1.Monitoramento de dados

O monitoramento da integridade de arquivos é essencial para a segurança de sistemas, pois permite identificar alterações inesperadas em arquivos que normalmente não deveriam ser modificados. **O software responsável por esse monitoramento é chamado de File Integrity Monitor** (**FIM**). No Windows, essa função pode ser realizada com a ferramenta **System File Checker** (**SFC**), que verifica e restaura arquivos críticos do sistema caso tenham sido alterados. No Linux, o **Tripwire** é uma solução popular que oferece monitoramento em tempo real para detectar mudanças suspeitas.

Outra abordagem para segurança é o uso de sistemas de prevenção contra intrusões baseados em host (HIPS), que podem identificar e bloquear ataques contra vulnerabilidades conhecidas, além de monitorar a integridade de arquivos. **Já a prevenção contra perda de dados** (DLP) **ajuda a evitar o vazamento de informações sensíveis, monitorando dados em uso** (ativos na memória do sistema), em movimento (sendo transmitidos pela rede) e em repouso (armazenados em dispositivos).

Os sistemas DLP podem ser integrados a firewalls de última geração ou funcionar como soluções independentes. Eles são usados para bloquear a transferência não autorizada de informações confidenciais, como números de documentos, dados médicos e registros financeiros. Esses sistemas podem impedir que informações sejam enviadas por e-mail, copiadas para dispositivos USB ou transferidas para serviços na nuvem. Um exemplo de incidente foi o caso do Departamento de Defesa dos EUA em 2008, quando um malware se espalhou por meio de um pendrive conectado a um computador militar, resultando na proibição temporária do uso de dispositivos USB na instituição.

As soluções DLP também monitoram tráfego de rede para impedir a transferência de informações sensíveis e podem ser implementadas em e-mails corporativos para evitar vazamentos. Um caso famoso ocorreu em 2016, quando um funcionário da Boeing acidentalmente enviou um e-mail para seu cônjuge contendo uma planilha com dados sigilosos de 36.000 funcionários. Uma solução DLP teria detectado e bloqueado o envio desse arquivo.

Além da proteção em dispositivos locais e redes, há soluções DLP para aplicações em nuvem, que analisam o tráfego e bloqueiam tentativas de upload de dados confidenciais. Essas soluções são capazes de identificar não apenas informações sensíveis, mas também possíveis ameaças como malware e tentativas de exfiltração de dados.

A segurança da informação depende de ferramentas de monitoramento e prevenção para garantir a integridade dos arquivos, evitar vazamentos de dados e

impedir ataques cibernéticos. O uso combinado de FIM, HIPS e DLP fortalece a proteção dos sistemas contra ameaças internas e externas.