Computing

Was ist DKIM?

- DKIM steht für **Domain Keys Indentified Mail** und ist ein **Identifikationsprotokoll** zur Sicherstellung der **Authentizität** von E-Mail-**Absendern**.
- Es unterstützt auf diese Weise den **Internet Service Provider** (**ISP**).
- Es handelt sich hierbei um ein Verfahren zur Unterscheidung zwischen **Spam-** oder **Phishing-E-Mails** und legalen **E-Mails**, zudem verhindert es **Spoofing**.
- DKIM ist eine Kombination aus **DNS** (**Domain Name System**) und **Public Keys**.
- Die Organisation **IETF** (**Internet Engineering Task Force**) hat dieses Verahren auch zur Standardisierung vorgeschlagen, es ist seit Ende 2004 in Erprobung.
- Als **Internetstandard** wird es unter **RFC 5672** geführt.
- DKIM ist eine Alternative zu **SPF** (**Sender Policy Framework**).
- Bei DKIM die ausgehende **Nachricht** im **Header** vom **Server** (nicht vom Anwender selbst) mit einem **privaten Schlüssel** und einer **digitalen Signatur signiert** bzw. **verschlüsselt**.
- Der Serverauf Empfänger-Seite ruft den Schlüssel aus dem Header ab, **entschlüsselt** diesen, und prüft, ob der Schlüssel in der **Mail** aus einer ihm bekannten Quelle stammt.
- Auf diese Weise kann DKIM die **Integrität** von E-Mails bewerten.
- Voraussetzung für den Einsatz von DKIM ist, dass **Mail-Server** und **Mail-Client** das Verfahren unterstützen.

Eindeutige ID: #1497
Verfasser: Christian Steiner
Letzte Änderung: 2016-12-22 12:34