Unidade 1 – Introdução a Segurança da informação no Ambiente Corporativo

Conceitos de segurança

Dados

Em segurança da informação um dado é considerado uma informação que ainda não foi tratada, processada ou organizada.

Informações

São conjuntos organizados de dados, que constituem uma ou mais mensagens com um significado relacionado a algum tipo de evento.

Sistema de informação

É um sistema que reúne, armazena, processa e fornece informações relevantes para a organização, de modo que a informação seja acessível e útil para aqueles que pretendem utilizar.

Segurança da informação

É um conjunto de princípios, técnicas, protocolos, normas e regras que visam garantir um melhor nível de confiabilidade a um sistema de informação e. Tem como objectivo proteger a informação de diversos tipos de ameaças, garantindo assim a continuidade dos negócios, minimizando os danos e maximizando o retorno dos investimentos.

ISO 27001

É uma norma internacional publicada pela International Standardization Organization (ISO) que descreve como uma organização deve fazer a gestão da segurança da informação. Tem como objectivo principal atenuar e gerir melhor os riscos da organização.

Principios de segurança

Confidencialidade

Este principio garante que a informação é acedida por usuarios autorizadas.

Integridade

Este principio garante que a informação não sofreu alterações durante a sua transmissão

Disponibilidade

Este principio garante que o sistema estará sempre disponivel.

Autenticidade

Este principio garante que os dados fornecidos sejam os verdadeiros e que o usuario é legitimo.

Não Repudio

Este principio garante que a pessoa não negue ter assinado ou criado a informação.

Politicas de segurança

Conjunto de protocolos, regras e práticas que regulam como uma organização gere, protege e distribui suas informações e recursos computacionais. Nas políticas de segurança devem ser divulgados e abordados os seguintes aspectos:

- Procedimentos de prevenção e detecção de vírus;
- Principios legais que devem ser observado quanto á tecnologia da informação;
- Principios de supervisão constante das tentativas de violação da segurança da informação;
- Consequências da violação das normas estabelecidas na politica de segurança da informação;
- Objectivos de segurança da organização;
- Classificação das informações (irrestritas, internas, confidenciais e secretas);
- Politica de senhas e de cópias de segurança (Backup);
-

Processo de implementação de politicas de segurança

Este processo esta dividido nas seguintes fases:

1. Análise das necessidades de segurança
2. Elaboração da proposta de politica de segurança
3. Discuções abertas com os envolvidos
4. Apresentação de um documento formal à alta administração
5. Aprovação da politica de segurança
6. Publicação da politica de segurança
7. Divulgação da politica de segurança
8. Treinamento dos envolvidos
9. Implementação da politica de segurança
10. Avaliação e identificação das mudanças necessárias
11. Revisão da politica de segurança.

Consequências da violação da politica de segurança

Não existe uma punição ou penalização geral para todos os casos em que a politica de segurança da informação é violada.

No documento formal da politica de segurança devem estar previstos procedimentos a serem adoptados para cada caso de violação especifico, de acordo com:

- Severidade do caso
- Amplitude da violação
- Tipo de infractor

A punição pode ser uma simples advertência verbal ou escrita ou até uma acção judicial (processo) depepndedo dos factores acima descritos.

Processo de alteração, revisão e actualização da pólitica de segurança

Com intuito de melhorar a segurança dos sistemas e do ambiente computacional, a politica de segurança deve:

- Ser alterada periodicamente
- Passar por um processo regular de revisão garantindo que caso ocorra qualquer mudança que Venha afectar a analise de risco inicial.
- Garantir que novas vulnerabilidades, mudanças organizacionais ou mudanças da infra-extrutura tecnológica estejam actualizadas na politica de segurança da informação.
- Haver análise periódica da efectividade da pólitica, demostrada pelo volume e impacto dos incidetes de segurança registados.

Controle de acesso

É uma tecnica composta por processos de autenticação, autorização e auditoria de contas de usuarios no sistema de gestão da segurança da informação. Tem como objectivo principal proteger equipamentos, aplicativos e arquivos de dados contra perda, modificação ou divulgação não autorizada.

Existem 2 tipos de controle de acesso : logicos e fisicos;

Controle de acesso logico

É um conjunto de procedimentos e medidas com o objectivo de proteger dados, programas e sistemas contra tentativas de acesso não autorizado feitas por pessoas ou outros programas de computador.

Os controles de acesso lógico são implantados com objectivo de garantir que:

- Apenas usuários autorizados tenham acesso aos recursos computacionais
- Os usuários tenham acesso apenas aos recursos realmente necessários para execuçao de suas tarefas
- O acesso aos recursos crítivos do sistema deve ser monitorado e restrito;
- Os usuarios não possam executar transacções incompatíveis com a sua função.

Os recursos a serem protegidos pelo controle de acesso logico são:

- Aplicativos (programas, codigo-fonte e objecto) - porque acesso não autorizado ao codigo fonte dos aplicativos pode ser usado para alterar as funções e a lógica do programa;
- Arquivos de dados – porque evita que os dados (ex: arquivos de configuração do sistema) sejam apagados ou alterados sem autorização,

- Utilitários e o sistema operativo – porque o acesso a utilitarios, como softwares de manutenção, monitoramento e diagnostico podem ser usados para alterar o funcionamento do sistema.
- Arquivo de senha – porque pode comprometer todo o sistema, pois uma pessoa não autorizada, ao obter o identificador (ID) e a senha (Password) de um usuário previlegiado, pode intencionalmente, causar danos ao sistema.
- Arquivos de log – porque os arquivos de log são usados para registar acções dos usuários, constitui uma optima fonte de informação para auditorias futuras.

Como os usuários sçao identificados e autenticados?

Existe um processo denominado logon usado para conceder o acesso aos dados e aplicativos em um sistema computacional.

Um processo de logon eficiente deve:

- Informar que o computador só deve ser acessado por pessoas autorizadas;
- Evitar o fornecimento de mensagens de ajuda que poderiam facilitar ao usuario não autorizado a completar o procedimento;
- Validar a informação de logon apenas quando todos os dados de entrada estiverem completos e correctos;
- Limitar o número de tentativas de logon sem sucesso (recomenda-se no maximo 3 tentativas);
- Limitar o tempo máximo para o procedimento de logon, caso exceda o sistema deverá encerrar o procedimento:

Controle de acesso físico

Tem como objectivo proteger equipamentos e informações contra usuarios não autorizados, previnindo o acesso a esses recursos.

O controle de acesso fisico deve basear-se em perimetros predefinidos nas imediações dos recursos computacionais, podendo ser explicita como uma sala cofre, ou implicita, como áreas de acesso restrito e a mesma pode ser abordada sob duas formas:

- Segurança de acesso – que consiste na protecção do material fisico não a pessoas não autorizadas.
- Segurança ambiental – que trata da prevenção de danos por causas naturais.

Recomendações para o controle de acesso fisico:

- Instalar sistemas de protecção e vigilância 24 Horas.x 7 dias por semana.
- Não instalar em áreas de acesso publico equipamentos que permitam o acesso á rede interna da organização.
- Orientar os funcionarios para não deixarem ligados os computadores quando se ausentarem por tempo prolongado.
- Utilizar mecanismos de controle de acesso físico em salas e áreas de acesso restrito (fechaduras, cameras, alarmes, etc).
- Proteger as linhas telefonicas internas e externas com dispositivos contra escuta.
- Proteger fisicamente as unidades de backup e restringir o acesso a computadores e impressoras que possam conter dados confidenciais.

Plano de continuidade de negócios

É um conjunto de estrategias e procedimentos que devem ser adoptados quando a instituição ou uma área depara-se com problemas que comprometem o funcionamento normal dos processos e a consequente prestação dos serviços.

Tem como objectivo garantir que o funcionamento dos sistemas informatizados seja restabelecdo ao menor tempo possivel a fim de reduzir os impactos causados por factos imprevistos.

Este plano está dividido em 3 modulos:

Plano de gestão de crises (PGC)

Define as tarefas das equipes envolvidas nas contigências incluindo procedimentos que devem ser realizados quando a empresa voltar á normalidade.

Exemplo: Estrategia de comunicação do facto ocorrido á imprensa.

Plano de contigência opeacional (PCO)

Define os procedimentos a fim de reduzir o tempo de indisponibilidade do serviços ou sistema.

Exemplo: Acções que devem ser tomadas em casos de queda de conexão com a internet.

Plano de recuperação de desastres (PRD)

Define o conjunto de cenários de desastres possiveis ou previamente ocorridos e os respectivos procedimentos de reacção para garantir que as actividades retomem a operação dentro de um prazo tolerável.

Exemplo: Centro de dados redundante.

Aspectos a ter em conta no processo de elaboração de um plano de continuidade de negocios

- Os riscos que a organização esta exposta.
- A probabilidade da ocorrência e os seus impactos.
- As consequências que poderão advir da interrupção de cada sistema computacional ou serviço.
- A identificação e priorização de recusos, sistemas e procecessos críticos.
- O tempo limite para recuperação dos recusos, sistemas e processos.
- As alternativas para recuperação dos recusos, sistemas e processos, mensurando os custos e beneficios de cada alternativa.

Aspectos a serem divulgados e abordados no plano de continuidade de negocios:

1. Condições e procedimentos para activação do plano
2. Procedimentos a serem seguidos imediatamente após a ocorrêencia de um desastre.
3. A instalação reserva, com especificação dos bens de informática nela disponiveis, como hardware, software e equipamentos de telecomunicações.
4. A escala de prioridade dos softwares, de acordo com o seu grau de interferencia nos resultados operacionais e financeiiros da instituição.
5. Arquivos, programas, procedimentos necessarios para que os aplicativos criticos entrem em operação ao menor tempo possivel mesmo que parcialmente.
6. Dependencia de recursos e serviços externos ao negócio.
7. Procedimentos necessarios para restaurar os serviços computacionais na instalação reserva.
8. Pessoas responsaveis por executar e comandar cada uma das actividades previstas no plano.

9. Instituções responsaveis por oferecer serviços, equipamentos, suprimentos ou qualquer outros bens necessarios para a restauração.
10. Contractos e acordos que façam parte do plano para recuperação dos serviços, como aqueles afectados com outros centros de processamento de dados.

Como garantir que o plano funcione como esperado:

- Treinamento e concientização dos envolvidos – O treinamento deve ser teórico e prático, inclusive com simulações garantindo que cada funcionario envolvido no plano, em caso de contigências, deve tr em mente as actividades que deve desempenhar em situações de emergência.
- Testes periódicos do plano – Devem assegurar que todos os envolvidos na recuperação e os alocados em outras funções criticas possuam conhecimento do plano.
- Processos de manutenção continua – Quando novos requisitos forem identificados, os procedimentos de emergencia relacionados devem ser ajustados de forma apropriada.

Unidade 2 – Controle Interno e Plano Director de Informática (PDI)

Conceitos de controle

Controle

Conjunto de procedimentos e métodos, com vista a verificar se as operações são realizadas conforme os principios estabelecidos.

Controle interno

Consiste num plano, métodos e medidas adoptados por uma organização com vista a salvaguardar os seus activos e verificar a exactidão e a fidedignidade dos seus dados.

Controle interno do sistema de informação

Tem em vista verificar diariamente se todas as actividade do sistema de informação estão a ser realizadas de acordo com os procedimentos definidos pela gestão de topo assim como os requesitos legais.

Comoponentes do sistema de controle interno

- Ambiente de controle – um conjunto de normas que caracterizam o funcionamento de uma entidade
- Avaliação de riscos - consiste em fazer levantamento de eventos que caso ocorram, impactam negativamente a condição da empresa em relação aos objectivos pré-estabelecidos.
- Procedimentos de controle – políticas e procedimentos que visam assegurar que as directrizes determinadas pela gestão de topo são cumpridas.
- Informação e comunicação – Permite que os funcionários recebam em tempo útil uma mensagem clara da alta administração de que as responsabilidades pelo controlo devem ser levadas a sério.
- Monitoria - a monitoria pela gestão de topo considera se o sistema de controlo interno está a operar como pretendido e se são modificados de forma apropriada quando as condições se alteram.

Finalidade do controlo interno no ambiente corporativo

Numa perspectiva da gestão de empresas o controle interno tem como objectivo final o seguinte:

1. Proteger os activos da organização.
2. Preservar a confidencialidade do sistema de informação e das suas informações.
3. Garantir a segurança ambiental (condições em que os recursos humanos realizam as operações – espaço físico, AC, seguros, equipamentos de escritório.
4. Manter a segurança lógica
5. Conseguir elevados níveis de eficácia, considerando o nível de satisfação do usuário e a adequação da informação obtida em função dos objectivos necessários à sua utilidade.
6. Manter a coerência das actividades com as orientações fornecidas pelas políticas da gestão de topo.

Limitações do controle interno

- Motivação por parte do orgão de gestão na manutenção de um bom sistema de contrele.
- A dimensão da empresa visto que a implementação de um bom sistema de controlo interno é mais dificil numa empresa com número reduzido de colaboradores. Ja que a segregação de funções, seria mais dificil de atingir.
- A relação custo/benefício é o outro aspecto a ter em conta, já que a implementação de um bom sistema de controle implica custos elevados, que podem superar os benefícios que dele se espera retirar.
- As transacções pouco usuais sendo que o controle interno desenhado para responder a uma determinada transacção. Aquelas que sejam pouco comuns não serão abrangidas pelo sistema de controle.
- Existência de erros humanos pois por mais sofisticado que o sistema de controlo interno seja, a sua eficiencia será sempre coloca em causa. Se em posições de maior responsabilidade não estiverem pessoas competentes moralmente e integras.

Principios fundamentais do controle interno

- Responsabilidade – As responsabilidades dos funcionarios devem estar claras, e de preferência por escrito
- Rotinas internas – Garante que todos processos e rotinas internas dos diferentes sectores estajam documenteados e actualizados.
- Acesso aos activos – O acesso aos activos de uma unidade deve ser limitado ao pessoal autorizado
- Segragação de funções – Os procedimentos destinados a detectar erros ou irregularidades no sistema, devem ser executados por pessoas que não estejam em posição de pratica-los
- Auditoria interna – Verifica se as normas internas são seguidas e se existe necessidade para modificação das já existentes.

Plano Director de Informática (PDI)

É um instrumento de diagnóstico, planeamento e getão dos recursos e processos relacionados a tecnologia da informação e comunicação (TICS). Tem como objectivo os seguintes :

- Atender as necesidades tecnológicas e de informações da instituição
- Permite alinhar o planeamento e a execução das acções de tecnologias de informação e comunicação aos objectivos da organização;

- Consolidar a importancia estrategica da area de tecnologia de informação e comunicação;

O plano director de informatica é normalmente desenvolvido para 5 anos mas recomenda-se que seja revisto anualmente.

Questões que devem ser abordadas no plano ditrector de informática

1. Qual é o cenario actual? Situação actual da organização (Meio interno e externo)
2. O que se pretende atingir? Visão da empresa (Tendências, Sustentabilidade, Inovação, ...)
3. Como atingir? Estratégia de acção (Actividades, ...)
4. Nivel de satisfação da empresa com o serviço de T.I ? Monitoria e avaliação (Desempenho. ...)

Ciclo PDCA [PLAN, DO, CHECK, ACT]

PLANEAR

Plan:
- Identificação do problema
- Escolha dos métodos
- Plano de Acção

FAZER

Do:
- Execução dos planos de acção
- Treinamento

Check:
- Verificação dos resultados

Act:
- Acções correctivas/ melhorias

VERIFICAR

AGIR

Possíveis dificuldades na execução do plano director de tecnologias de informação [PDTI] OU PDI

- O MERCADO, AS NOVAS TECNOLOGIAS E A ECONOMIA – Fazem com que o plano director de TI sofra ajustes, dificultando manter a coerência do plano com as estratégias, objectivos e directrizes dos usuários
- RESISTÊNCIA A MUDAÇAS POR PARTE DE ALGUNS FUNCIONARIOS – Incerteza por parte dos funcionários em relação ao emprego e aos valores ou perspectivas diferentes.
- DELEGAÇÃO DE AUTORIDADE E FALTA DE PARTICIPAÇÃO DA GESTÃP DE TOPO – Por acreditar que o assunto tratado, é extremamente técnico e dispensa sua colaboração.
- A FALTA DE DOCUMENTAÇÃO DOS SISTEMAS ANTERIORES – Dificulta muito na análise da situação actual, uma vez que se faz necessário o estudo dos sistemas que actualmente estão sendo utilizados na organização.

Consequências do não desenvolvimento de um plano de director de tecnologias de informação.

- Desenvolvimento de sistemas sem integração e documentação
- Mudanças nas prioridades da organização sem reavaliar o que já tem organizado
- Dimensionamento errado dos recursos humanos na área de Tecnologias de informação
- Implementação de sistemas malsucedidos
- Desmotivação dos profissionais da área

Unidade 3 – Introdução a Auditoria Informática

Conceitos

Auditoria

É uma actividade que consiste na emissão de uma opinião profissional sobre o objecto em análise, afim de confirmar se cumpre adequadamente as condições que lhe são exigidas.

Auditoria de Sistemas

É o processo de recolha e avaliação de evidencias com vista a saber e determinar se um sistema de informação salvaguarda os bens e mantém a integridade dos dados.

Auditoria de Sistemas de Informação

Tipos de auditoria de sistemas

A auditoria informática pode ser interna ou externa

- INTERNA se o auditor faz parte da empresa
- EXTERNA se o auditor for externo da empresa

Importancia da auditoria de sistemas

- Garante a integridade dos dados manipulados
- Estabelece e mantém procedimentos documentados para planeamento e utilização dos recursos computacionais da empresa, verificando aspectos de segurança e de qualidade
- Evita fradude e garante o bom desempenho do sistema de informação
- Auxilia a organização na avaliação e validação do ciclo administrativo
- Garante o alcance da qualidade dos sistemas

Fases da auditoria de sistemas

- PRÉ-AUDITORIA – Fase de planeamento da auditoria no qual se organiza a equipe de auditores e se envia para o sector a ser auditado um notificação acompanhada do plano de auditoria.
- AUDITORIA – Fase de inicio da auditoria no qual se realiza *reunião de abertura*, realização do *trabalhos de auditoria* de sistemas de informação e a *reunião de encerramento*.
- PÓS-AUDITORIA – Emissão do relatório de auditoria, planeamento de acções juntamente com o cliente e o acompanhamento das acções correctivas.

Perfil de um auditor informático

O auditor informático deve ter conhecimentos sobre vários frameworks de melhores praticas para realizar boas recomendações em seu trabalho;

- COBIT – Control Objectives for Information and Related Technologies
- PMBOK – Project Management Body of Knowledge
- ITIL – Information Technology Infranstruture Library / IT Service Management
- ISO27001 – Information Security Management
- CMMI – Capability Maturity Model Integration

Para alem dos frameworks acima listados deve ter conhecimentos em

- Desenvolvimento de Sistemas De Informação
- Gestão de Projectos
- Sistemas Operativos
- Linguagens de programação
- Auditoria de computação, conhecendo o ambiente a ser auditado
- Ter conhecimentos sobre o negocio da organização
- Segurança de sistemas

Aliado a esses requesitos o auditor informático deve

- Ter o maximo de cuidado com a gestão da informação
- Imparcialidade no juizo
- Zelo na realização dos trabalhos e exposição das conclusões

Todos os membros da equipe auditora informática deve ter

- Conhecimentos da área e experiencia pratica anterior de trabalho em centros de processamento de dados, desenvolvimento de sistemas, hardware, software ou serviços na área de informática
- Conhecimentos básicos em informática desde sistemas operativos, software básico, base de dados e processamento distribuido, softwares de controlo de acesso e metodologias de desenvolvimento de sitemas, entre outros
- Conhecimentos adicionais de tecnicas como Computer Assisted Audit Techniques [CAATs]

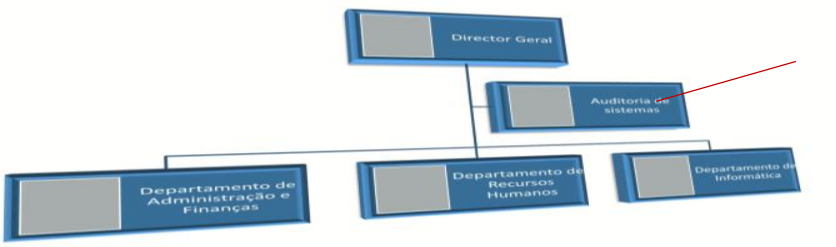
Razões pelas quais deve se fazer Auditoria em uma organizaçãp

Dentre várias razões que proporcionam a auditoria podemos citar

- Para verificar se um sistema, executa as suas funções conforme o planeado e se os resultados obtidos são os esperados
- Para identificar oportunidades de melhoria, pois todo sistema deteriora-se com o tempo
- Para garantir a qualidade do produto ou serviço ou pela necessidade de acompanhar uma acção correctiva
- Para verificar se as instruções documentadas estãp disponiveis para consulta, se elas estão sendo seguidas e se elas são adequadas para assegurar a satisfação dos clientes
- Para verificar se o sistema continua a atender aos requisitos especificados e se está sendo implementado de acordo com a qualidade de serviços e padrões exigidos.

Posicionamento da auditoria dentro da organização

- O departamento de auditoria deve ser um departamento autónomo e independente
- É recomendável que reporte direcamente ao nivel mais elevado possivel dentro da organização como a Direcção Geral ou Conselho de Administração de modo a manter a liberdade de agir sobre todas as áreas da organização, sem restrições



Algumas tecnicas de analise e controle usadas na auditoria

- Programas de computador
- Simulação de dados
- Analise presencal
- Rastreamento de programas
- Entrevista
- Analise de relatorios
- Analise de logs
- Analise do codigo fonte
- Exibição parcial da memoria snapshot

Relação entre auditoria e segurança da informação

A segurança da informação e a auditoria de sistemas são interdependentes, ou seja, uma dependente da outra pra produzerem os efeitos desejaveis.

Segurança da informação

- Garante a integridade dos dados
- Medidas de prevenção conta ataques internos e externos

Auditoria de sistemas

- Garante que os dados estejam realmente íntegros, proporcionando um pefeito processamento, obtendo os resultados esperados.
- Identifica ameaças e oportunidades para a empresa e cria cenário para uma resposta competitiva e eficáz

Para que uma organização continue competitiva no mercado ela deve manter um controle efectivo sobre as suas áreas e isso é feito através do processo de auditoria.

Unidade 4 – Análise e Gestão do Risco Em Segurança Da Informação

Conceitos

Vulnerabilidade

É uma fragilidade ou fraqueza, que pode fornecer uma porta de entrada para um atacante

Analise de Vulnerabilidade

É o processo de identificação de falhas e vulnerabilidade conhecidas, presentes no ambiente e que o expõe a ameaças. Essas falhas podem ser causadas por erros de programação, má configuração ou simplismente uma falha humana.

Ameaça

É um agente ou um acção que se aproveita de uma vulnerabilidade

Risco

É a relação entre a probabilidade e o impacto da ameaça ocorrer.

Etapas da gestão de riscos

- Diagnostico do risco
- Priorização do risco
- Mitigação do risco

Ataque

É a incidencia da ameaca sobre uma vulnerabilidade

Tipos de Ataque

- INTERNO – Este ataque é de alguma forma facilitado pelo pessoal interno da organização, como funcionarios insatisfeitos, funcionarios mal treinados ou outro tipos de funcionarios mal intencionados.
- EXTARNO - Este ataque é feito por pessoal de fora da organização como crackers, concorrentes ou espiões,

Fases de um ataque

- Colecta de informações
- Ánalise de vulnerabilidades
- Uso de ferramentas de ataque

Unidade 5 – Pentest, Análise Forense e Auditoria de Segurança

PenTest [Teste de Penetração]

É um tipo de auditoria de segurança da informação que adopta a prespectiva de um potencial atacante como modo de operação. Com este teste é possivel desenvolver uma avaliação objectiva das potenciais vulnerabilidades e vectores de ataque existentes, identificando assim o que pode ser acessado, roubado ou danificado em um ataque real.

As observaçoes recolhidas de um teste de penetração são um requerimento obrigatorio para o desenvolvimento de procedimentos internos para previnir ou mitigar potenciais vulnerabilidades.

Estas observações são também uma fonte de informação necessaria para uma forte análise de risco, uma vez que o perfil recolhido sobre a infra-estructura representa riscos realmente quantificaveis.

Tipos de PenTest

Existem 3 tipos de teste de penetração e o que diferencia um do outro é a quantidade de informação fornecida por parte da organização aos analistas especializados.

BlackBox

O consultor não assume qualquer conhecimento prévio da infraestrutura a ser testada. Simula um ataque de um cracker por fora ou por dentro da empresa que tenta invadir os sistemas.

GreyBox

O consultor assume algum conhecimento prévio da infraestrutura, como um conjunto de credenciais da rede. Simula o acesso de um colaborador ou prestador de serviço mal-intencionado

WhiteBox

Neste tipo, a organização fornece aos pentesters, o conhecimento completo da infraestrutura a ser testada, incluindo diagramas de rede, código fonte, informações de endereços IPs e credenciais ao acesso. Simula um ataque interno realizado por um utilizador que tem conhecimento do ambiente de rede, como um funcionário da área de tecnologias de informação.

Razões para fazer um PenTest

- Para entender os reais riscos que vulnerabilidades especificas apresentam ao negócio
- Para testar de facto a segurança da rede ou do sistema de informação
- Para determinar se os investimentos actuais estão realmente detectando e prevenindo os ataques
- Para testar e garantir a proactividade da rede ou sistema

Etapas para realização de um PenTest

1. Definição do tipo de teste
2. Definição do escopo, profundidade e planeamento dos testes
3. Execução dos testes e colecta de evidencias
4. Desenvolvimento do relatório
5. Apresentação do relatório e apoio no plano de correcção

Aspectos legais a ter em conta num PenTest

- LIMITES DO TESTE – Determinar até que ponto pode ir a actividade.
- HORÁRIOS – Em que períodos irão decorrer os testes, períodos de menor utilização e menos críticos.
- EQUIPE DE SUPORTE – Caso haja algum efeito colateral do ataque é necessário prevenir com uma equipe de suporte preparada para tomar providencias.
- PERMISSÃO ASSINADA – Deve ser feito um documento assinado pelo responsável da empresa, com os nomes das pessoas da equipe autorizada a realizar os testes.

Regularidade de um PenTest

Um teste de penetração pode ser feito mais de uma vez por ano. Recomenda-se no mínimo trimestralmente ou após qualquer mudança significativa na rede de dados ou na ambiente web.

Ferramentas para execução de um PenTest

Existem vários programas ou ferramentas que facilitam a execução de um PenTest.

- Kali Linux é um sistema operativo feito para hackers e para realização de testes de penetração.
- ParrotSec é um sistema operativo feito para hackers e para realização de testes de penetração.

Diferença entre um Hacker e um Cracker

Hackers são indivíduos que possuem conhecimentos profundos na informática e que dedicam a maior parte do seu tempo a conhecer, modificar softwares, hardwares e redes de computadores.

Crackers também possuem conhecimentos profundos em informática, porem utilizam de forma maléfica.

Análise Forense

- É uma prática invetigativa importante para as empresas como para a policia, que usa métodos cientificos para identificar, preservar, analisar e documentar evidencias localizadas em computadores ou outros dispositivos electronicos.
- É a ciencia que estuda a aquisição, preservação, recuperação e analise de dados armazenados em recursos computacionais e procura caracterizar crimes de informática de acordo com as ecidencias digitais encontradas no sistema invadido.

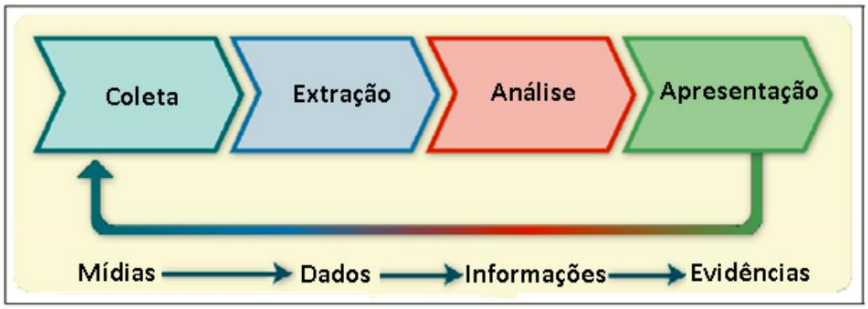
Proposito da analise forense

A analise forense é empregada em diversos tipos de cenários tanto para fins

- Legais – Invesitgação de casos de espionagem
- De Exercicio de acções disciplinares internas – uso indevido de recursos computacionais da empresa

Tem como propósito facilitar ou possibilitar uma prosterior reconstrução de eventos criminais, ou ajudar a antecipar acções não autorizadas que se mostram anormais a comportamentos esperados ou planeados.

Etapas da analise forense no contexto computacional



1. Colecta de dados – Realiza-se a colecta de fontes que provalvelmente contenham evidencias digitais ou possuam alguma relação com o evento investigado.

- Identificação – Reconhecimento dos materiais uteis para a pericia ou que podem ser uma possivel fonte de evidencias digitais [Computadores pessoais ou servidores]
- Apreensão – O equipamento é isolado de forma a determinar quais fontes são mais relevantes para a investigação
- Preservação – Certeza de que uma evidencia extraida deve ser adequadamente manuseada e protegida para assegurar que nenhuma evidencia seja danificada, destruida ou mesmo comprometida pelos maus procedimentos usados na investigação e que nenhum virus ou codigo malicioso seja istroduzido em um computador durante a analise forense
- Verificação da integridade – Ultima fase da colecta de dados, que consiste na analise dos dados para saber se são íntegros ou não.

2. Extração de dados – Esta etapa consiste em avaliar e extrair somente as informações relevantes a investigação, por exemplo, o arquivo de log do sistema de um servidore pode conter milhares de entradas, porem somente algumas delas podem interessar á investigação

3. Análise de dados – Nesta etapa são analisados os dados e informações extraidas da etapa anterior e tem a finalidade de identificar pessoas, locais e eventos, determinando como esses elementos estão inter-relacionads, pois dessa maneira, será possivel realizar uma descrição precisa e conclusiva da investigação.

4. Apresentação – É a etapa final do processo de analise forence. Nesta etapa, a tarefa é documentar as evidencias digitais encontradas e apresenta-las ás autoridades competentes

Principais tecnicas de colecta de informação

Tecnica de imagem

Esta tecnica, quando realizada através de equipamentos e softwares forenses especificos, permitem uma duplicação fiel dos dados e a preservação do material apreendido.

A tecnica de imagem é uma tecnica de duplicação que realiza uma cópia exata e fiel dos dados contidos em um dispositivo de armazenamento computacional para outro.

Equipamentos para bloqueio de escrita e duplicação forense

São dispositivos simples utilizado para garantir que, durante o processo de cópia ou de acesso, as informações e os dados digitais contidos no dispositivo de armazentametno computacional permaneçãm inalterados.

Softwares e sistemas operativos para duplicação forense

Sistema para clonagem ou duplicação de evidencias [Norton Ghost]

Ferramentas para colecta de dados voláteis

Uso de ferramentas capazes de fazerem a colecta de dados em dispositivos voláteis como a memoria RAM.

Principais ferramentas usadas para a fase de colecta

- Caller IP – Monitora a entrada, saida e invasão de ips que estçao conectados ou tentando conectar, apresentando o mapa do mundo, a sua localização com endereço, telefone e responsavel pelo ip.
- RecoveryMyFiles – Recupera dados apagados ou formatados
- SmartWhols – Verifica o endereço IP e o Dominio na internet, sendo apenas necessária a indicação do IP ou Dominio, apresentando na tela a localização destes, gerando endereço, telefone,

resposntavel pelo IP ou pelo dominio em questao, em resumo, todos os dados referentes a uma determinada organização

- E-Mail Tracker – Fornece o local de origem do e-mail, sua rota e a empresa responsavel.
- EnCase – Permite a recuperação de dados, base de dados de evidencias, analisa hardwares, analisa logs, permite a analise de evidencias sem alterá-las, dentre outras funcionalidades.

Este material foi feito para facilitar o vosso estudo. Não serei responsavel por qualquer tentativa de uso para fins ilicitos.

Denylson Danial Baná