Information Disclosure

2. Ein Angreifer kann verschlüsselte Dateien mittels Brute-Force entschlüsseln, weil keine geeigneten Sicherheitsmaßnahmen dagegen vorhanden sind.

3. Ein Angreifer kann sicherheitsrelevante Fehlermeldungen sehen.

4. Ein Angreifer kann Dateninhalte lesen, weil die Nachrichten (z.B. E-Mails oder Cookies) nicht verschlüsselt sind, selbst wenn der Transportkanal verschlüsselt ist.

5. Ein Angreifer kann unter Umständen Daten lesen, die mit einem nicht standardisierten kryptografischen Algorithmus verschlüsselt sind.

6. Ein Angreifer kann Daten lesen, die lediglich versteckt oder verschleiert sind (z.B. für eine Undo-Funktion), so dass dem Nutzer gar nicht bewusst ist, dass die Daten (noch) existieren.

7. Ein Angreifer kann als “Man in the Middle” verschlüsselte Daten lesen, weil die Endpunkte einer Netzwerkverbindung nicht authentisiert sind.

Fortsetzung umseitig

Information Disclosure

Information Disclosure cont.

8. Ein Angreifer kann (sensible) Informationen mithilfe eines Such-Indexers, Loggers oder eines anderen Mechanismus zugreifen.

9. Ein Angreifer kann sensible Informationen in einer Datei lesen, weil deren Zugriffsrechte falsch gesetzt sind (schwache ACL).

10. Ein Angreifer kann mangels Zugriffsbeschränkung eine sensible Datei lesen.

J. Ein Angreifer kann den statischen Schlüssel finden, der zur Verschlüsselung genutzt wird.

Q. Ein Angreifer kann einen Kommunikatioinskanal vollständig mitlesen, weil dieser unverschlüsselt ist.

K. Ein Angreifer kann Netzwerkinformationen lesen, weil keine Kryptografie genutzt wird.

A. Sie haben einen neuen Information Disclosure Angriff erfunden.