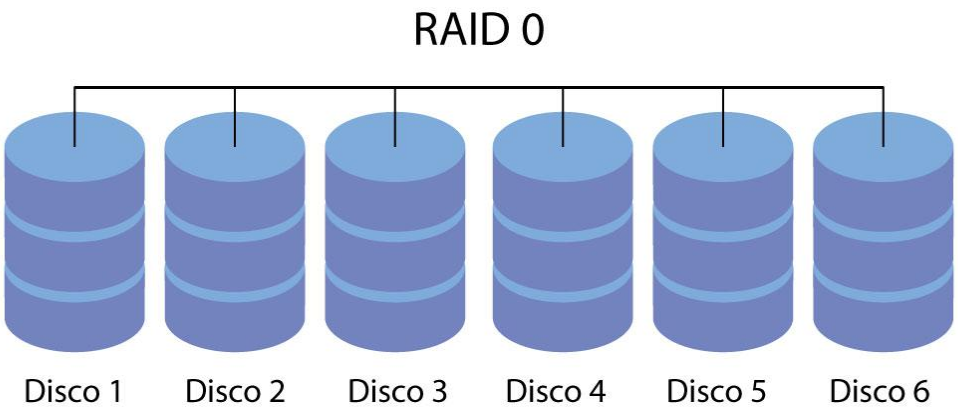
custo baixo para expansão de memória.

Desvantagens:

caso algum dos setores de algum dos HDs venha a apresentar perda de informações, o mesmo arquivo que está dividido entre os mesmos setores dos demais HDs não terão mais sentido existir, pois uma parte do arquivo foi corrompida, ou seja, caso algum disco falhe, não tem como recuperar;

não tem espelhamento;

não é usada paridade.



2. RAID 1 (Mirroring)

RAID-1 é o nível de RAID que implementa o espelhamento de disco, também conhecido como *mirror*. Para esta implementação são necessários dois discos ou mais. O funcionamento deste nível é simples: todos os dados são gravados em discos diferentes; se um disco falhar ou for removido, os dados preservados no outro disco permitem a não descontinuidade da operação do sistema.

Vantagens:

caso algum setor de um dos discos venha a falhar, basta recuperar o setor defeituoso copiando os arquivos contidos do segundo disco;

segurança nos dados (com relação a possíveis defeitos que possam ocorrer no HD).

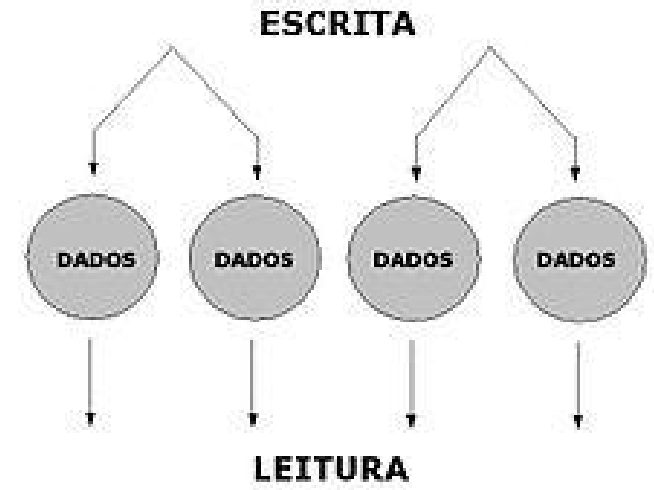
Desvantagens:

custo relativamente alto se comparado ao RAID 0;

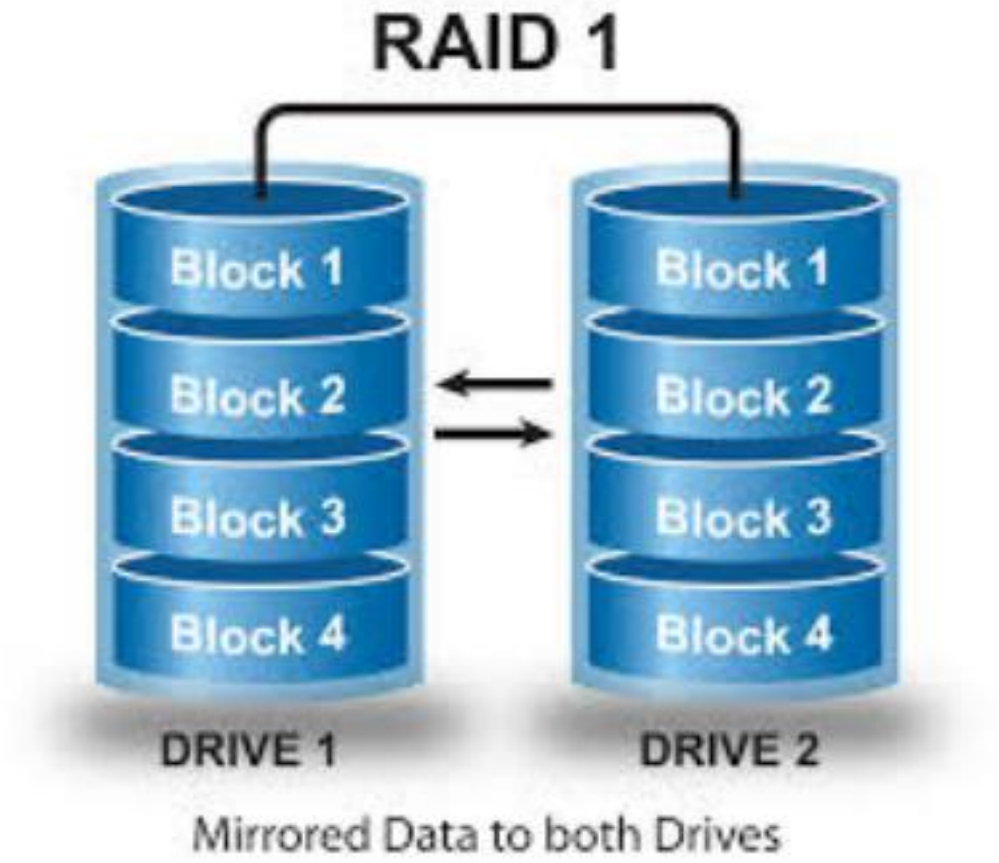
ocorre aumento no tempo de escrita;

Tem espelhamento;

não é usada paridade.



RAID-1: A escrita é feita em pares de unidades enquanto a leitura ocorre em todas as unidades ao mesmo tempo.



3. RAID 2

O RAID 2 surgiu no final dos anos 80, quando os HDs ainda não possuíam checagem de erros. Assim, pode-se dizer que o RAID 2 é similar ao RAID 0, mas possuindo algoritmos de Hamming ECC (*Error Correcting Code*), que é a informação de controle de erros, no lugar da paridade.

Além disso, pode-se ter várias configurações, como 10 discos normais + 4 discos somente para ECC. Este fato possibilita uma proteção adicional, porém o RAID 2 ficou obsoleto pelas novas tecnologias de disco já possuírem este tipo de correção internamente.

O RAID 2 origina uma maior consistência dos dados se houver queda de energia durante a escrita. Baterias de segurança e um encerramento correto podem oferecer os mesmos benefícios.

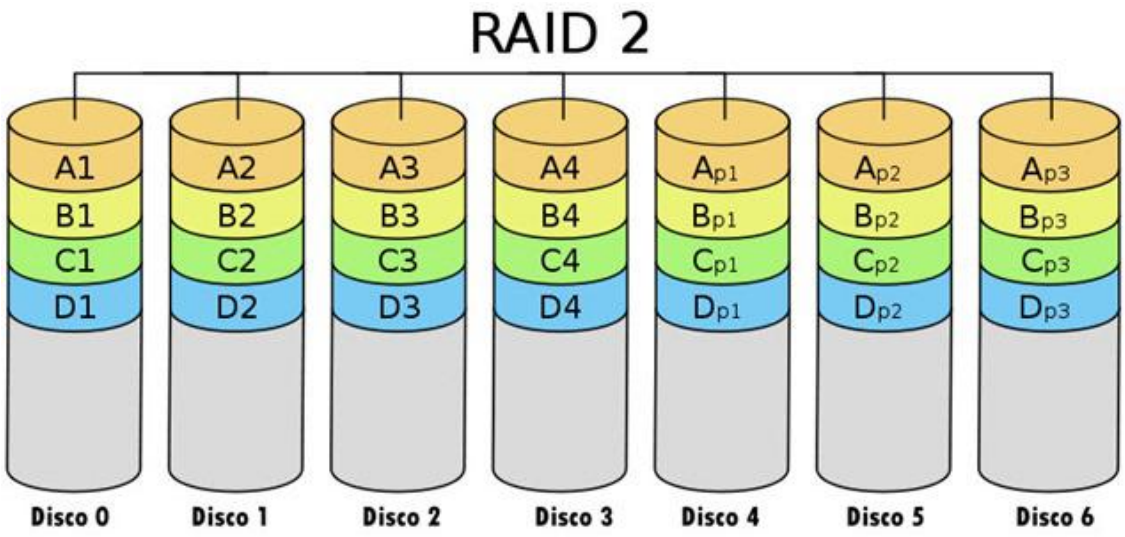
Vantagem:

usa ECC, diminuindo a quase zero as taxas de erro, mesmo com falhas de energia.

Desvantagens:

hoje em dia, há tecnologias melhores para o mesmo fim.

dependendo da configuração e necessidade da empresa, era necessário a mesma quantidade de discos ECC para discos normais, isto é, desperdício de espaço que poderia ser usado para dados.



4. RAID 3

O RAID 3 é uma versão simplificada do RAID nível 2. Nesse arranjo, um único bit de paridade é computado para cada palavra de dados e escrito em um drive de paridade. À primeira vista, pode parecer que um único bit de paridade dá somente detecção de erro, e não correção de erro.

Para o caso de erros aleatórios não detectados, essa observação é verdadeira.

Todavia, para o caso de uma falha de drive, ela provê correção total de erros de um bit, uma vez que a posição do bit defeituoso é conhecida. Se um drive falhar, o controlador apenas finge que todos os seus bits são "zeros". Se uma palavra apresentar erro de paridade, o bit que vem do drive extinto deve ter sido um "um", portanto, é corrigido.

A fim de evitar o atraso em razão da latência rotacional, o RAID 3 exige que todos os eixos das unidades de disco estejam sincronizados. A maioria das

unidades de disco mais recentes não possuem a opção de sincronização do eixo, ou se são capazes disto, faltam os conectores necessários, cabos e documentação do fabricante.

Vantagens:

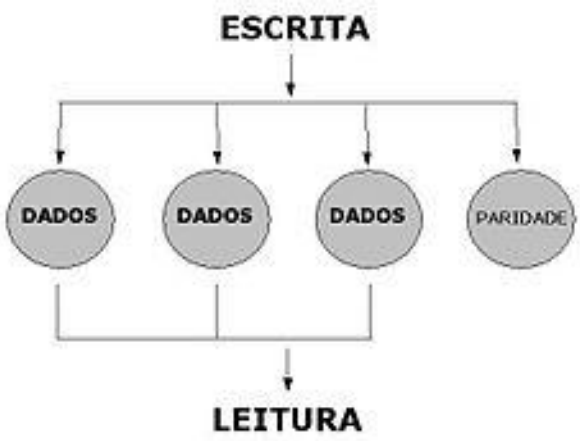
leitura rápida;

escrita rápida;

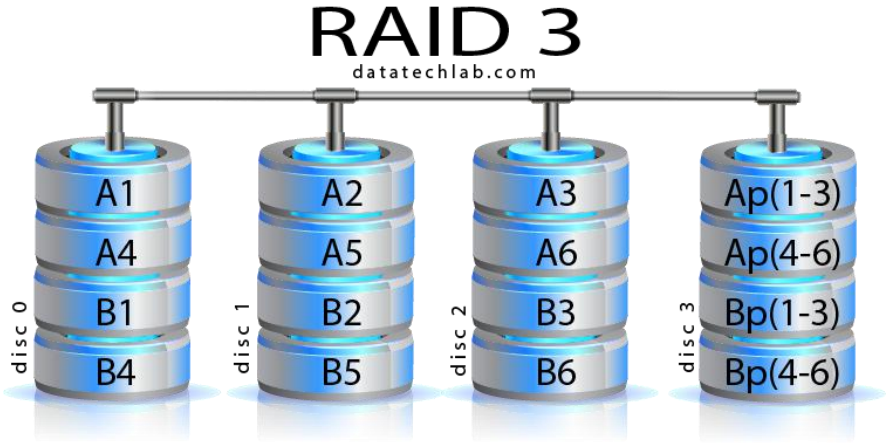
possui controle de erros.

Desvantagem:

Montagem difícil via *software*.



RAID-3: Escrita e Leitura ocorrem em todas as unidades. Mas diminui o tempo de transferência de dados.



5. RAID 4

O RAID 4 funciona com três ou mais discos iguais. Um dos discos guarda a paridade (uma forma de soma de segurança) da informação contida nos discos.

Se algum dos discos avariar, a paridade pode ser imediatamente utilizada para reconstituir o seu conteúdo. Os discos restantes, usados para armazenar dados, são configurados para usarem segmentos suficientemente grandes (tamanho medido em blocos) para acomodar um registro inteiro. Isto permite leituras independentes da informação armazenada, fazendo do RAID 4 um *array* perfeitamente ajustado para ambientes transacionais que requerem muitas leituras pequenas e simultâneas.

O RAID 4 assim como outros **RAID'**s, cuja característica é utilizarem paridade, usam um processo de recuperação de dados mais envolvente que *array*s espelhados, como RAID 1. Este nível também é útil para criar discos virtuais de grande dimensão, pois consegue somar o espaço total oferecido por todos os discos, exceto o disco de paridade. O desempenho oferecido é razoável nas operações de leitura, pois podem ser utilizados todos os discos em simultâneo.

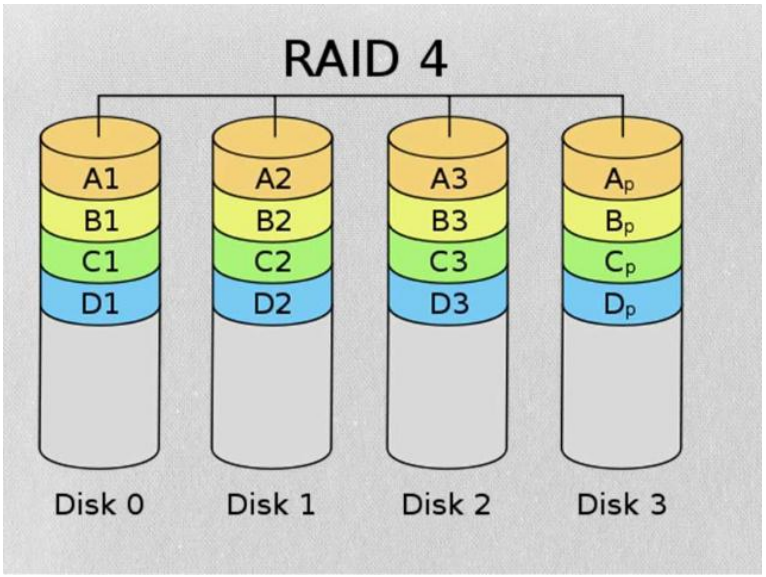
Sempre que os dados são escritos no *array*, as informações são lidas do disco de paridade e um novo dado sobre paridade deve ser escrito para o respectivo disco antes da próxima requisição de escrita ser realizada. Por causa dessas duas operações de I/O, o disco de paridade é o fator limitante do desempenho total do *array*. Devido ao facto do disco requerer somente um disco adicional para proteção de dados, este RAID é mais acessível em termos monetários que a implementação do RAID 1.

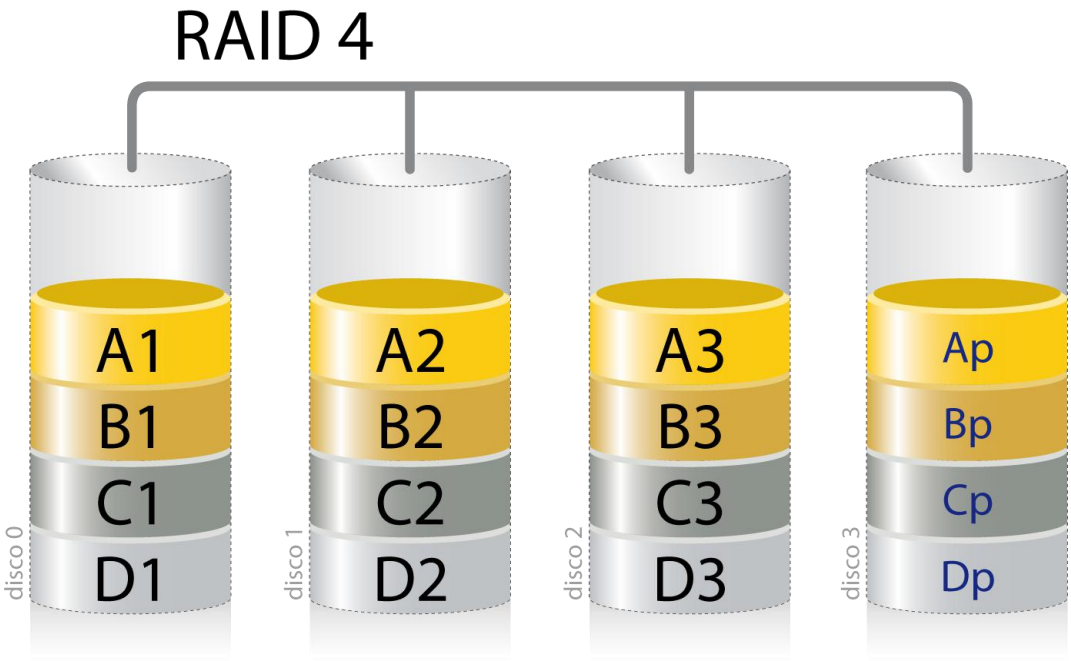
Vantagens:

- taxa de leitura rápida;
- possibilidade do aumento de área de discos físicos.

Desvantagens:

- taxa de gravação lenta;
- em comparação com o RAID 1, em caso de falha do disco, a reconstrução é difícil, pois o RAID 1 já tem o dado pronto no disco espelhado;
- tecnologia não mais usada por haver melhores para o mesmo fim.





6. RAID 5 (Paridade distribuída)

O **RAID 5** é frequentemente usado e funciona similarmente ao RAID 4, mas supera alguns dos problemas mais comuns sofridos por esse tipo.

As informações sobre paridade para os dados do *array* são distribuídas ao longo de todos os discos do *array*, ao invés de serem armazenadas num disco dedicado, oferecendo assim mais desempenho que o RAID 4, e, simultaneamente, tolerância a falhas.

Para aumentar o desempenho de leitura de um *array* RAID 5, o tamanho de cada segmento em que os dados são divididos pode ser optimizado para o *array* que estiver a ser utilizado. O desempenho geral de um array RAID 5 é equivalente ao de um RAID 4, exceto no caso de leituras sequenciais, que reduzem a eficiência dos algoritmos de leitura por causa da distribuição das informações sobre paridade.

A informação sobre paridade é distribuída por todos os discos; perdendo-se um, reduz-se a disponibilidade de ambos os dados e a paridade, até à recuperação do disco que falhou. Isto causa degradação do desempenho de leitura e de escrita.

Ao usar 8 HDs de 20 GB cada um, em RAID 5, em um total de 160 GB de dados, teremos 20 GB de paridade (capacidade de 1 HD) e 140 GB disponíveis.

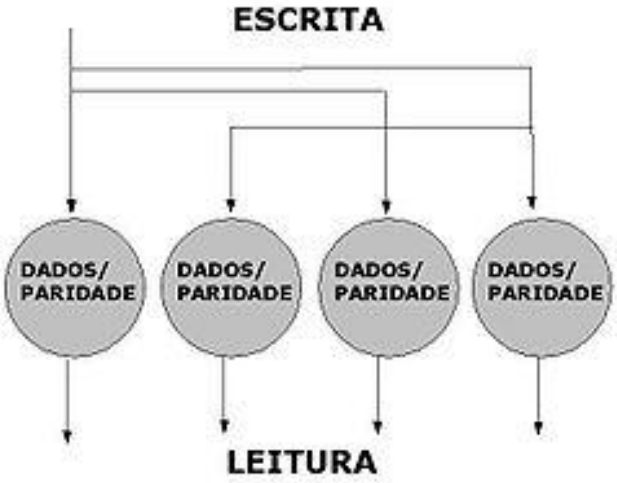
Vantagens:

maior rapidez com tratamento de ECC;

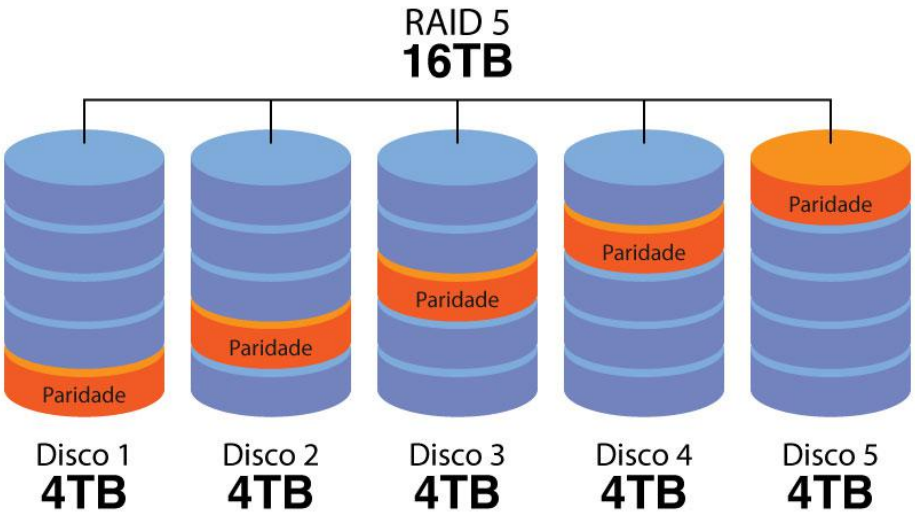
leitura rápida (porém escrita não tão rápida).

Desvantagem:

sistema complexo de controle dos discos.



RAID-5: Escrita precisa de paridade atualizada e leitura pode ser feita em todas as unidades ao mesmo tempo.



7. RAID 6 (Paridade Dual)

É um padrão relativamente novo, suportado por apenas algumas controladoras. É semelhante ao RAID 5, porém usa o dobro de bits de paridade, garantindo a integridade dos dados no caso da perda de até 2 dos HDs ao mesmo tempo. Mínimo de 4 HDs para ser implementado. Ao usar 8 HDs de 20 GB cada um, em RAID 6, em um total de 160 GB de dados, teremos 40 GB de paridade (capacidade de 2 HDs) e 120 GB disponíveis.

Vantagem:

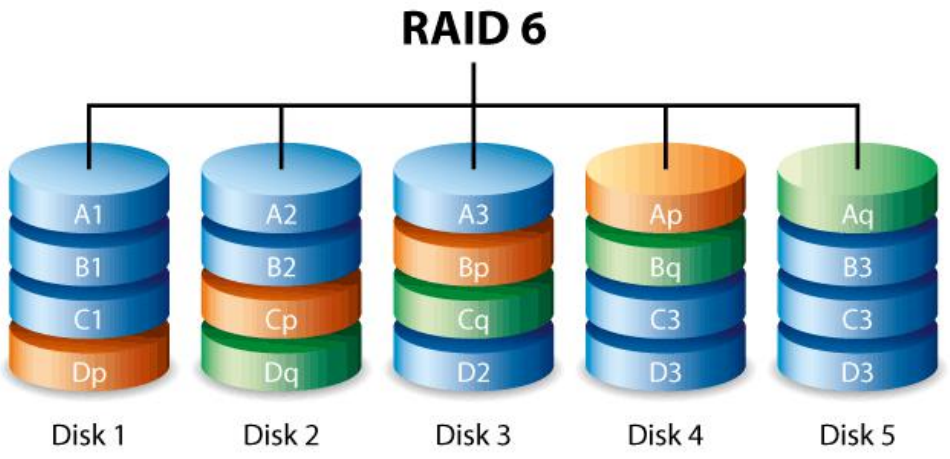
possibilidade falhar 2 HDs ao mesmo tempo sem perdas.

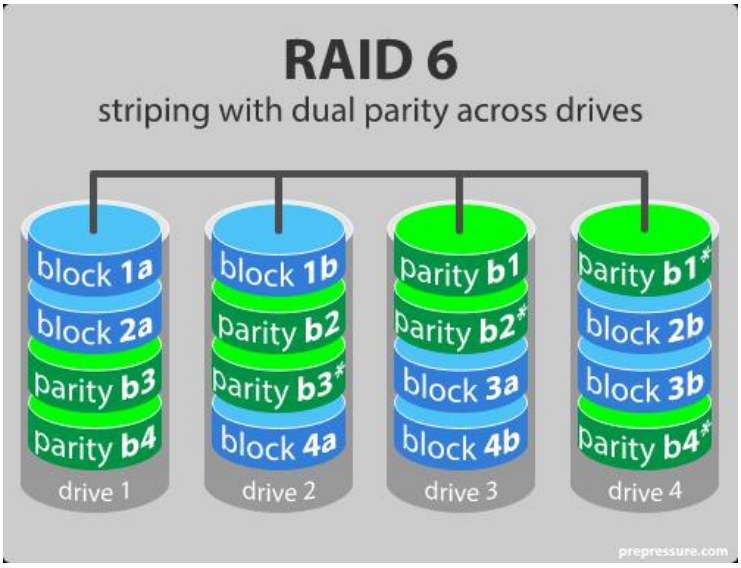
Desvantagens:

precisa de N+2 HDs para implementar por causa dos discos de paridade;

escrita lenta;

complexo sistema de controle dos HDs.





Projetando zonas de segurança

O projeto de zonas de segurança é um importante aspecto da segurança do computador. Você tem muitas abordagens diferentes para realizar um bom projeto sólido. Algumas compensações do projeto envolvem riscos e dinheiro. Você pode criar camadas de segurança para proteger os sistemas de conexão menos segura, e você pode usar tradução de endereços para esconder recursos. Novos métodos e ferramentas para projetar redes seguras estão sendo introduzidos em uma base regular. O que é importante lembrar é que um projeto de segurança boa é algo que você vai querer rever em uma base regular com base no que você aprendeu sobre os seus riscos de segurança.

Tecnologias

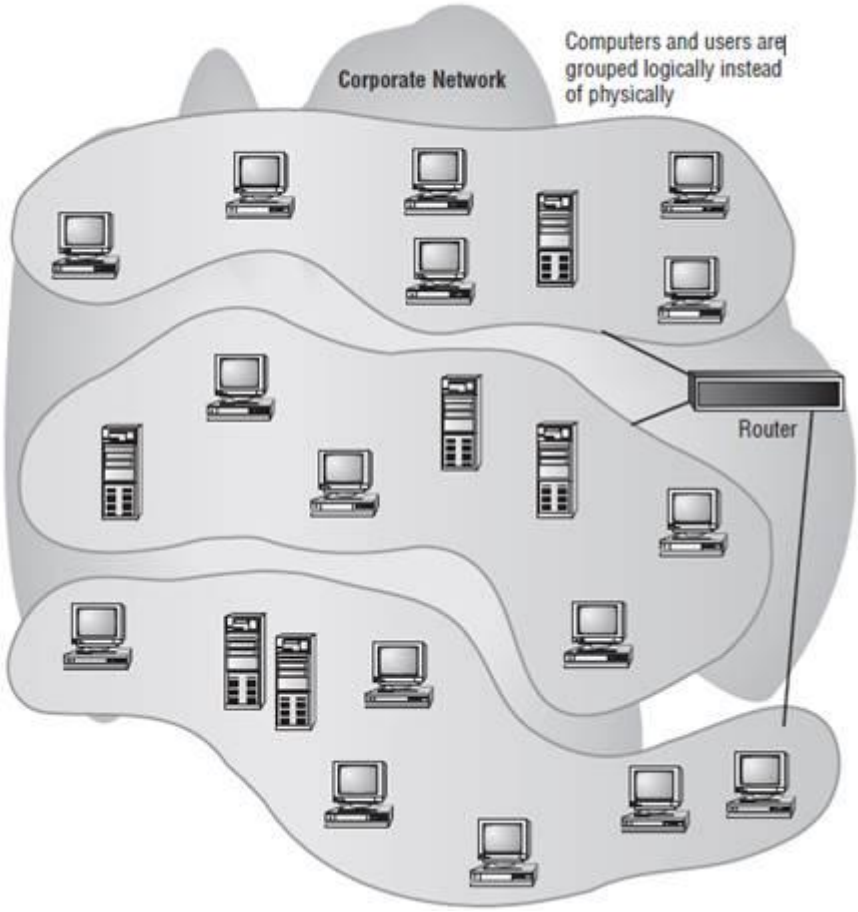
Uma das coisas agradáveis sobre tecnologia é que ela está sempre mudando. Uma das coisas ruins sobre tecnologia é que ela está sempre mudando. Relativamente muitas das novas tecnologias tornaram-se disponíveis para ajudar você a criar um sistema menos vulnerável. As três tecnologias que esta seção irá focar são Redes locais virtuais (VLANs), Tradutor de Endereços de Rede (NAT) e Tunelamento. Estas tecnologias permitem melhorar a segurança em sua rede em muito pouco custo adicional.

8. VLAN

A VLAN permite a criação de grupos de usuários e sistemas e segmentá-los

na rede. Essa segmentação permite que você esconda segmentos da rede de outros segmentos e controle o acesso. As VLANs também pode ser configurada para controlar os caminhos que os dados percorrem para ir de um ponto a outro. Você pode pensar em uma VLAN como uma boa maneira de conter o tráfego para uma determinada área em uma rede. Figura 1.14 ilustra a criação de três VLANs em uma única rede.

FIGURE 1.14 A typical segmented VLAN

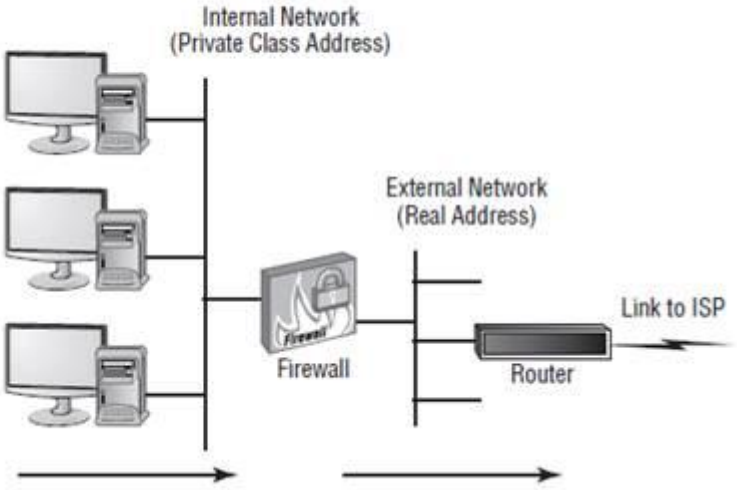


9. NAT

O NAT cria uma oportunidade única para auxiliar na segurança de uma rede. Originalmente, o NAT estendeu o número de endereços de Internet utilizáveis. O NAT permite a uma organização apresentar um único endereço na Internet para todas conexões de computador. O servidor NAT fornece endereços IP para os

hosts ou sistemas na rede e controla o tráfego de entrada e saída. Uma empresa que utiliza NAT apresenta uma única ligação de rede. Esta conexão pode ser através de um roteador ou um servidor NAT. A única informação que um intruso vai ser capaz de conseguir é que a conexão tem um único endereço. O NAT efetivamente esconde sua rede do mundo. Isto torna muito mais difícil determinar quais os sistemas existentes no outro lado do roteador. O servidor NAT efetivamente funciona como um firewall para a rede. A maioria dos novos roteadores dão suporte a tradução NAT. Ele fornece um firewall simples e barato para redes pequenas. A figura 1.15 apresenta um router NAT para prestação de serviços de uma rede. O roteador apresenta um endereço único para todas as conexões externas sobre a Internet.

FIGURE 1.15 A typical Internet connection to a local network



10. Tunelamento

O Tunelamento refere-se à capacidade de criar uma conexão virtual dedicada entre dois sistemas ou redes. O túnel é criado entre as duas extremidades por encapsular os dados mutuamente acordados por protocolo para a transmissão.

Na maioria dos túneis, os dados transmitidos através do túnel aparecem no outro lado, como parte da rede.

Protocolos de encapsulamento incluem geralmente dados de segurança, bem como criptografia. Vários padrões populares emergiram

Figura 9 mostra uma conexão ser feita entre duas redes através da Internet. Esta parece ser a única ligação a cada uma das extremidades da rede.

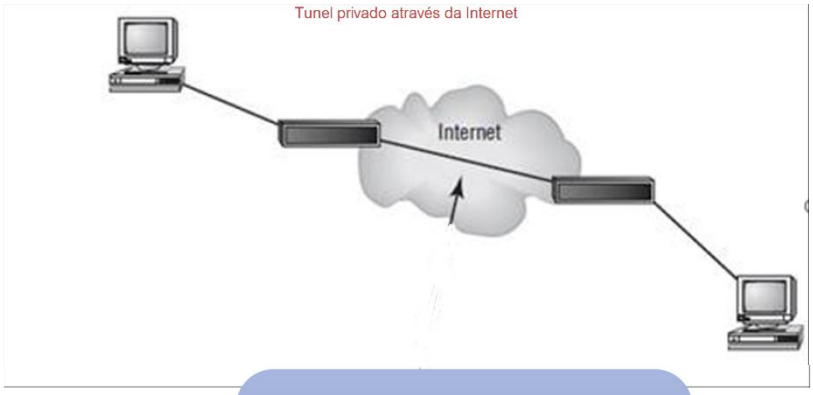


Figura 10 - Túnel Privad

Figura 11 - Requisitos de segurança do negócio

As seções seguintes explicam os diferentes requisitos de negócio que precisam ser abordados ao projetar uma topologia de segurança. A não consideração de qualquer um destes aspectos pode tornar todo o projeto e ineficaz e falho.

Identificação de ativos

Cada empresa ou organização tem bens e recursos que são valiosos.

Estes ativos devem ser contabilizados, tanto fisicamente e funcionalmente. Identificação de Ativos é o processo em que uma empresa tenta colocar um valor na informação e sistemas no lugar.

Em alguns casos, pode ser tão simples como sistemas de contagem e licenças de software. Estes tipos de avaliações de ativo físico são parte do processo normal de contabilidade de uma empresa que deve ser realizado de forma rotineira.

A parte mais difícil de um processo de identificação de ativo está em tentar atribuir valor à informação. Em alguns casos, você pode encontrar-se apenas capaz para determinar o que aconteceria se a informação ficasse indisponível ou fosse perdida. Se a ausência desta informação fosse efetivamente desligar os negócios, esta informação não tem preço. Se você tem este tipo de informação, determinar quais os métodos e abordagens que você deve tomar para proteger a informação se torna mais fácil.

Você não necessariamente atribui o mesmo valor para a fórmula da Coca-Cola que você atribuiria para a receita de arroz e frango de sua mãe. A fórmula Coca-Cola valeria uma fortuna para uma pessoa que a roubou. Eles poderiam vender aos concorrentes e se aposentar; receita de sua mãe iria fazer um bom jantar, mas não seria especialmente valioso do ponto de vista financeiro.

Avaliação de Risco

Existem várias maneiras de realizar uma análise de risco ou avaliação de risco. Elas variam desde fórmulas à base de métodos altamente científicos a uma conversa com o proprietário. Em geral, você vai querer tentar identificar os custos da substituição de dados ou sistemas roubados, os custos de inatividade, e praticamente qualquer outro fator que você pode imaginar.

Depois de ter determinado os custos, você pode então avaliar a probabilidade

que certos tipos de eventos irão ocorrer e qual é o resultado mais provável se

a ocorrer. Se você trabalha em Nova York, qual é a probabilidade de danos

para o seu negócio a partir de um terremoto? Será que a sua avaliação de risco coloca uma alta probabilidade de um terremoto em sua lista de principais preocupações? Por outro lado, como poderia uma pessoa sensata ter imaginado ou mesmo previsto para 11 de setembro de 2001, o atentado ao World Trade Center?

Muitos provedores, centros de dados, e as empresas tiveram que repensar as avaliações de risco por causa dessa tragédia.

Identificação da ameaça

Implementar uma política de segurança requer que você avalie os riscos tanto de ameaças aos dados e rede, internas e externas. Faz-se muito pouco uma boa implementação de um ambiente de alta segurança para proteger a sua empresa de fora, se a ameaça é principalmente interna. Se um membro da sua equipe traz um disco contendo um vírus para o escritório e carrega-o em um computador, o vírus pode se espalhar em toda a rede e efetivamente ser imune a suas medidas de segurança externas. Este é um problema muito comum nas escolas, bibliotecas e ambientes onde as pessoas regularmente utilizam recursos compartilhados.

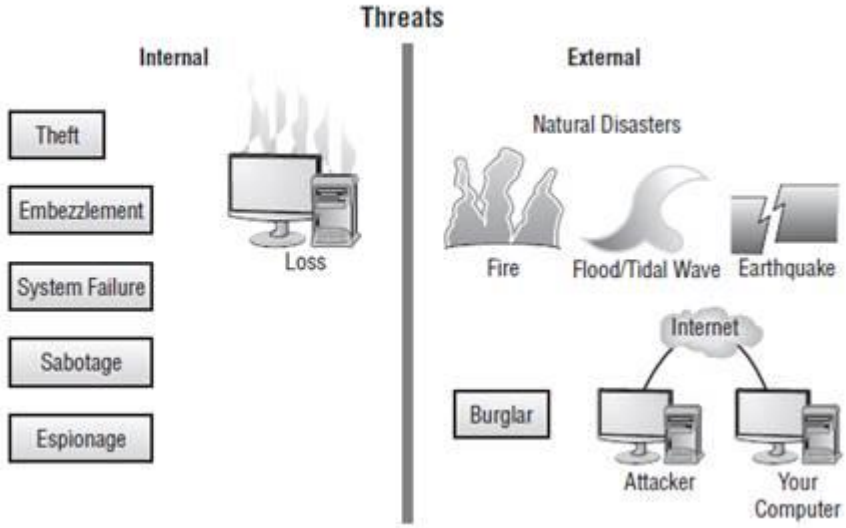
Se uma biblioteca dispõe de computadores para uso público, e os computadores estão em uma rede, um vírus pode infectar todos os sistemas ao longo da rede.

Medidas de segurança externas não vão prevenir potenciais danos ou perda de dados.

Ameaças internas também incluem fraude de funcionário, abuso ou alteração de dados e roubo de propriedade. Estas ameaças requerem que ambos, políticas e sistemas sejam postos em prática para detectar e mitigar essas possibilidades. Investigar e fazer recomendações para a gestão de mudanças procedurais e políticas é um papel fundamental para os profissionais de segurança de computadores. A figura 1.18 retrata

alguns exemplos de ameaças internas e externas.

FIGURE 1.18 Internal and external threats in an organization



Ameaças internas

As mais bem divulgados ameaças internas envolvem abusos financeiros. Alguns destes abusos são verdadeiras fraudes ou roubo. Estes tipos de ameaças, especialmente em um ambiente com muitos computadores, podem ser muito difíceis de detectar e investigar.(16)

Estas ameaças são tipicamente contínuas e envolvem pequenas transações em longos períodos. Um incidente recente de fraude que ocorreu em uma grande companhia de software envolveu um contador que gerou cheques falsos em pagamento de trabalho que nunca ocorreu.

Este funcionário foi capaz de superar $100.000 em pagamentos fraudulentos feitos a empresas que ele ou parentes haviam criado a mais de alguns meses. Levou uma quantidade considerável de investigação por auditores de computadores e financeiros para determinar como isso ocorreu.(17)

A partir de uma perspectiva de segurança do computador, essa foi uma ameaça interna o resultada de falhas, tanto financeiras, operacional, e de controles de segurança do computador. Estes tipos de incidentes, provavelmente, ocorrem com mais frequência do que alguém quer admitir.

Outro incidente envolveu um funcionário que estava usando recursos informáticos para operar um serviço de contabilidade financeira. Este empregado vinha executando este negócio por vários anos. Quando a empresa descobriu, ele foi imediatamente demitido e teve seus registros confiscados.

Durante a investigação, o processo usado para coletar provas inadvertidamente o contaminou. A cadeia de evidências neste caso foi quebrada. Quando o empregado foi ao tribunal sobre esta situação, o seu advogado foi capaz de levar evidência

para fora do campo. Mesmo que este funcionário tenha sido claramente culpado, o juiz rejeitou o caso por falta de provas admissíveis.

Ele, então, processou a empresa por demissão ilegal, assédio e vários outros encargos. Ele ganhou esses fatos, e ele conseguiu seu emprego de volta. Neste exemplo, as políticas e os sistemas internos postos em prática para detectar, investigar e corrigir este problema quebraram. Ele custou à empresa uma enorme quantidade de dinheiro e permitiu uma volta como fraudador conhecido na empresa.

Ameaças externas

Muitas das ameaças internas que uma empresa deve lidar é ter procedimentos

e métodos que são padrão em todos os setores. Ameaças externas, por outro lado, estão a aumentar a um ritmo alarmante. Alguns anos atrás, a maioria dos incidentes em computadores ocorreu por grupos de crianças ou "amadores", que estavam principalmente querendo se divertir. Na maioria das vezes estes incidentes tiveram naruteza maliciosa. Alguns deles envolvem alterações ou destruição de dados e registros.(13)

Hoje, muitas empresas utilizam bases de dados online, fazer pedidos, processos de pagamentos, rastrear remessas, gerenciar inventário e gerenciar outras informações importantes utilizando sistemas complexos. Estes sistemas estão ligados a outros que contêm registros corporativos privados, segredos comerciais, planos estratégicos, e muitos outros tipos de informações valiosas.

Infelizmente, quando estes sistemas são comprometidos, toda uma empresa pode ser comprometida. Os incidentes ocorrem quando brechas de segurança permaneceram abertas por anos sem conhecimento da empresa que isso já ocorreu. Uma das maiores alegrias de um criminoso profissional é criar e explorar este tipo de violação de segurança. Os primeiros métodos de sistemas de rachaduras eram primitivos e trabalhosos. Hoje, existem pacotes de software que encontram alvos automaticamente e, em seguida, sistematicamente atacam o alvo para encontrar suas vulnerabilidades. Muitas dessas ferramentas usam interfaces gráficas necessitam poucos conhecimentos técnicos de um aspirante a hacker.

Muitos sistemas de computadores estão sendo repetidamente e metodicamente atacados pela curiosidade ou por criminosos que tentam cometer um crime.(5)

O trabalho de um profissional de segurança de computadores nesta situação é detectar o ataque, encontrar formas de combatê-lo e auxiliar a aplicação da lei em averiguação da atividade.

Vulnerabilidades

Provavelmente a maior área de preocupação que um especialista em segurança de computadores terá que resolver, gira em torno das capacidades de segurança do software e sistemas utilizados no negócio. Até recentemente, muitos fabricantes de sistemas operacionais pago apenas serviço de bordo para a segurança. Um sistema operacional muito popular usava um esquema de segurança com logon e senha. Quando o prompt de logon aparecia, tudo o que tinha a fazer era apertar o botão Cancelar e o sistema forneceria a maior parte dos recursos de rede e de acesso local a todos os recursos. Se a proteção de tela foi protegida por senha, você teve que digitar a senha

para desbloquear o sistema ou reiniciá-lo para que o sistema seja inseguro. Isto foi pior do que não ter segurança. Muitos usuários pensam que isso significava que eles tinham um sistema seguro. Eles não fizeram, e muitos roubos de dados por colegas de trabalho ocorreram como resultado.(16)

O TCP / IP (Protocolo de Controle de Transmissão / Protocolo da Internet) protocolo de rede, utilizado pela maioria das redes corporativas, foi projetado para permitir a comunicação em um ambiente de confiança. Este protocolo foi essencialmente experimental e usado por escolas e agências governamentais para a pesquisa. Enquanto é muito robusto, em seu tratamento de erros, é por sua própria natureza não seguro. Muitos ataques em redes modernas ocorrem através do protocolo TCP / IP. O capítulo 2, "Conheça seu inimigo ", discute o TCP / IP e os problemas de segurança associados. Felizmente, o TCP / IP é mais seguro do que muitos dos protocolos ainda instalados em redes atuais.

Os sistemas operacionais e programas aplicativos têm sido vulneráveis a ataques externos e internos. As empresas de software querem vender software que são fáceis de usar, graficamente, orientado e facilmente configurado. Usuários querem a mesma coisa. Infelizmente, isto cria problemas adicionais de segurança em muitas redes.

Um dos produtos mais populares em uso hoje permite que e-mail e anexos iniciem execução de programas ou instruções incorporadas em uma mensagem.

Isso permite que as mensagens de e-mails tenham uma formatação simpática, mas também permite que e-mails carreguem vírus que podem danificar redes ou se espalhar para outras redes.(1)

O fabricante deste software agora está lançando atualizações de segurança, mas parece que cada vez que introduz uma atualização de segurança, alguém vem com uma nova forma em torno das atualizações.

Muitos fabricantes de sistemas operacionais estão completamente repensando as medidas de segurança. Eles têm reconhecido que seus produtos não podem proteger as empresas que os utilizam de perda de dados ou abuso. Tornou-se um problema tão grande para muitos clientes que o suporte a segurança está se tornando disponível pela maioria dos fabricantes de sistema operacional e software e rede. No passado, vulnerabilidades de segurança foram escondidas pelos fabricantes de software;

agora estão a ser publicadas e as soluções são fornecidas assim que a vulnerabilidade é descoberta. Isto, obviamente, ajuda a hackers que sabem que estas mudanças não vão ser feitas em muitos sistemas de computadores por um tempo.

Em um sentido mais básico, o progresso é o pior pesadelo do especialista em segurança. Como certificado Segurança+, você é parte da equipe que deve avaliar ameaças aos sistemas já instalados.

VIRTUAL BOX

Modos de rede no VirtualBox

O VirtualBox é uma aplicação multi-plataforma de virtualização. Com ele, é possível executar múltiplos sistemas operacionais ao mesmo tempo em máquinas virtuais. Cada máquina virtual poderá ter sua configuração específica de hardware, como se fossem computadores reais, e o suporte à rede é bastante refinado, com diversos modos de operação. Na seção de rede das configurações da máquina virtual, é possível determinar como o VirtualBox concede os adaptadores de rede e os modos de operação na VM. O VirtualBox é bastante flexível na virtualização da rede. Os modos de operação dos adaptadores virtuais são em consideração ao hardware de rede físico do hospedeiro. Para cada adaptador de rede habilitado é possível especificar um dos seguintes modos de virtualização:

11. Não Conectado - Not attached - Desconectado.

Neste modo, o VirtualBox informa ao sistema convidado que a placa de rede está presente, porém não há conexão, como se não houvesse um cabo de rede plugado. É um modo de simular uma retirada do cabo da placa de rede.

12. NAT (Network Address Translation)

O IP do guest é reconvertido no host usando NAT. Não dá pra acessar a VM guest de fora, nem mesmo do host. Apenas a VM guest acessa o que está fora (na Internet). É a configuração padrão para testar um sistema de forma isolada da máquina host.

13. NAT (Network Address Translation) - NAT Network

As VMs fazem parte de uma mesma rede e acessam redes externas (Internet inclusive). Mas assim como no modo NAT, a máquina host e as demais máquinas da mesma rede local real não enxergam as máquinas da rede NAT. É possível nomear e definir configurações da rede NAT.

É o modo padrão de rede no VirtualBox. Com este modo, o VirtualBox age como um roteador, mapeando o tráfego, mascarando os IPs e possibilitando a

comunicação da VM com a rede externa. O sistema convidado recebe um endereço IP que não faz parte da rede externa, do servidor DHCP integrado ao VirtualBox, e portando, durante todo o tráfego, os endereços e portas são traduzidos. Cada máquina virtual terá um roteador particular e elas não farão parte de uma mesma rede, impossibilitando a comunicação entre elas.

Este modo é necessário quando não é possível a máquina virtual obter um endereço IP real da rede externa. Ou quando deseja tornar a VM invisível e inalcançável pela rede externa, pelo menos não diretamente.

14. Placa Em Modo Bridge - Bridged networking

A VM guest se comporta como uma máquina fisica na rede. Ela acessa a placa de rede do host. Se o host trocar entre rede cabeada e wireless é necessário reconfigurar. Muito útil para virtualizar um servidor e acessar no mesmo host, ou na mesma rede.

Neste modo, o VirtualBox usa um driver de dispositivo para interceptar e injetar dados no adaptador de rede físico, tornando-se um adaptador de rede por software. O sistema convidado, usando este adaptador de rede por software, consegue conectar-se diretamente na rede externa e assim receber um endereço IP válido na rede externa.

O sistema hospedeiro e também todas as máquinas da rede, na qual a máquina hospedeira pertence, enxergarão normalmente a VM pela rede como se a VM fosse uma máquina real.

É um modo geralmente utilizado em sistemas convidados que são servidores de rede. Este modo possui algumas limitações dependendo do sistema operacional hospedeiro.

15. Rede Interna - Internal Networking

Rede interna ao sistema de virtualização. Não conecta ao host e nem à Internet. Precisa IP fixo, ou um DHCP dentro da rede interna (que pode ser configurado automaticamente). Permite múltiplas redes internas e configuração de roteamento.

Este modo é utilizado para criar uma rede por software onde somente as máquinas virtuais selecionadas ficarão visíveis entre elas. Nenhuma máquina da rede externa, nem mesmo o próprio hospedeiro enxergará as VMs da rede interna.

Desta forma, todo o tráfego ficará restrito à rede interna e completamente isolado e escondido da rede externa.

É um modo seguro de se fazer rede entre as VMs, pois será impossível capturar pacotes pela rede externa.

16. Placa De Rede Exclusiva De Hospedeiro - Host-only Adapter

Similar ao Internal Networking, porém a máquina host participa da rede. Assim é possível usar um navegador, ou clientes SSH. Mas as máquinas dentro da rede host only não acessam redes externas (Internet inclusa).

Neste modo, o VirtualBox monta uma rede contendo somente o hospedeiro e um conjunto de máquinas virtuais, sem a necessidade do adaptador de rede físico do hospedeiro. É um modo híbrido entre o modo bridge e o modo de rede interna, as VMs se enxergarão entre si e ao hospedeiro, como se estivessem conectadas a uma mesma rede física, porém, como a rede interna está conectada somente à interface virtual do hospedeiro, o acesso a rede externa não é possível.

O VirtualBox cria no sistema hospedeiro uma interface virtual de rede, semelhante a interface de loopback. Esta interface proporciona a conectividade entre as VMs e o sistema hospedeiro.

17. Driver Genérico - Generic Driver

Segundo a documentação "um modo raramente usado". A documentação relata como exemplo a configuração de um tunel UDP para a conexão direta entre duas VMs executadas em diferentes hosts.

Permite ao usuário selecionar um driver que pode ser incluído no VirtualBox, numa recompilação, ou fornecido por um pacote de extensão.

Possui submodos os quais permitem que máquinas virtuais, em hospedeiros distintos, fiquem conectadas numa mesma infraestrutura de rede. Em outras palavras, permite a conexão em rede de sistemas convidados que estão em diferentes sistemas hospedeiros.

Generalizando, é uma parte opcional do VirtualBox que só está incluída no código fonte. O pacote fornecido pela Oracle não inclui os drivers necessários.

18. RESUMO

Modo de Rede	Acessa Internet?	Comunica com o Host?	Comunica com outras VMs (rede de VMs)?	Visível na rede local do host?
NAT	Sim	Não*	Não	Não
NAT Network	Sim	Não*	Sim	Não
Bridged networking	Sim	Sim	Sim	Sim
Internal Networking	Não	Não	Sim	Não
Host-only Adapter	Não	Sim	Sim	Não

	NAT	NAT Networking	Bridged Adapter	Internal Network	Host-Only
Guest pode ser conectar com o Host?	SIM	SIM	SIM	NÃO	NÃO
Host pode se conectar ao Guest?	NÃO	NÃO	SIM	NÃO	SIM
Guest pode se conectar a rede externa?	SIM	SIM	SIM	NÃO	NÃO
Guest pode se conectar a outro Guest na mesma rede?	NÃO	SIM	SIM	SIM	SIM
Outros computadores na rede do Host podem se conectar ao Guest?	NÃO	NÃO	SIM	NÃO	SIM

História da criptografia

A **história da criptografia** começa há milhares de anos. Até décadas recentes, ela havia sido a história do que poderia ser chamado de criptografia clássica — isto é, de métodos de criptografia que usam caneta e papel, ou talvez auxílios mecânicos simples. No começo do século XX, a invenção de complexas máquinas mecânicas e electro-mecânicas, tais como a máquina com rotores Enigma, providenciou meios mais sofisticados e eficientes de encriptação; e a posterior introdução da eletrônica e computação permitiu elaborar esquemas de ainda maior complexidade, muitos completamente inadequáveis ao papel e caneta.

Criptografia, junção de duas palavras gregas κρυπτός (kriptós – secreto, escondido) e γράφειν (gráfein – escrita), é, resumindo, o uso de técnicas para transformar texto ou dados legíveis em informação ilegível, que não possa ser compreendida.

E não é algo novo. Povos antigos como os espartanos e romanos fizeram uso de cifras criptográficas em suas trocas de mensagens.

Para facilitar, dividimos as cifras criptográficas em dois períodos: a criptografia clássica e a criptografia moderna.

Criptografia Geral

Na criptografia, encriptação é o processo de codificação de uma mensagem ou informação, de forma que, somente as pessoas autorizadas conseguem ter acesso. O processo de encriptação não isenta de interferências, mas, evita que o conteúdo possa ser visualizado por qualquer um interceptador. Ela é formada por quatro princípios iniciais, sendo eles: Confidencialidade, autenticação, não repúdio e a integridade da informação, (assim, o remetente não consegue negar o envio da informação).

Dentro da criptografia também ocorre a de criptografia, sendo ela o processo contrário da encriptação, onde somente criadores das plataformas e pessoas com um alto conhecimento na área conseguem efetuar, mesmo assim, é exigido grandes recursos computacionais e conhecimento, além do tempo dedicado a essa atividade ser intenso.

É importante ressaltar que nenhuma forma de criptografia é totalmente segura,

Nela podemos citar as:

Assimétricas (Públicas): As chaves são públicas e para cada acesso é gerada uma chave. É mais recomendado utilizar em casos em que irá ser utilizada por diversas pessoas e a localidade de cada usuário é distante.

Simétricas (Privadas): As chaves utilizadas serão idênticas, tanto pelo fornecedor quanto pelo receptor, dessa forma, é melhor ser utilizada para casos em que conseguimos enviar a chave pessoalmente, já que, a partir do momento em que enviamos via web, a mesma pode estar sendo exposta.

Antigamente era muito utilizado por militares e pelo governo como forma de facilitar comunicações secretas, isso tem diminuído com o tempo. Agora, é bem mais comum ser utilizado para a proteção de informações em diversos tipos de sistemas civis.

Hoje em dia, a utilização dessa ferramenta se tornou essencial para quaisquer usuários. Com a evolução das formas de invasões, houve a evolução da criptografia, tendo assim, codificações desde 256 até 1024 bits.

Criptografia nas redes wi-fi

As conexões sem fio, deixam uma grande brecha na segurança, pois pessoas com conhecimentos técnicos conseguem efetuar a interceptação de dados de uma rede.

Desse modo, foram feitas evoluções nas técnicas de criptografia, permitindo assim, uma conexão segura para os usuários, domésticos e na área empresarial, como resultado, as transações financeiras, dados e informações sigilosas estão mais protegidas.

Criptografia clássica

O primeiro uso conhecido da criptografia foi encontrado em hieróglifos irregulares esculpidos em monumentos do Antigo Império do Egito (a cerca de

Figura 12 - Hieróglifo - https://aventurasnahistoria.uol.com.br/noticias/reportagem/como-ler-textos-em-hieroglifo.phtml

4500 anos).

Porém, não podem ser considerados como tentativas sérias de comunicações secretas, mas sim de ser mensagens misteriosas, intrigas ou mesmo diversão para os alfabetizados. Seguem outros exemplos de usos da criptografia, ou algo parecido. Algumas tabuletas de argila na Mesopotâmia, um pouco mais tarde, foram utilizadas para proteger informações, por exemplo, receitas de valor comercial. Mais tarde ainda, estudiosos hebreus fizeram uso de simples cifras de substituição monoalfabética (como a cifra Atbash), começando talvez em torno de 500 a 600 a.C.

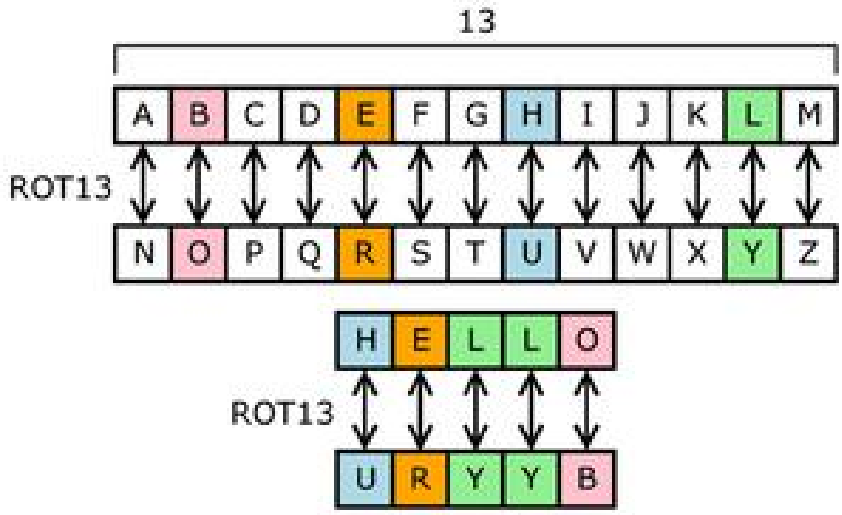


Figura 13 - Cifra de substituição - https://pt.wikipedia.org/wiki/Cifra_de_substitui%C3%A7%C3%A3o

Podemos chamar de criptografia clássica o período que vai desde os povos antigos, passando pela Idade Média e chegando até as máquinas eletromecânicas, utilizadas principalmente durante a Segunda Guerra Mundial.

Dentre as cifras clássicas mais conhecidas temos o scytale espartano, a de César e a de Vigenère. E como máquina eletro-mecânica temos a Enigma.

1. Scytale

Scytale, um dispositivo primitivo da criptografia.

A cifragem com o scytale (bastão, em grego) ou cítala espartana consistia em se enrolar uma fita de tecido em um bastão de madeira de dada largura. A frase a ser cifrada era escrita na fita no comprimento do bastão, denserolada e enviada disfarçada (como um cinto por exemplo) e ao chegar ao destino deveria ser enrolada num bastão de mesma largura para que a mensagem fosse decifrada.

Também era conhecida como bastão de Licurgo, embora alguns estudiosos citem que este tipo de cifra não passa de um mito.

Acredita-se que os gregos antigos conheciam cifras (por exemplo, a cifra de transposição scytale utilizada pelos militares de Esparta). Heródoto fala-nos de mensagens secretas escondidas sob a cera em tabletes de madeira ou como uma tatuagem na cabeça de um escravo oculta pelo cabelo crescido, embora estes não sejam devidamente exemplos de criptografia por si só, já que a mensagem, uma vez conhecida, é de fácil leitura; o que ficou conhecido como esteganografia. Outro método grego foi desenvolvido por Políbio (agora chamado de "Quadrado de Políbio").[1] Os romanos conheciam um pouco de criptografia também (por exemplo, a cifra de César e suas variações).

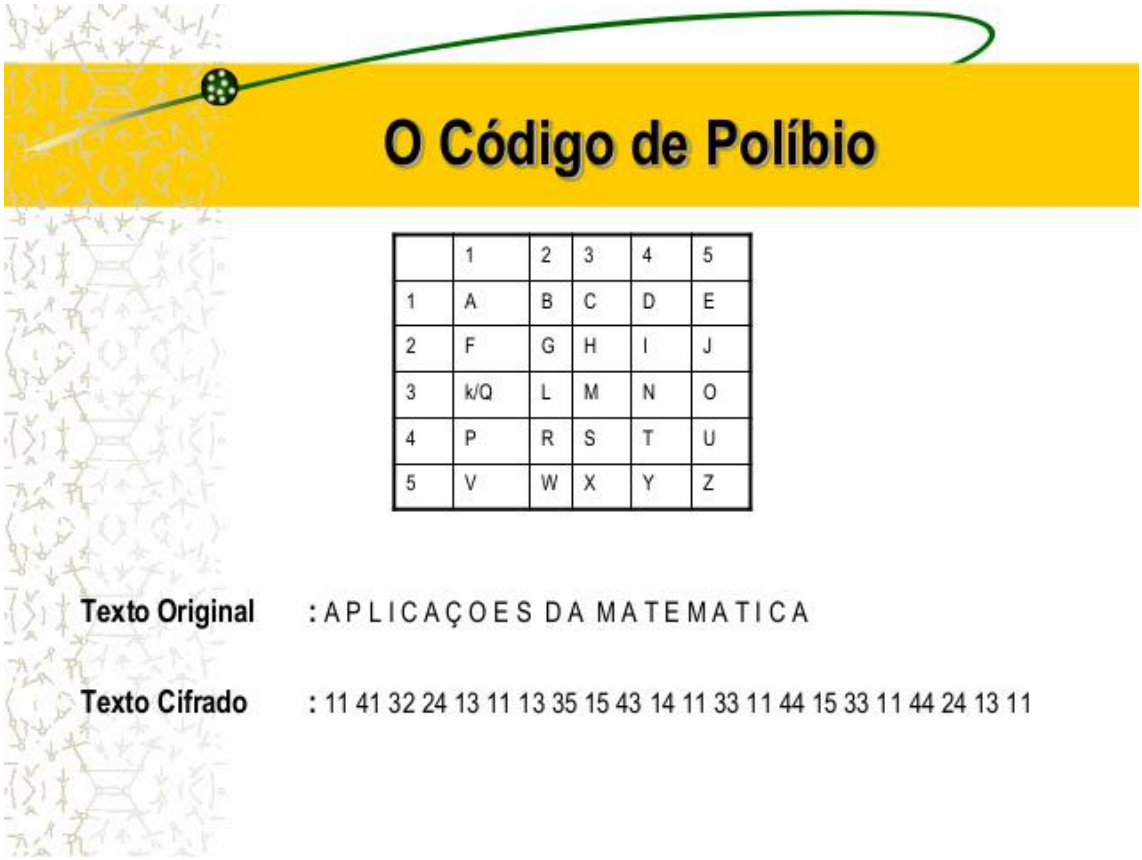
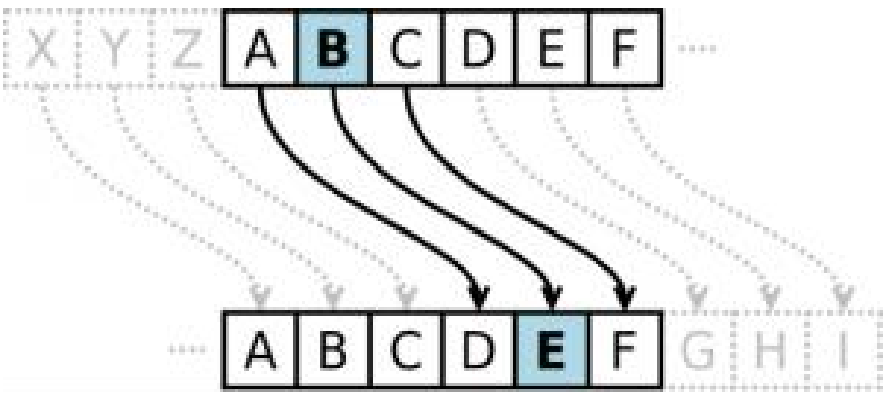


Figura 14 - Quadrado de políbio - https://pt.slideshare.net/RogerioNascimento/revisao-aula

Cifra de César



Uma das cifras mais conhecidas é a cifra de César, que foi utilizada por Júlio

César para se comunicar com suas tropas durante as guerras que travava.

Esta cifra é bastante simples, consiste na substituição de uma letra do alfabeto por seu correspondente três casas adiante, ou seja, a letra A é substituída

pela letra D, a letra B pela letra E e assim por diante. Neste caso, o algoritmo da cifra é a troca de uma letra por outra em uma determinada posição. E a chave, neste caso, é o número 3.

Cifra de Vigenère – a cifra indecifrável

A cifra de Vigenère (atribuída equivocadamente a Blaise de Vigenère) foi descrita primeiramente pelo italiano Giovan Battista Bellaso, em 1553, em sua obra

	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
A	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
B	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A
C	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B
D	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C
E	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D
F	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E
G	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F
H	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G
I	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H
J	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I
K	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J
L	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K
M	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L
N	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M
O	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N
P	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O
Q	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P
R	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q
S	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R
T	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S
U	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T
V	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U
W	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V
X	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W
Y	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X
Z	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y

La cifra del. Sig. Giovan Batista Bellaso e por muito tempo foi considerada como *le chiffre indéchiffrable* (a cifra indecifrável) quando, em meados do século XIX, Charles Babbage e Friedrich Kasiki encontraram um método de resolvê-la.

Seu processo de cifragem é assim: o usuário cifrará a mensagem com uma chave alfabética; caso a quantidade de caracteres da chave for menor que o tamanho de caracteres da mensagem, a chave será repetida até ambas terem a mesma quantidade de caracteres. Fazendo uma relação entre as duas (a mensagem e a chave), cada letra da mensagem será cifrada com um alfabeto definido pelo caracter da chave ao qual estará relacionada.

A máquina Enigma

Até o início do século XX as cifras desenvolvidas podiam ser solucionadas sem a necessidade de uma máquina, bastava tempo e dedicação.

Mas, com o surgimento da mecanização, algumas máquinas foram desenvolvidas com o intuito de acelerar tanto o processo de cifragem/decifragem como em dificultar a criptoanálise das mensagens cifradas.

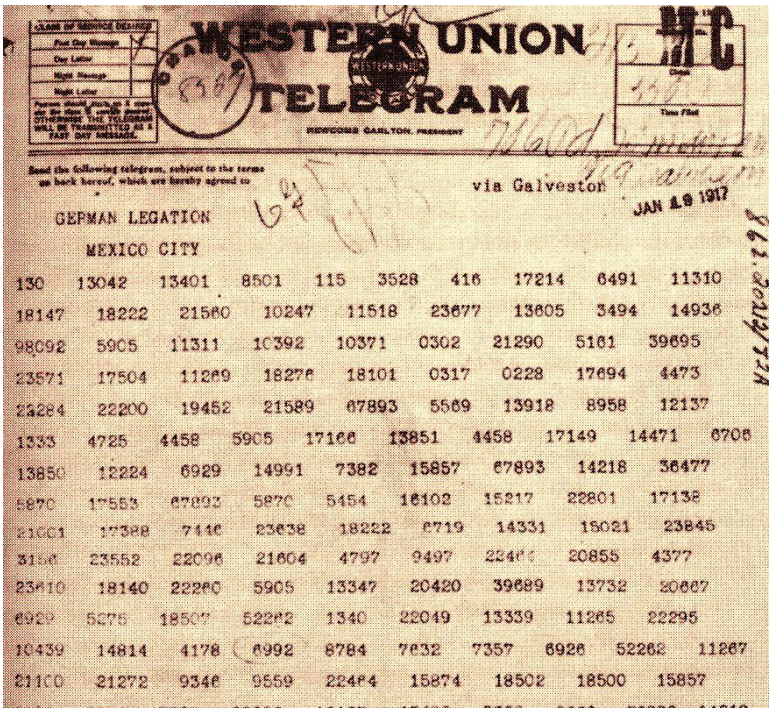
Dentre estes equipamentos o mais conhecido é a máquina Enigma, utilizada pelos alemães durante a Segunda Guerra Mundial.

A Enigma lembra um pouco uma máquina de escrever, onde ao invés de colocar o resultado no papel, ele era mostrado em um painel luminoso com os caracteres do alfabeto. A chave usada para cifrar/decifrar uma mensagem era configurada por meio de rotores eletromecânicos (3 ou mais) que podiam ser alterados conforme a necessidade para formar a chave.

Foi considerada como impossível de se decifrar uma mensagem cifrada com a Enigma.

Sua quebra só foi possível devido a esforços de poloneses e ingleses, sendo Alan Turing o mais lembrado em ter trabalhado na quebra da cifragem da Enigma.

O desenvolvimento da criptografia foi acompanhado pelo desenvolvimento da criptoanálise - a "quebra" de códigos e cifras. A descoberta e aplicação, desde cedo, de análise de frequência para a leitura de comunicações criptografadas, muitas vezes, alterou o curso da história. Portanto, o Telegrama Zimmermann que motivou a entrada dos Estados Unidos na Primeira Guerra Mundial e o fato de que os Aliados conseguiram decifrar as cifras da Alemanha Nazista, encurtou a Segunda Guerra Mundial, em algumas avaliações, em até dois anos.



WESTERN UNION

TELEGRAM

via Galveston

JAN 19 1917

GERMAN LEGATION

MEXICO CITY

130 13042 13401 8501 115 3528 416 17214 6491 11310

18147 18222 21560 10247 11518 23677 13605 3494 14936

98092 5905 11311 10392 10371 0302 21290 5161 39695

23571 17504 11269 18276 18101 0317 0228 17694 4473

24284 22200 19452 21589 67893 5569 13918 8958 12137

1333 4725 4458 5905 17166 13851 4458 17149 14471 6706

13850 12224 6929 14991 7382 15857 67893 14218 36477

5870 17553 67893 5870 5454 16102 15217 22801 17138

21001 17388 7446 23638 18222 6719 14331 15021 23845

3156 23552 22098 21604 4797 9497 22464 20855 4377

23610 18140 22260 5905 13347 20420 39689 13732 20667

6929 5870 18502 52262 1340 22049 13339 11265 22295

10439 14814 4178 6992 8784 7632 7357 6926 52262 11267

21100 21272 9346 9559 22464 15874 18502 18500 15857

Figura 15- Telegrama de Zimmerman - https://cafenofront.wordpress.com/2017/03/04/o-telegrama-ziermann-1917-alemaes-oferecem-o-texas-e-outros-territorios-ao-mexico/

BEFNSTOPFF.

Até à década de 1970, a criptografia segura foi amplamente utilizada para a proteção de governos. Dois eventos trouxeram-a diretamente para o domínio

público: a criação de um padrão de criptografia de chave simétrica (DES), e a invenção da criptografia de chave pública.

Figura 16 - Análise de frequência para algoritmos de substituição simples -https://pt.wikipedia.org/wiki/An%C3%A1lise_de_frequ%C3%AAncia

Criptografia medieval

A primeira página do manuscrito de Alquindi ***On Deciphering Cryptographic Messages***, contendo as primeiras descrições da criptoanálise e análise de frequência.

Ver também: Manuscrito Voynich

Figura 17 - Manuscrito Voynich -https://pt.wikipedia.org/wiki/Manuscrito_Voynich

Foi provavelmente por motivos religiosos e através da análise textual do Alcorão que levou à invenção da técnica de análise de frequência para quebrar cifras de substituição monoalfabética por Alquindi, um matemático árabe, por volta de 800 (Ibraim Alquindi -1992).

Foi o avanço mais fundamental da criptoanálise até a Segunda Guerra Mundial. Alquindi escreveu um livro sobre criptografia "Risalah Istikhraj fi al-Mu'amma" ("Manuscrito para decifrar mensagens criptográficas"), no qual ele descreve as primeiras técnicas de criptoanálise, inclusive para cifras polialfabética, classificação de cifra, fonética e sintaxe árabe, e, o mais importante, as primeiras descrições sobre a análise de frequência.[2] Ele também expôs métodos de cifragem, a criptoanálise de certas cifragens, e análise estatística de letras e combinações de letras em árabe.

	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
A	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
B	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A
C	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B
D	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C
E	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D
F	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E
G	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F
H	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G
I	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H
J	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I
K	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J
L	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K
M	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L
N	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M
O	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N
P	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O
Q	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P
R	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q
S	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R
T	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S
U	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T
V	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U
W	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V
X	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W
Y	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X
Z	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y

Figura 18 - Cifra de substituição polialfabéticas - https://pt.wikipedia.org/wiki/Cifra_polialfab%C3%A9tica

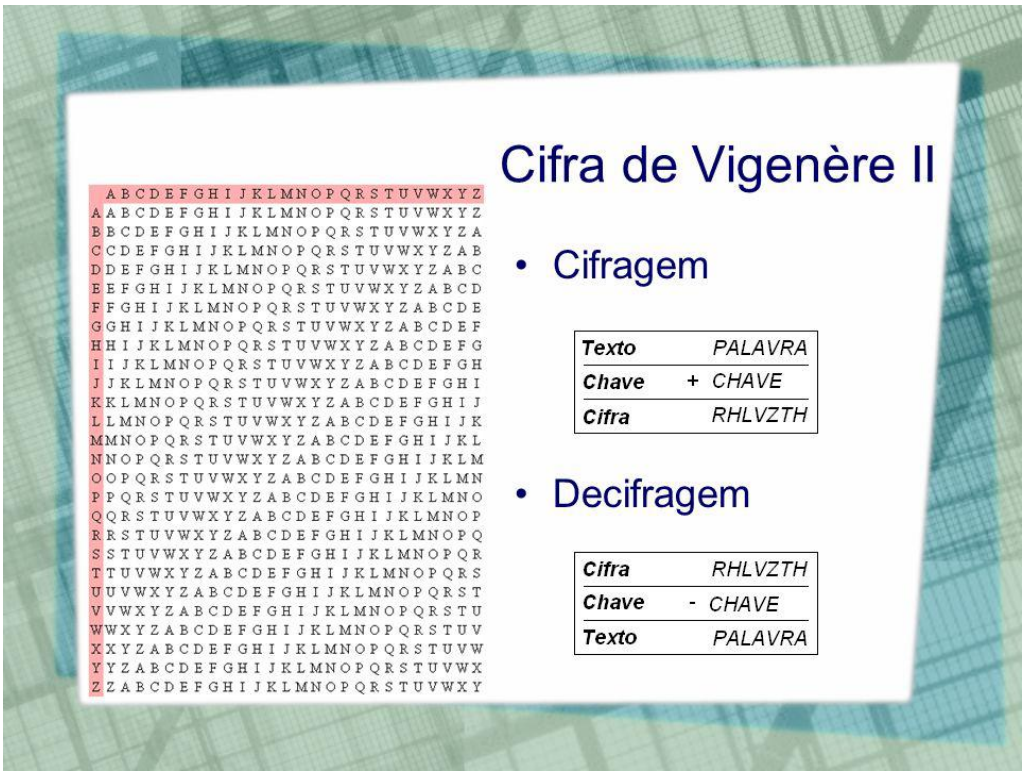
Ahmad al-Qalqashandi (1355–1418) escreveu o *Subh al-a 'sha*, uma enciclopédia de 14 volumes, que incluía uma seção sobre criptologia. Esta informação foi atribuída a Taj ad-Din Ali ibn ad-Duraihim ben Muhammad ath-Tha 'alibi al-Mausili que viveu de 1312 a 1361, mas cujos trabalhos em criptografia perderam-se. A lista de cifras nesta obra incluía a de substituição e a de transposição, e pela primeira vez, a cifra de múltiplas substituições para cada letra da mensagem de puro-texto. São também atribuídos a Ibn al-Duraihim uma exposição em criptoanálise e um exemplo, incluindo o uso de tabelas de frequência de letras e conjuntos de letras que não podem aparecer juntas em uma palavra.

Tabela 1 - tabelas de frequência de letras e conjuntos de letras - https://pt.wikipedia.org/wiki/Frequ%C3%AAncia_de_letras

Letra	Francês [8]	Alemão [9]	Espanhol [10]	Português [11]
a	7636%	6.51%	12.53%	14.63%
b	0.901%	1.89%	1.42%	1.04%
c	3260%	3.06%	4.68%	3.88%
d	3669%	5.08%	5.86%	4.99%
e	14715%	17.40%	13.68%	12.57%
f	1066%	1.66%	0.69%	1.02%
g	0.866%	3.01%	1.01%	1.30%
h	0.737%	4.76%	0.70%	1.28%
i	7529%	7.55%	6.25%	6.18%
j	0.545%	0.27%	0.44%	0.40%

k	0.049%	1.21%	0.01%	0.02%
l	5456%	3.44%	4.97%	2.78%
m	2968%	2.53%	3.15%	4.74%
n	7095%	9.78%	6.71%	5.05%
o	5378%	2.51%	8.68%	10.73%
p	3021%	0.79%	2.51%	2.52%
q	1362%	0.02%	0.88%	1.20%
r	6553%	7.00%	6.87%	6.53%
s	7948%	7.27%	7.98%	7.81%
t	7244%	6.15%	4.63%	4.34%
u	6311%	4.35%	3.93%	4.63%
v	1628%	0.67%	0.90%	1.67%
w	0.114%	1.89%	0.02%	0.01%
x	0.387%	0.03%	0.22%	0.21%
y	0.308%	0.04%	0.90%	0.01%
z	0.136%	1.13%	0.52%	0.47%

Essencialmente, todas as cifras continuaram vulneráveis a técnica de criptografia de análise de frequência até o desenvolvimento da cifra polialfabética, e muitos permaneceram assim posteriormente. A cifra polialfabética foi melhor explicada por Leon Battista Alberti por volta do ano 1467, por isso ele foi chamado de "pai da criptologia Ocidental". Johannes Trithemius, em sua obra *Poligraphia*, inventou a tabula recta, uma componente crítica da cifra de Vigenère. O criptógrafo



francês Blaise de Vigenère inventou um sistema polialfabético prático que leva seu nome, a cifra de Vigenère.

Na Europa, criptografia tornou-se (secretamente) mais importante como uma consequência da competição política e da revolução religiosa. Por exemplo, na Europa durante e após o Renascimento, cidadãos de vários estados italianos - Estados Pontifícios e a Igreja Católica Romana, inclusive - foram responsáveis pela rápida proliferação de técnicas de criptografia, algumas das quais refletem o entendimento (ou mesmo conhecimento) do progresso polialfabético de Alberti. 'Cifras avançadas', mesmo depois de Alberti, não eram tão avançadas como seus inventores / desenvolvedores / usuários afirmavam (e até acreditavam). Elas foram regularmente quebradas. Este excesso de otimismo pode ser inerente em criptografia para ele era então, e permanece até hoje, fundamentalmente difícil saber com precisão o grau de vulnerabilidade do seu sistema é realmente. Na ausência de conhecimento, as suposições e esperanças, como seria de esperar, são comuns. Este excesso de otimismo pode ser inerente a criptografia pois era, e ainda é, fundamentalmente difícil saber com precisão o grau de vulnerabilidade de

Figura 19 - Cifra de Vigenére - https://slideplayer.com.br/slide/395381/

um sistema. Na ausência de conhecimento, as suposições e esperanças, como seria de esperar, são comuns.

Criptografia, criptoanálise, e traição de agente/mensageiro secreto destacaram-se na Conspiração de Babington, durante o reinado da Rainha da Inglaterra Elizabeth I, o que acabou na execução de Maria Stuart, Rainha da Escócia. Uma mensagem cifrada do tempo do Homem da Máscara de Ferro (decifrada logo antes de 1900 por Étienne Bazeries) lançou alguma luz sobre a identidade do prisioneiro, porém, infelizmente, não definitiva.

Fora da Europa, após o fim da Idade de Ouro muçulmano na mão dos mongóis, a criptografia permaneceu relativamente subdesenvolvida. A criptografia no Japão não parece ter sido utilizada até cerca de 1510, e técnicas avançadas não foram conhecidas até após a abertura do país ao Ocidente, no início da década de 1860. Durante a década de 1920, oficiais da Marinha polonesa ajudaram os militares japoneses no desenvolvimento de códigos e cifras.

Criptografia de 1800 a II Guerra Mundial

Embora a criptografia tenha uma história longa e complexa, até o século XIX não foi desenvolvido nada mais do que abordagens ad hoc para a criptografia ou criptoanálise (a ciência de encontrar fragilidades em sistemas de criptografia). Um exemplo é o trabalho de Charles Babbage, durante a Guerra da Crimeia, em análise matemática de cifras polialfabética, remodelado e publicado pouco depois

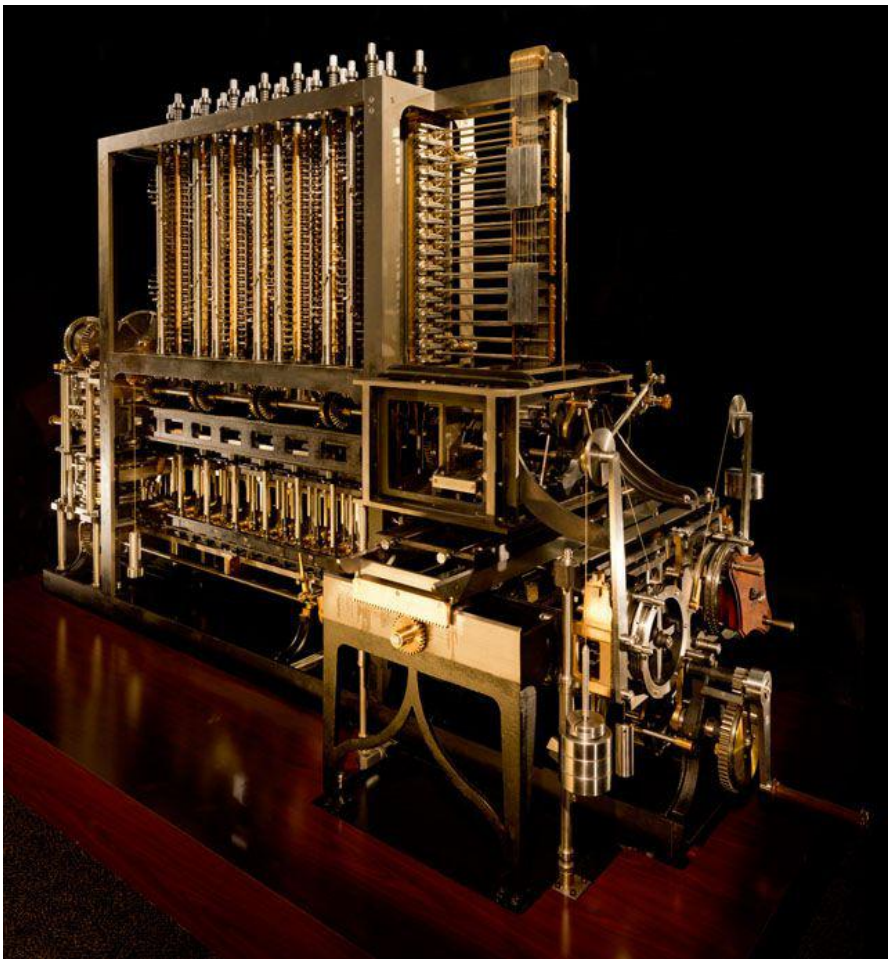


Figura 20 - Máquina de Charles Babbage - https://br.pinterest.com/pin/419397784020663364/

pelo Prússio Friedrich Kasiski.

A criptografia, neste momento, começa a se consolidar com regras consistentes; como, por exemplo, as encontradas nos escritos sobre criptografia de Auguste Kerckhoffs, no final do século XIX e na Constituição Americana passou a ser protegida no século XVIII. Edgar Allan Poe usou métodos sistemáticos para resolver enigmas na década de 1840. Em particular, ele colocou um anúncio de suas habilidades no jornal da Filadélfia *Alexander's Weekly (Express) Messenger*,

solicitando submissões das cifras, das quais ele passou a resolver quase tudo. Seu sucesso criou uma agitação pública por alguns meses.[7] Mais tarde, ele escreveu um ensaio sobre os métodos de criptografia, que tornou-se útil como uma introdução para os criptoanalistas britânicos na quebra dos códigos e cifras alemãs durante a I Guerra Mundial, e uma história famosa, *O Escaravelho de Ouro*, onde a criptoanálise era um elemento de destaque.

2. MAU USO DA CRIPTOGRAFIA

Criptografia, e seu uso incorreto, estiveram envolvidos na conspiração que levou à execução de Mata Hari e na conivência que levou à farsa da condenação e prisão de Dreyfus, no início do século XX. Felizmente, criptógrafos também estavam envolvidos em expor as maquinações que originaram os problemas de Dreyfus; Mata Hari, em contrapartida, foi baleada.

Na Primeira Guerra Mundial a Sala 40 do Almirantado quebrou os códigos navais alemães e desempenhou um papel importante em vários combates navais durante a guerra, particularmente na detecção de grandes missões alemãs no Mar do Norte que levou às batalhas de Dogger Bank e Jutlândia, já que a frota britânica foi enviada para interceptá-los. No entanto sua contribuição mais importante provavelmente foi em decodificar o Telegrama Zimmermann, um telegrama do Ministério do Exterior alemão enviado via Washington para o seu embaixador Heinrich von Eckardt] no México, que desempenhou um papel importante na entrada dos Estados Unidos na guerra.

Em 1917, Gilbert Vernam propôs uma cifra de teletipo em que uma chave previamente preparada, mantida em fita de papel, é combinada caractere a caractere com a mensagem de puro-texto para produzir o texto cifrado. Isto levou ao desenvolvimento de dispositivos eletromecânicos como máquinas de cifra.

Métodos matemáticos foram desenvolvidos no período anterior à Segunda Guerra Mundial (particularmente na aplicação de técnicas estatísticas para criptoanálise e desenvolvimento de cifras de William F. Friedman e na ruptura inicial da versão do Enigma do Exército Alemão por Marian Rejewski) em 1932.

Criptografia na II Guerra Mundial

O Enigma foi amplamente usado pela Alemanha Nazista; sua criptoanálise pelos Aliados deu origem a Ultra Inteligência.

Até a Segunda Guerra Mundial, as máquinas de codificação mecânica e eletromecânica estavam em uso, embora - onde essas máquinas eram impraticáveis - sistemas manuais ainda eram utilizados. Grandes avanços foram feitos, tanto na concepção de cifras quanto na criptoanálise, tudo em sigilo. Informações sobre esse período começou a ser desclassificado como o período de segredo oficial britânico de 50 anos terminou, como os arquivos dos EUA abriu lentamente, e como memórias sortidas e artigos foram publicados. Informações sobre esse período começaram a ser desclassificadas assim que o período de

segredo oficial britânico de 50 anos terminou, os arquivos dos EUA serem abertos e as memórias e artigos terem sido publicados.

Os alemães fizeram uso pesado, em várias versões, de um rotor eletromecânico conhecido como Enigma. O matemático Marian Rejewski, no escritório de cifras da Polônia, em dezembro de 1932 deduziu a estrutura detalhada do Enigma do exército alemão, usando matemática e documentação

Figura 21 -Marian Rejewski - Instytut Pamięci Narodowej

limitada fornecida pelo capitão Gustave Bertrand da inteligência militar francesa.

Esse foi o maior avanço na criptoanálise em mais de mil anos, segundo o historiador David Kahn. Rejewski e seus colegas matemáticos do escritório de cifras, Jerzy Rozycki e Henryk Zygalski, continuaram a estudar o Enigma e acompanharam a evolução dos componentes da máquina do exército alemão e seus procedimentos de codificação.

Como os recursos dos poloneses tornaram-se escassos devido às alterações introduzidas pelos alemães, e como a guerra se aproximava, o escritório de cifras, sob as instruções do Estado-Maior polonês, em 25 de julho de 1939, em Varsóvia, representantes da inteligência francesa e britânica começaram a trabalhar nos segredos da decodificação do Enigma.

Logo após o estopim da Segunda Guerra Mundial em 1 de setembro de 1939, o pessoal-chave do escritório de cifras foi evacuado em direção ao sudeste, em 17 de setembro, quando a União Soviética atacou a Polônia, eles cruzaram a fronteira com a Romênia.

De lá eles chegaram a Paris, França; na estação de inteligência franco-polonesa, PC Bruno, próxima a Paris, eles continuaram quebrando o Enigma, colaborando com criptógrafos britânicos em Bletchley Park, já que os ingleses já

tinham agilidade na quebra do Enigma. Na devida altura, os criptógrafos britânicos (muitos deles mestres de xadrez e matemáticos, tais como William Gordon Welchman, Max Newman e Alan Turing, fundador conceitual da computação moderna) fizeram um progresso substancial na tecnologia de decodificação do Enigma.

Figura 22 - Bletchley Park - https://www.hisour.com/pt/bletchley-park-buckinghamshire-united-kingdom-47703/

No final da guerra, em 19 de abril de 1945, os oficiais militares superiores da Grã-Bretanha foram informados de que eles nunca poderiam revelar que a cifra Enigma alemã tinha sido quebrada, pois daria ao inimigo derrotado a chance de dizer que "não foram bem e bastante espancados".

Criptógrafos da Marinha dos Estados Unidos (com a colaboração de criptógrafos ingleses e holandeses depois de 1940) invadiram vários sistemas de criptografia da Marinha Japonesa.

A quebra de um deles, JN-25, levou à vitória dos EUA na Batalha de Midway; e o fato foi publicado no Chicago Tribune logo após a batalha, embora os japoneses pareciam não ter notado, porque continuaram a usar o sistema JN-25.

Figura 23 - sistema JN-25 - https://www.historiassegundaguerramundial.com/anecdotario/anecdotas-inteligencia-militar/page/2/?lang=pt

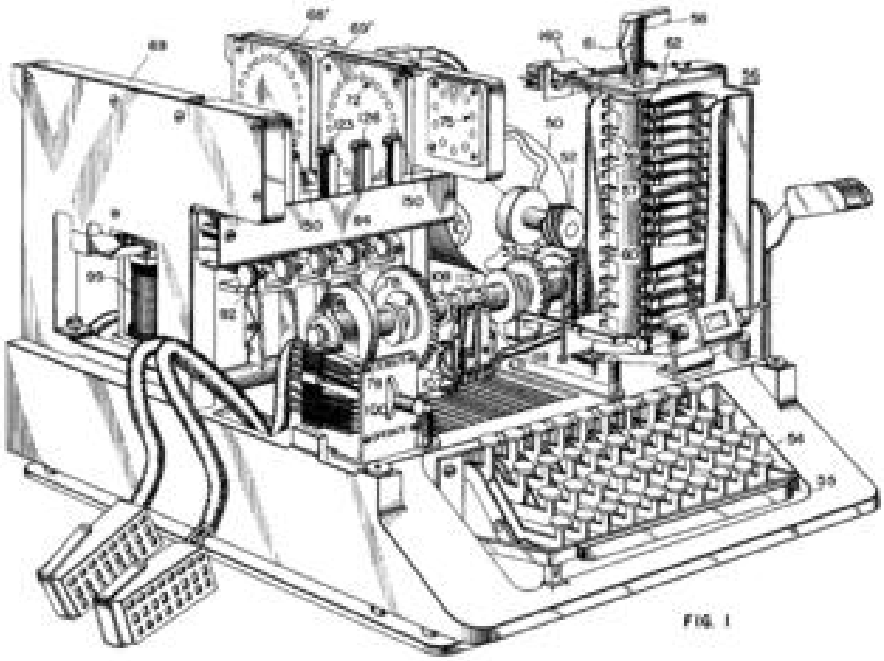
Figura 24 - Sistema JN 25

Um grupo do Exército dos EUA, o SIS (Serviço de Inteligência de Sinais), conseguiu quebrar o mais seguro sistema de codificação diplomática japonês (uma máquina eletromecânica 'telerruptor' chamada pelos americanos de Purple), mesmo antes da Segunda Guerra Mundial começar. Os americanos se referem à inteligência resultante da criptoanálise, talvez especialmente a partir da máquina Purple, como 'Magic'. O que os ingleses chamam de 'Ultra', particularmente a partir de tráfego de mensagens protegidas pelas diversas versões do Enigma. Um termo britânico anterior para Ultra tinha sido 'Boniface', na tentativa de sugerir, se traído, que poderia ter um agente individual como uma fonte.

Os militares alemães também implantaram várias máquinas mecânicas em one-time pad. Bletchley Park chamou as cifras de FISH, e Max Newman e seus colegas projetaram e implantaram o Heath Robinson, o primeiro computador digital eletrônico programável, o Colossus, para ajudar com sua criptoanálise. O Ministério do Exterior alemão começou a usar o one-time pad em 1919; parte do tráfego foi lido na Segunda Guerra Mundial, como resultado da recuperação de uma parte do conjunto de chaves, na América do Sul, que foi descartado displicentemente por um mensageiro alemão.

O Ministério das Relações Exteriores japonês utilizou um sistema desenvolvido localmente baseado no telerruptor elétrico (chamado de Purple pelos EUA), e tinha usado várias máquinas semelhantes para agregar algumas embaixadas japonesas. Uma delas foi chamada de 'M-machine' pelos EUA, outra

máquina era conhecida como 'Red'. Todas foram quebradas, de uma forma ou de outra, pelos Aliados.



SIGABA é descrito na Patente dos EUA 6.175.625, arquivado em 1944 mas somente emitido em 2001.

Entre as máquinas de codificação dos Aliados usadas na Segunda Guerra Mundial estão a britânica TypeX e a americana SIGABA; ambas eram rotores eletromecânicos semelhantes ao Enigma, mas com grandes melhorias. Nem uma nem outra foi quebrada durante a guerra. Os poloneses utilizaram a máquina Lacida, mas a sua segurança foi classificada como abaixo do que devia (pelos criptógrafos do Exército Polonês no Reino Unido), e seu uso foi interrompido. As tropas dos EUA no campo usavam o M-209 e ainda, o menos seguro, M-94. Agentes britânicos do SOE usavam inicialmente "cifras poema" (poemas memorizados eram as chaves de encriptação/desencriptação), mas mais tarde durante a Segunda Guerra, eles modificaram para o one-time pad.

A cifra de VIC (usada pelo menos até 1957, associada ao espião Rudolf Abel) foi uma cifra de mão muito complexa, e muitos afirmam ser a cifra mais complicada que foi utilizada pelos soviéticos, de acordo com David Kahn em *Kahn on Codes*.

Criptografia moderna

O uso da matemática em criptografia e criptoanálise tem avançado desde a Segunda Guerra Mundial. Mesmo assim, só foi possível a utilização eficaz da

criptografia para aplicações usuais, através da ampla utilização de computadores e da Internet como um meio de comunicação. Antes a criptografia era utilizada apenas por governos ou grandes empresas.

1. Shannon

A era da criptografia moderna começa realmente com Claude Shannon, indiscutivelmente o pai da criptografia matemática, com o trabalho que ele fez durante a Segunda Guerra Mundial sobre a segurança das comunicações. Em 1949 ele publicou *Communication Theory of Secrecy Systems* no *Bell System Technical Journal* e um pouco mais tarde o livro *The Mathematical Theory of Communication*, com Warren Weaver.[9] Ambos abordavam os resultados de seu trabalho na Segunda Guerra Mundial. Estes, além de outros trabalhos em teoria da informação estabeleceram uma sólida base teórica para a criptografia e também para grande parte da criptoanálise. E com isso, a criptografia desapareceu em parte das comunicações de organizações secretas do governo como a NSA, GCHQ, e seus equivalentes em outros lugares. Muito pouco trabalho tornou-se público novamente até meados da década de 1970, quando tudo mudou.

2. Um padrão de criptografia

Em meados da década de 1970 houve dois grandes avanços públicos (ou seja, não-secreto). Primeiro foi a publicação do projeto DES no *Registo Federal* dos EUA em 17 de março de 1975.

A cifra DES proposta foi apresentada por um grupo de pesquisa da IBM, a convite do National Institute of Standards and Technology (agora NIST), em um esforço para desenvolver instalações seguras de comunicações eletrônicas para as empresas, como bancos e outras grandes organizações financeiras.

Depois de "conselhos" e modificações introduzidas pelo NSA, agindo nos bastidores, que foi aprovado e publicado como FIPS publicado em 1977 (atualmente em FIPS 46-3). DES foi a primeira cifra publicamente acessível a ser "abençoada" por uma agência nacional, como a NSA. A liberação de sua especificação pelo NBS estimulou uma explosão de interesse público e acadêmico em criptografia.

O antigo DES foi oficialmente substituído pelo AES em 2001, quando NIST anunciou FIPS 197. Depois de um concurso, o NIST selecionou Rijndael, apresentado por dois criptógrafos belga, para ser o AES. DES, e variantes mais seguras dele (como a 3DES), são usadas ainda hoje, tendo sido incorporado em muitos padrões nacionais e organizacionais. No entanto, o seu tamanho de chave de 56 bits tem se mostrado insuficiente para evitar ataques de força bruta (um certo ataque, empreendido pelo grupo de direitos civis EFF, em 1997, conseguiu em 56 horas.[10]).

Em consequência, o uso da cifra DES é, sem dúvida, inseguro para uso em novos projetos de criptografia, e as mensagens protegidas por sistemas de encriptação mais velhos usando DES, ou seja, as mensagens enviadas a partir de 1976 usando DES, também estão em risco. Independentemente da qualidade intrínseca da cifra DES, o seu tamanho de chave (56 bits) foi considerado muito pequeno por alguns, mesmo em 1976, principalmente por Whitfield Diffie. Havia suspeitas de que organizações governamentais até então tinha poder computacional suficiente para quebrar mensagens DES; claramente outros alcançaram essa capacidade.

Figura 25 -Diffie & Hellman Receive the 2015 Turing Award

3. Chave pública

O próximo conceito, em 1976, foi talvez ainda mais importante, pois mudou fundamentalmente a forma como sistemas de criptografia funcionam. Surgiu com a publicação do artigo New Directions in Cryptography de Whitfield Diffie e Martin Hellman. Eles introduziram um método radicalmente novo de distribuição de chaves criptográficas, que ia em direção a solução de um dos problemas fundamentais da criptografia, distribuição de chaves, e tornou-se conhecido como Diffie-Hellman. O artigo também estimulou o desenvolvimento público quase que

imediato de uma nova classe de algoritmos de cifragem, os algoritmos de chave assimétrica.

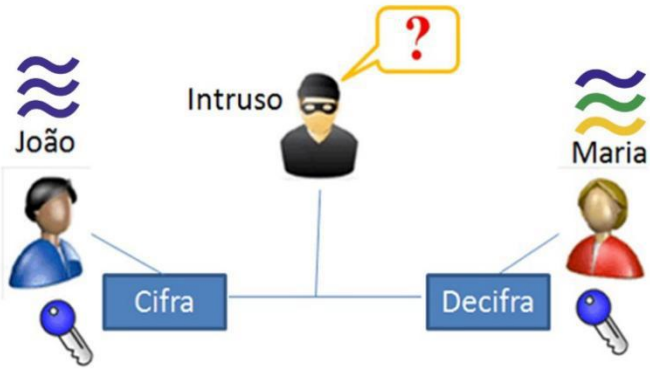


Figura 26- Chave pública - https://libracoinbrasil.com/libra-chave-publica/

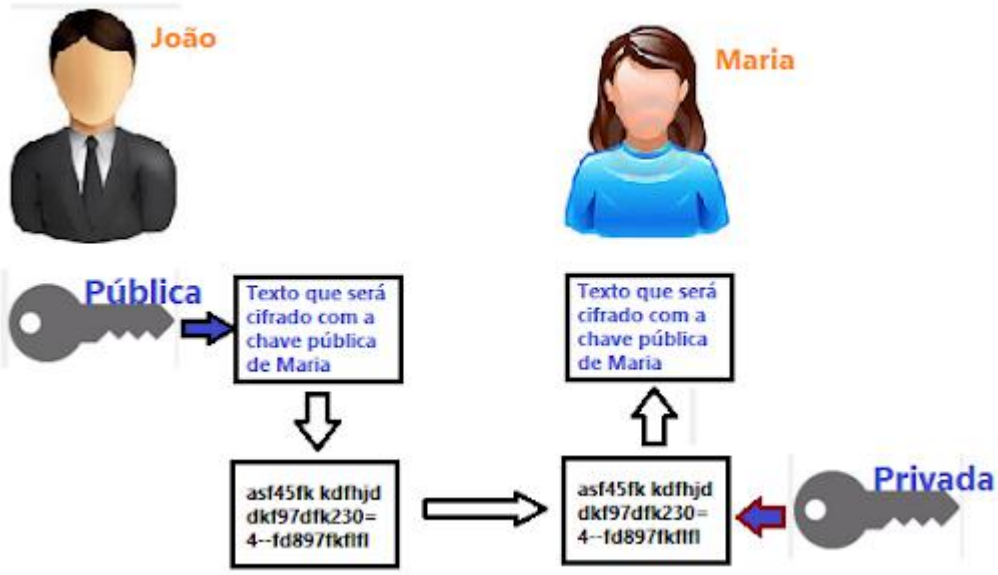


Figura 27 - Algoritmos de chave Assimétrica - http://www.macoratti.net/Cursos/Cripto/net_cripto5.htm

Antes disso, todos os algoritmos de cifragem modernos tinham sido algoritmos de chaves simétricas, no qual a mesma chave criptográfica é usada com o algoritmo oculto definido pelo remetente e pelo destinatário, e que deve ser

Figura 28 - Chaves assimétricas - https://www.gta.ufrj.br/grad/07_2/delio/Criptografiaassimtrica.html

mantido em segredo. Todas as máquinas eletromecânicas utilizadas na Segunda Guerra Mundial foram desta categoria lógica, como foram as cifras de César e a Atbash e essencialmente todos os sistemas de codificação ao longo da história. A "chave" para um código é, naturalmente, o livro de códigos, que também deve ser

distribuído e mantido em segredo, assim acontece com a maioria dos problemas na prática.

Por necessidade, a chave em cada sistema, teve que ser trocada entre as partes comunicantes de alguma forma segura antes da utilização do sistema (o termo normalmente usado é 'através de um canal seguro'), como um mensageiro de confiança com uma maleta algemada ao pulso, ou um contato face a face, ou um pombo-correio leal. Esta exigência não é trivial e muito rapidamente se torna incontrolável à medida que o número de participantes aumenta, ou quando os canais seguros não estão disponíveis para a troca de chaves, ou quando, como é prática sensata de criptografia, as chaves são frequentemente alteradas. Em particular, se as mensagens são destinadas a não serem lidas por outros usuários, uma chave isolada é necessária para cada par possível de usuários. Um sistema deste tipo é conhecido como uma chave secreta ou sistema criptográfico de chave simétrica. O método Diffie-Hellman (e sucessivas melhorias e variantes) faz as operação desses sistemas de modo muito mais fácil e mais seguro, o que nunca foi possível antes em toda a história.

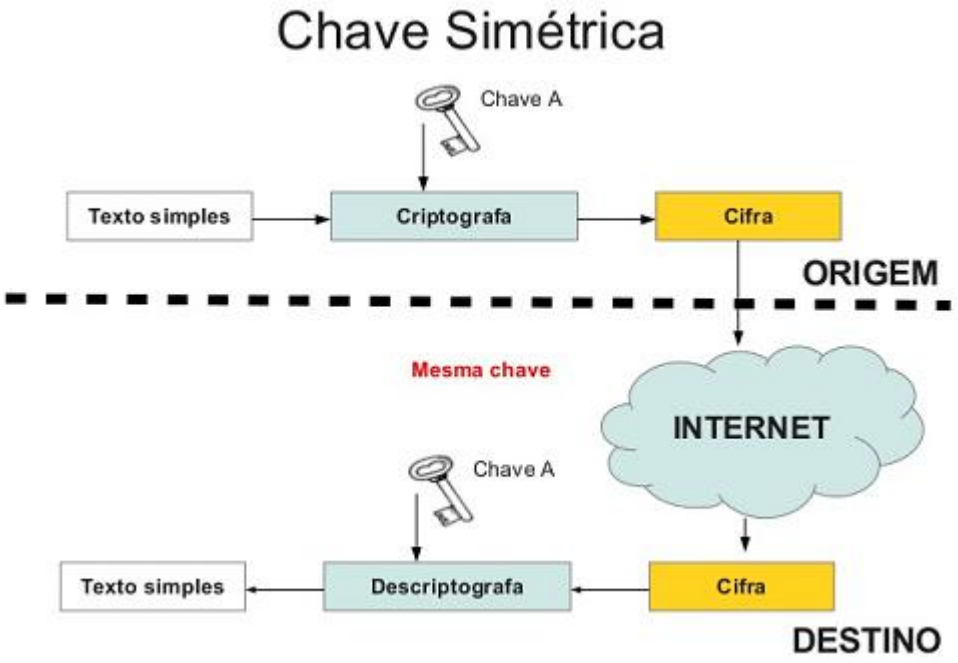


Figura 29 - Algoritmos de Chave Simétrica - http://www.macoratti.net/Cursos/Cripto/net_cripto4.htm

Em contraste, a criptografia de chave assimétrica utiliza um par de chaves matematicamente relacionadas, onde cada uma delas decifra a criptografia usando a outra. Alguns, mas não todos, destes algoritmos têm a propriedade adicional de

que uma das chaves do par não pode ser deduzida a partir da outra por qualquer método conhecido, além de tentativa e erro. Um algoritmo deste tipo é conhecido como sistema de chave pública ou sistema de chave assimétrica. Usando esse algoritmo, apenas um par de chaves é necessário por usuário. Ao designar uma das chaves do par como privada (sempre em segredo), e a outra como pública (muitas vezes disponível), nenhum canal seguro é necessário para a troca de chaves. Enquanto a chave privada permanece secreta, a chave pública pode ser conhecida por um tempo muito longo sem comprometer a segurança, tornando-o seguro para reutilizar o mesmo par de chaves indefinidamente.

Para dois usuários de um algoritmo de chave assimétrica se comunicarem de forma segura por um canal inseguro, cada usuário deverá conhecer as suas chaves públicas e privadas, bem como a chave pública do outro usuário. Considere este cenário básico: Alice e Bob têm um par de chaves já utilizadas durante anos com muitos outros usuários. No início da mensagem, eles trocam chaves públicas, não cifradas através de uma linha insegura. Alice, em seguida, cifra uma mensagem usando sua chave privada, e então cifra esse resultado usando a chave pública de Bob. A mensagem duplamente cifrada é então enviada como dados digitais através de um fio de Alice para Bob. Bob recebe o fluxo de bits e decodifica-o usando sua própria chave privada, e depois decodifica o novo fluxo de bits usando a chave pública de Alice. Se o resultado final for reconhecido como uma mensagem, Bob pode estar confiante de que a mensagem veio realmente de alguém que conhece a chave privada de Alice (presumivelmente dela mesma, se ela tem sido cuidadosa com sua chave privada), e de que qualquer abelhudo no canal iria precisar da chave privada de Bob para compreender a mensagem.

Algoritmos assimétricos dependem, para a sua eficiência, de uma classe de problemas de matemática chamada de função unidirecional, que exigem relativamente pouco poder computacional para ser executada, mas muito poder computacional para inverter, se a inversão for possível. Um exemplo clássico de uma função unidirecional é a multiplicação de números primos muito grandes. É bastante rápido determinar o produto de dois primos grandes, mas muito difícil de encontrar os fatores do produto de dois primos grandes. Por causa das funções unidirecionais, a maior parte do conjunto de chaves possíveis são más escolhas para chaves de sistemas de criptografia; apenas uma pequena fração das possíveis chaves de um determinado comprimento é apropriada, e os algoritmos assimétricos exigem chaves muito longas para atingir o mesmo nível de segurança fornecido por chaves simétricas mais curtas. A necessidade de gerar os pares de

chaves e executar as operações de codificação e decodificação fazem com que os algoritmos assimétricos se tornem computacionalmente caros, em comparação com a maioria dos algoritmos simétricos. Uma vez que algoritmos simétricos geralmente podem usar qualquer sequência de (aleatória, ou pelo menos imprevisível) bits como uma chave, uma *chave de sessão* disponível pode ser rapidamente gerada para uso a curto prazo. Em consequência, é comum usar uma chave assimétrica longa no lugar de uma chave simétrica disponível, muito mais curta e também mais forte. O algoritmo assimétrico mais lento envia uma chave de sessão simétrica, e o algoritmo simétrico mais rápido assume o controle para o restante da mensagem.

A criptografia de chave assimétrica, o método Diffie-Hellman, e os mais conhecidos algoritmos de chave pública e privada (isto é, o que normalmente é chamado de algoritmo RSA) possivelmente foram desenvolvidos de forma independente em uma agência de inteligência do Reino Unido antes do anúncio público por Diffie e Hellman em 1976. GCHQ liberou os documentos alegando que eles tinham desenvolvido a criptografia de chave pública antes da publicação do artigo de Diffie e Hellman. Vários artigos confidenciais foram escritos no GCHQ durante os anos 1960 e 1970 que levaram a esquemas essencialmente idênticos ao de criptografia RSA e do método Diffie-Hellman em 1973 e 1974. Alguns destes já foram publicados, e os inventores (James H. Ellis, Clifford Cocks e Malcolm Williamson) tornaram públicos (parte de) seus trabalhos.

4. Política de criptografia

A evolução do público da década de 1970 quebrou o monopólio sobre a criptografia de alta qualidade realizado por organizações governamentais (ver *Crypto* de Steven Levy, relato jornalístico de algumas controvérsias políticas da época nos EUA). Pela primeira vez, as organizações de fora do governo tiveram acesso a criptografia de alta qualidade, que não seria quebrada nem mesmo pelo governo. controvérsias e conflitos consideráveis, tanto públicos como privados, surgiram após a quebra do monopólio sobre a criptografia. E ainda continuam. Em muitos países, por exemplo, a exportação de criptografia está sujeita a restrições. Até 1996, exportação de criptografia dos EUA que usava chaves de mais de 40 bits (muito pequena para ser segura contra um invasor experiente) foi severamente limitada. Em 2004, o ex-diretor do FBI, Louis Freeh, testemunhou perante a Comissão do 11 de Setembro, realizada para a definição da nova legislação contra a utilização pública de criptografia.

Uma das pessoas mais significativas a favorecer a criptografia de qualidade para uso público foi Phil Zimmermann. Ele escreveu e, em 1991, lançou o PGP (privacidade bastante boa), um sistema criptográfico de altíssima qualidade. Ele distribuiu uma versão gratuita do PGP, quando se sentiu ameaçado pela legislação do governo dos EUA que exigia a inclusão de Porta dos fundos em todos os produtos de criptografia desenvolvido dentro dos EUA. Seu sistema foi lançado mundialmente logo depois que ele lançou nos EUA, e então iniciou-se uma longa investigação criminal contra ele pelo Departamento de Justiça do Governo dos EUA, pela suposta violação das restrições à exportação. O Departamento de Justiça, posteriormente, retirou o processo contra Zimmermann, e a distribuição gratuita do PGP continuou ao redor do mundo. PGP acabou por se tornar um padrão IETF aberto (RFC 2440 ou OpenPGP).

5. Criptoanálise moderna

Embora as cifras modernas, como a AES e as cifras assimétricas de altíssima qualidade são amplamente consideradas inquebráveis , projetos e implementações fracos ainda são por vezes adotados e ainda existem quebras de sistemas de criptografia implementados nos últimos anos. Exemplos notáveis de projetos de criptografia quebrados incluem o primeiro esquema de criptografia Wi-Fi, WEP, o Content Scramble System usado para cifrar e controlar o uso de DVD, as cifras A5/1 e A5/2 usadas em telefones celulares GSM, e a cifra CRYPTO1 utilizada amplamente nos cartões inteligentes MIFARE Classic da NXP Semiconductors, uma divisão desmembrada da Philips Electronics. Todas elas são cifras simétricas. Até agora, nenhuma das ideias matemáticas da criptografia de chave pública foram provadas serem "inquebráveis", sendo assim algum avanço na análise matemática pode tornar os sistemas dependente dessas ideias, inseguros. Enquanto alguns observadores bem informados prevêem esse avanço, o tamanho da chave recomendado para a segurança como uma boa prática continua aumentando à medida que a capacidade computacional necessária para quebrar códigos se torna mais barata e disponível.

Referências bibliográficas

1. Dulaney E. CompTIA Security+ study guide. 2011.
2. Bell DE. Looking back at the bell-La padula model. Proc - Annu Comput Secur Appl Conf ACSAC. 2005;2005:337–51.
3. Tittel E. CISSP : Study Guide. 2003.
4. Cannon, David L.; Bergmann, Timothy S.; Pamplin B. CISA - Certified Information Systems Auditor - Study Guide. Wiley Publishing I, editor. Indianapolis, Indiana; 2006.
5. Dulaney E. Comptia security + study guide: sy0-401. Sons JW and, editor. Indianapolis; 2014.
6. Krutz RL. The CISSP® prep guide. Gold 2ª Ed. Wiley Publishing I, editor. Indianapolis, Indiana; 2003.
7. Krutz RL&, Vines RD. The CISSP Prep Guide : Russell The Journal Of The Bertrand Russell Archives. 2003.
8. Peixoto MCP. Engenharia Social e Segurança da Informação na Gestão Corporativa. Brasport, editor. Rio de Janeiro; 2006.
9. Prof. Ricardo F. Custódio. Criptografia e Segurança em Redes de computadores.
10. Harris S. CISSP® All-in-One Exam Guide, Fourth Edition. The McGraw-Hill Companies., editor. Chicago; 2008.
11. Cbk C. No Title.
12. Meyers M. CompTIA A+ Certification All-in-One Exam Guide, 8th Edition. 8th ed. New York: McGraw-Hill Osborne Media; 2012.
13. Bhardwaj PK. A+, Network+, Security+ Exams - In A Nutshell. 2007. 813 p.
14. Dulaney E. CompTIA Security+ study guide. 2011;
15. Principios e conceitos de gerenciamento de segurança Principios de conceitos de gerenciamento de segurança.
16. Emmett Dulaney. CompTIA Security+ Deluxe Study Guide. 2011. 696 p.
17. James Michael Stewart, Ed Tittel MC. CISSP - Certified Information Systems Security Professional - Study Guide - Fourth Edition. Wiley Publishing I, editor. Indianapolis, IN; 2008.
18. <http://dan-scientia.blogspot.com.br/2012/03/modos-de-rede-no-virtualbox.html>