1.Digital forensics

Como profissionais de segurança, somos frequentemente responsáveis pela coleta de dados quando um incidente de segurança ocorre. O processo de forense digital não só ajuda a entender o que aconteceu, mas também permite melhorar a proteção contra futuros ataques e fornecer informações para processos legais. A coleta e o armazenamento correto desses dados são essenciais, pois podem ser usados em processos legais anos depois. A RFC 3227 define diretrizes para coleta e arquivamento de evidências, estabelecendo boas práticas para aquisição, análise e documentação dos dados coletados.

Uma solicitação comum nesse contexto é a **retenção legal** (*legal hold*), **geralmente iniciada por advogados ou entidades legais, que exige a preservação de dados específicos**. O responsável por atender a essa solicitação é o custodiante de dados, que deve avaliar e garantir que todas as informações necessárias sejam coletadas e armazenadas corretamente. Esses dados são geralmente armazenados em repositórios seguros e podem exigir conversão de formatos, como transformar e-mails armazenados em formatos proprietários para texto legível. A integridade dos dados precisa ser garantida, pois qualquer alteração pode comprometer a validade das evidências.

Para garantir que os dados permaneçam inalterados, é essencial manter uma cadeia de custódia (chain of custody). No mundo físico, evidências são seladas em sacos lacrados; no digital, isso é feito por meio de **hashes e assinaturas digitais**. Isso permite rastrear quem acessou os dados e confirmar que não foram modificados ao longo do tempo. Em casos de ataques mais complexos, onde múltiplos sistemas são afetados, cada peça de informação coletada deve ter sua cadeia de custódia documentada.

A aquisição de dados pode ocorrer de várias fontes, como discos rígidos, memória do sistema, firmware ou logs de firewalls e servidores. Em sistemas virtuais, pode ser necessário capturar imagens completas da máquina virtual, garantindo que toda a configuração seja preservada. Além disso, dados podem ser encontrados em locais inesperados, como arquivos temporários, lixeira, históricos de navegador e credenciais salvas.

A documentação detalhada do processo de coleta é essencial para garantir que as informações possam ser usadas corretamente no futuro. Um relatório forense normalmente inclui um resumo do incidente, descrição dos procedimentos adotados, verificações de integridade dos dados e, se necessário, análises e conclusões sobre o evento investigado.

O armazenamento seguro das evidências é uma parte fundamental da forense digital. Como processos legais podem ocorrer anos depois do incidente, é necessário preservar os dados de forma que possam ser acessados com segurança quando

necessário. No caso de dispositivos móveis, que podem ser apagados remotamente, é crucial fazer cópias antes de prosseguir com a análise. Além disso, alguns sistemas possuem criptografia que bloqueia o acesso aos dados ao serem desligados, tornando essencial a captura das informações enquanto o dispositivo ainda está ligado.

A **descoberta eletrônica** (***e-discovery***) é outro aspecto importante da forense digital. **Trata-se do processo de coleta, preparação e fornecimento de documentos eletrônicos para uso jurídico**. A e-discovery se concentra apenas na aquisição de dados, enquanto a análise forense posterior determina se há informações relevantes e se os dados foram alterados ou excluídos. Isso pode envolver a recuperação de arquivos deletados para entender a extensão do incidente.

O processo forense digital exige rigor técnico e metodológico para garantir que as informações coletadas sejam úteis e admissíveis em processos legais. Seguir as melhores práticas de aquisição, armazenamento e documentação é essencial para preservar a integridade das evidências e fortalecer a segurança da organização.