1.Hexadecimal Parkeriano

O hexadecimal Parkeriano é um conjunto de seis elementos da segurança da informação proposta por Donn B. Parker. O termo foi cunhado por M. E. Kabay. O hexadecimal Parkeriano soma mais três atributos aos três atributos clássicos de segurança do triângulo CIA. Em segurança da informação, um backup ou o processo de fazer backup se refere a fazer cópia dos dados de forma que essas cópias adicionais possam ser usadas para restaurar o original após um evento de perda de dados.

Os atributos do hexadecimal Parkeriano são os seguintes:

1. Confidencialidade

2. Posse ou Controle

3. Integridade

4. Autenticidade

5. Disponibilidade

6. Utilidade

Esses atributos da informação são atômicos, no sentido de que não são divididos em outras partes constituintes; não sobrepõem, já que se referem a aspectos únicos da informação. Qualquer violação de segurança da informação pode ser descrita como aquilo que afeta um ou mais desses atributos fundamentais da informação.

2.Risco

Um risco é a probabilidade de um agente ameaçador tirar vantagem de uma vulnerabilidade e o correspondente impacto nos negócios. Se um firewall tem diversas portas abertas, há uma maior probabilidade de um invasor usar uma delas para acessar a rede de forma não autorizada. Se os usuários não forem treinados nos processos e procedimentos, haverá uma maior probabilidade de um funcionário cometer um erro, intencional ou não, que possa destruir dados. O risco amarra a vulnerabilidade, a ameaça e a probabilidade de exploração ao impacto resultante nos negócios.

Na prática:

1. Um incêndio pode surgir na sua empresa

2. Um funcionário que não trabalha no departamento de RH obtém acesso a informações sensíveis ou privadas

3. Alguém aparece como um funcionário e tenta obter informação

4. Sua empresa é atingida por uma falha de energia

5. Um hacker consegue obter acesso à rede de TI da empresa

3.Ameaça

Uma ameaça é uma potencial causa de um incidente não desejado, o que pode resultar em prejuízo ao sistema ou à organização. A entidade que tira vantagem de uma vulnerabilidade é referida como agente ameaçador.

Um agente ameaçador pode ser um invasor acessando a rede através de uma porta no firewall, um processo acessando dados de uma forma que viole a política de segurança, um tornado destruindo uma instalação ou um funcionário cometendo um erro não intencional que pode expor informações confidenciais ou destruir a integridade de um arquivo.

4.Vulnerabilidade

Uma vulnerabilidade é uma fraqueza de um ativo ou grupo de ativos que pode ser explorada por uma ou mais ameaças. Uma vulnerabilidade caracteriza a ausência ou a fraqueza de uma proteção que pode ser explorada. Essa vulnerabilidade pode ser um serviço rodando em um servidor, aplicações ou sistemas operacionais desatualizados, acesso irrestrito para entrada de chamadas no modem, uma porta aberta no firewall, uma segurança física fraca que permita a qualquer pessoa entrar em uma sala de servidores ou a não aplicação de gestão de senhas em servidores e estações de trabalho.

5.Exposição

Uma exposição é a circunstância de estar exposto às perdas provenientes de um agente ameaçador. Uma vulnerabilidade expõe uma organização a possíveis ameaças. Se a gestão de senhas for fraca e as regras para senhas não forem aplicadas, a empresa fica exposta à possibilidade de ter a senha de usuários capturada e usada de forma não autorizada. Se uma empresa não tem seu cabeamento inspecionado e não estabelece medidas proativas de prevenção contra incêndios, ela se expõe a incêndios potencialmente devastadores.

6.Contramedida e salvaguarda

Uma contramedida é posta em prática para mitigar o risco em potencial. Ela pode ser uma configuração de software, um dispositivo de hardware ou um procedimento que elimine a vulnerabilidade ou reduza a probabilidade de um agente ameaçador ser capaz de explorar a vulnerabilidade. Exemplos de contramedidas incluem a gestão de senhas fortes, um guarda de segurança, mecanismos de controle de acesso em sistemas operacionais, a implementação de senhas da BIOS e treinamento de conscientização sobre segurança.