1.Backup

O propósito de fazer backups, ou cópias reversas, é manter a integridade e a disponibilidade da informação e das instalações computacionais. As consequências da perda de informação dependem da idade da informação que pode ser recuperada a partir do backup. É importante, portanto, considerar o intervalo em que os backups são feitos. Quanto tempo podemos nos permitir recuperar novamente a informação que foi perdida ? É importante que o backup seja testado regularmente. Além de realmente fazer e testar os backups, também é necessário considerar como os backups são manejados. Os backups são retirados de prédios altamente seguros e depois colocados em armários destrancados ? Ou os backups são colocados próximos ao servidor com os dados originais ? Os dados são criptografados ? Por quanto tempo os backups são armazenados ? Isso atende aos requisitos legais de armazenamento.

2.Registro de monitoração

Com o aumento dos ataques de malware, e também com o mau comportamento, intencional ou não, de usuários, é necessário ter a capacidade de registrar eventos e produzir evidências. Para esse propósito, é essencial ter um bom registro

2.1 Registro de evento (log)

O registro de evento (log) é a coleção de atividades de sistemas e de usuários, exceções, falhas e eventos de segurança da informação. Ao coletar os logs de eventos é importante que você olhe para as informações coletadas; caso contrário, a coleta de logs é inútil. Tenha em mente que os logs devem ser mantidos em um local seguro e protegidos contra modificações ou exclusão das informações coletadas. Antes de começar a coletar os logs, pense sobre o que registrar, por quanto tempo manter os logs e quem deve acessar a informação. Para garantir que logs diferentes possam ser usados para investigar um evento de segurança, os relógios do sistema devem ser sincronizados com uma única fonte de referência de tempo. Tenha em mente que arquivos de log contendo dados pessoais devem ser protegidos conforme as leis de privacidade.

2.2 Controle de software operacional

Software operacional é o software usado nos sistemas operacionais. Dentro de uma organização, a manutenção de softwares operacionais por usuários finais não deve ser permitida e só deve ser efetuada pelos operadores depois de testada. É importante pensar em uma estratégia de restauração caso algo dê errado ao atualizar os sistemas operacionais, mesmo após um bom teste

2.3 Gestão de vulnerabilidades técnicas

Uma vulnerabilidade é uma fragilidade de um ativo ou grupo de ativos que pode ser explorada por uma ou mais ameaças. Uma vulnerabilidade caracteriza a ausência

de proteção ou a fragilidade de uma proteção que pode ser explorada. Essa vulnerabilidade pode ser um serviço executando em um servidor, aplicações ou sistemas operacionais não corrigidos, acesso discado irrestrito via modem, uma porta aberta em um firewall, segurança física fraca que permite que qualquer pessoa entre em uma sala de servidor ou um fraco gerenciamento de senha em servidores e estações de trabalho.

2.4 Gerência de vulnerabilidades técnicas

Uma vulnerabilidade técnica é uma fraqueza em um sistema computacional que permite que alguém ataque o sistema computacional vulnerável. Existem muitas vulnerabilidades que são encontradas por hackers éticos ou por coincidência. Todo sistema operacional possui vulnerabilidades, às vezes conhecidas e às vezes desconhecidas pelo proprietário. É importante que, tão logo a vulnerabilidade seja conhecida, medidas apropriadas sejam tomadas para prevenir que atacantes explorem a vulnerabilidade.

Para vulnerabilidades desconhecidas, um processo de gestão de incidentes é necessário para garantir uma resposta apropriada no caso de uma violação. Para vulnerabilidades conhecidas, os fornecedores provavelmente fornecerão atualizações ou correções. Essas correções devem ser testadas e verificadas para garantir que o software operacional continue funcionando como planejado. Se não houver correção disponível, o risco pode ser minimizado adotando medidas de segurança, como, por exemplo, isolamento do sistema, adaptação de firewall e maior monitoramento.