Prof. Doutor Engº Pedro S. Teta
Vice-Ministro, Ministerio da Ciência e Tecnologia
Coordenador da Comissão Nacional das TICs
Angola

www.pedroteta.org

SEGURANÇA E CRIME INFORMATICO

SEGURANÇA DA INFORMAÇÃO

1. Todas tecnologias e avanços têm colocado muitas organizações em uma posição delicada em alguns casos. Problemas de origem interna e externa tem marcado o dia-a-dia, seja para proteger seus segredos, suas estrategias ou até mesmo a protecção do capital humano.

2. A realidade actual demonstra que com o crescimento da informática crescem também todos os fenomenos ligados a pirataria e a sabotagem informática, para não falar das próprias dificuldades que surgem quando há uma avaria, o pagamento involuntário ou não de ficheiros ou mesmo simples ataques por vírus informáticos.

Riscos e vulnerabilidade

- Quais são os pontos vulneráveis do ambiente computacional da minha organização?
- Quais são as ameaças que podem causar algum incidente de segurança para organização?
- Quais são os riscos se a organização não proporcionar protecção adequada as informações criticas e estratégicas necessárias a sua sobrevivência?
- Quais são as melhores soluções para os problemas do ambiente computacional da organização?
- O que fazer para proteger o ambiente computacional desta organização contra ataques internos e externos?
- O que é necessário para manter nossos sistemas críticos em funcionamento 24 horas por dia?

SEGURANÇA

Alguns pontos são importantes a determinar, que qualquer organização deve sempre tê-los em mente:

- O que deve ser protegido?
- Contra o que seria Necessário proteger?
- Como seria feita a proteção

FINALIDADE E IMPORTANCIA

- Prover protecção aos recursos da organização (sistemas, pessoas, informações, equipamentos) e tem como finalidade diminuir os riscos existentes em todos os ambientes.
- Segurança da informação é a base para dar as organizações a possibilidade e a liberdade necessária para a criação de novas oportunidades de negócios

BENEFICIOS

- Redução dos riscos contra vazamento da informação confidencias/sigilosas.
- Redução da probabilidade de fraudes
- Redução dos erros devido a formação e mudança de comportamento
- Manuseio correto das informações confidencias

OBJECTIVOS

- Redução da probabilidade de ocorrência de incidentes de segurança
- Redução dos danos/perdas causados por incidentes de segurança
- Recuperação dos danos em caso de desastre/incidente

OBJECTIVOS

DISPONIBILIDADE

- Pressupõe manter acesso continuo e ininterrupto, quer dizer a informação deve estar disponível para pessoa certa e no momento em que ela precisa.

INTEGRIDADE

- Consiste em proteger a informação contra qualquer tipo de alteração sem autorização explicita do autor da mesma.
- Uma forma comum de proteção contra a perda da integridade é o mecanismo de criptografia aplicada as informações que necessitam deste tipo de proteção.

CONFIDENCIALIDADE

- É a propriedade eu visa manter o sigilo, o segredo ou a privacidade das informações, evitando que pessoas, entidades ou programas não autorizadas tenham acesso as mesmas.

CRIME INFÓRMATICO

- O objectivo desta abordagem sobre o crime informatico é discutir alguns aspectos a ter em conta na análise de algumas actividades nocivas praticadas voluntariamente ou não através dos meios computacionais ou para atingir e afectar negativamente a segurança dos sistemas e redes de informação que são propriedades do estado, de empresas, cidadãos etc.
- Aproveitando-se de algumas falhas de segurança que em maior ou menor grau se pode encontrar nos sistemas informaticos das instituições e não só , algumas pessoas ou organizações criminosas podem aceder aos sistemas e danificar a informação ou pura e simplesmente tirar proveito do conhecimento de uma informação que pode em certos casos até ser classificada (“segredo do estado”).

CRIME INFÓRMATICO

- Alguns dos crimes podem atentar contra os direitos Dos cidadãos. São caso disso os abusos da lei da propriedade intelectual quando os prevaricadores se aproveitam do trabalho de outrem para daí tirar proventos monetários ou de outra espécie.
- Sendo que os computadores estão cada vez mais disseminados e é fácil com base neles cometer alguns dos crimes que, de outra modo, seriam muito difíceis de praticar, deve-se aplicar medidas severas e a altura de forma a poder dissuadir as pessoas para a sua prática já que os prejuízos causados por esta via podem ser muito elevados e nalguns casos simplesmente de valor estratégico incalculável.

RESPONSABILIDADE PENAL

- 1)As pessoas colectivas devem responder pelos crimes mencionados na lei da criminalidade informatica em fase de elaboração e que tenham sido cometidos em seu nome e no interesse colectivo pelos seus membros ou representantes.
- 2) A responsabilidade mencionada no ponto 1 não existe se os crimes forem cometidos contra ordens ou instruções expressas ou sem o conhecimento directo de quem de direito.
- 3) Independentemente de haver ou não responsabilização colectiva, os agentes criminosos, que tenham agido em nome ou pelo interesse de uma pessoa colectiva, não se furtam da responsabilidade individual em relação aos crimes praticados.
- 4) As pessoas colectivas, uma vez incriminadas, respondem pelas penalizações atribuídas aos seus elementos. Se os crimes forem praticados contra os interesses do estado poderão ser condenadas ainda a cessação completa das suas actividades no território nacional.

CRIMES DE PIRATARIA

Incorre neste crime :

- Quem intencionalmente reproduzir, divulgar, ou assumir publicamente como sendo seu um programa informático ou qualquer outro código informático escrito ou já publicado por uma outra pessoa.
- Quem intencionalmente reproduzir, montar, imitar, divulgar, ou assumir publicamente como sendo seu parte ou a totalidade do projecto electrónico ou um protótipo de um equipamento ou um sistema informático de autoria de uma outra pessoa será punido a uma pena de até 3 anos de prisão ou multa de ....
- Qualquer pessoa que intencionalmente tenha tentado, mesmo sem sucesso, praticar os actos descritos nas alíneas anteriores.

CRIMES DE ACESSO ILEGITIMO

Incorre neste crime :

- Qualquer pessoa que intencionalmente tenha tido, sem a devida autorização, acesso a um sistema ou uma informação ou tenha ultrapassado o nível de autorização que tinha para ter acesso a um sistema ou uma informação que para o efeito estava sob regime de acesso condicionado ou restrito;
- Qualquer pessoa que intencionalmente tenha utilizado um dispositivo, um programa ou qualquer processo especial que o mesmo sabe que consegue ultrapassar as restrições impostas para o acesso a um sistema classificado como de acesso restrito e não tenha dado a conhecer este facto as pessoas responsáveis ou solicitado antes uma autorização especial para o efeito do acesso;

CRIMES DE ACESSO ILEGITIMO

- Qualquer pessoa que tenha revelado a terceiros uma forma que permitiu a estes últimos ultrapassar as restrições impostas para o acesso a um determinado sistema;
- Qualquer pessoa que tenha sabido de terceiros a forma de poder contornar as restrições de acesso e não tenha revelado antes aos responsáveis do sistema e tenha usado o mesmo conhecimento para aceder ou permitir o acesso a outras pessoas num sistema de acesso restrito;
- Qualquer pessoa que intencionalmente tenha tentado, mesmo sem sucesso, praticar os actos descritos nas alíneas anteriores.

CRIMES DE INTERCEPÇÃO ILEGÍTIMA DA INFORMAÇÃO

Incorre neste crime :

- Quem intencionalmente interceptar ou desviar, através de meios computacionais ou outros, sem estar autorizado para o efeito, informações que estavam num computador alheio ou circulando pela ou com destino a rede informática .
- Qualquer pessoa que intencionalmente tenha tentado, mesmo sem sucesso, praticar o acto descrito na alínea anterior.

CRIMES DE BURLA E FALSIFICAÇÃO

Incorre neste crime :

- Quem intencionalmente modificar, apagar ou acrescentar dados ou programas, ou usar qualquer outro processo através de meios informáticos, com a finalidade de confundir ou dificultar o trabalho aos orgãos judiciais ou em processos posteriores em que estes dados e programas podiam servir de meios de prova.
- Qualquer pessoa que intencionalmente tenha usado documentos ou outros resultados provenientes dos processos de falsificação descrito no ponto anterior com a finalidade de obter benefícios ilegítimos para si ou para terceiros.
- Qualquer pessoa que tenha intencionalmente tentado, mesmo sem sucesso, praticar os actos descritos nas alíneas anteriores.

CRIME DE SABOTAGEM

Incorre neste crime :

- Qualquer pessoa que, sem autorização explicita para o efeito, tenha utilizado um processo de modificação da informação ou configuração inicial de maneira a acabar por enfraquecer, prejudicar ou danificar um programa ou um sistema informático;
- Qualquer pessoa que tenha escrito e transferido ou disseminado directamente ou por via indirecta um programa malicioso com a intenção final de prejudicar ou causar danos nos sistemas informáticos em que o mesmo esteja presente ou seja executado;
- Qualquer pessoa que intencionalmente tenha escrito e usado, ou transferido e usado directamente ou por via indirecta um programa malicioso numa máquina ou numa rede informática e com a intenção final de prejudicar o seu bom funcionamento;

CRIMES DE ROUBO DE IDENTIDADE

Incorre neste crime :

- Qualquer pessoa que, sem autorização explicita para o efeito, tenha utilizado os elementos de identificação de um outro de forma a poder aceder a um sistema informático, receber, enviar ou processar informações como se fosse o legítimo detentor da identidade;
- Qualquer pessoa que tenha intencionalmente tentado, mesmo sem sucesso, praticar os actos descritos na alínea anterior.

CRIMES DE ROUBO DE MARCA

Incorre neste crime :

- Qualquer pessoa que, sem autorização explicita para o efeito, tenha utilizado ou registado uma marca que já tenha sido reconhecida como sendo propriedade de uma outra entidade com a intenção de aproveitar o sucesso já granjeado pela marca noutros sectores de actividade, ou prejudicar o bom nome e a boa imagem desta entidade.
- Qualquer pessoa que tenha intencionalmente tentado, mesmo sem sucesso, praticar os actos descritos na alínea anterior.

CRIMES DE INVASÃO DA PRIVACIDADE

Incorre neste crime :

- Qualquer pessoa que, sem autorização explicita para o efeito, tenha utilizado um processo de vigilância recorrendo aos meios computacionais com a intenção de utilizar os dados assim recolhidos para fins ilícitos ou para prejudicar o bom nome e a imagem da pessoa vigiada.

INVASÃO DA PRIVACIDADE

- Qualquer pessoa que, sem autorização explicita para o efeito, tenha fornecido a terceiros os dados de identificação electrónica de uma pessoa e que lhe tinham sido revelados para um determinado fim, no intuito desta pessoa, mesmo sem querer, ser objecto de contactos indesejados, de campanhas difamatórias ou de sensibilização para operações comerciais ou outras por parte de terceiras entidades com quem o lesado nunca manteve alguma relação.
- Qualquer pessoa que tenha intencionalmente tentado, mesmo sem sucesso, praticar os actos descritos na alínea anterior.

COMO EVITAR O CRIME

- Definição de normas a seguir aquando da aquisição de sistemas informáticos e de mecanismos de teste.
- Definição de um conjunto básico de programas a instalar para o controle dos acessos ao sistema.
- Definição de um conjunto de programas para a monitorização e aferição do bom funcionamento dos sistemas.
- Realização de cursos e outras acções de formação para os administradores dos sistemas informáticos afectos ao estado.

COMO EVITAR O CRIME

- Constituição de uma “task-force” composta por alguns quadros que devem acompanhar todos os aspectos de segurança e tomar as medidas necessárias para uma rápida solução de quaisquer problemas que surjam.
- Constituição de uma rede de troca de informação especialmente dedicada aos assuntos de segurança informática.
- Constituição de um grupo de “piratas amigos” que servem para o teste da robustez dos sistemas e acompanhamento geral da evolução das técnicas de ataque e sabotagem informática.

Obrigado pela Atenção

www.pedroteta.org