L3 1. Datensicherheit im Internet

1.4 Cookies

Cookies sind kleine Dateien, die nach dem Besuch einer Internetseite auf dem PC oder Smartphone abgelegt werden. In dieser Datei werden Informationen gespeichert, die im Zusammenhang mit der jeweiligen besuchten Internetseite stehen. Sie merken das z. B. daran, dass Sie beim Ausfüllen des Online-Bestellzettels Daten, die sie einmal eingetragen haben, nicht immer wieder eintippen müssen. In den Browseroptionen können Sie einstellen, ob und von welcher Webseite Cookies gespeichert werden und wann diese gelöscht werden sollen.

Weil Cookies keine ausführbaren Programme sind, stellen sie kein direktes Sicherheitsrisiko dar. Dennoch sind sie nicht unproblematisch: Cookies werden auch eingesetzt, um Internetseiten auf Ihre persönlichen Wünsche zuzuschneiden. Problematisch ist, dass hierbei ein sehr genaues Nutzerprofil angelegt werden kann. Unternehmen setzen solche Cookies zum Beispiel ein, um passende Werbung anzuzeigen.

Zwei Arten von Cookies

Es sind zwei Arten von Cookies zu unterscheiden: Die dauerhaften Cookies und die Session-Cookies. Dauerhafte Cookies bleiben über Monate oder gar Jahre auf Ihrem Computer – zumindest dann, wenn sie nicht automatisch oder manuell gelöscht werden. Die Session-Cookies dagegen werden automatisch immer dann gelöscht, wenn der Browser geschlossen wird. Diese nutzten etwa Banken für das Online-Banking. Ein Sicherheitsrisiko stellen diese Cookies nicht dar. Problematisch sind die dauerhaften Cookies. Denn diese können über eine lange Zeit das Nutzungsverhalten des Anwenders protokollieren – etwa, nach welchen Produkten in welchen Online-Shops er sucht.

Ein weiteres Risiko bergen Cookies auf öffentlich zugänglichen Computern. Manche soziale Netzwerke sorgen durch Cookies dafür, dass Anwender angemeldet bleiben, wenn sie nur den Browser geschlossen, sich aber nicht aktiv ausgeloggt haben. Der nächste Benutzer des öffentlichen Computers kann dann im Profil des vorherigen Anwenders stöbern und gegebenenfalls Schaden anrichten

Cookies von Drittanbietern

Generell gilt, dass nur die Webseite die Cookies auslesen darf, die sie selbst gesetzt hat – Online-Shop A darf also nicht den Cookie von Online-Shop B auslesen. Allerdings gibt es auch noch sogenannte Drittanbieter, also zum Beispiel Werbeagenturen, die Werbebanner auf verschiedenen Webseiten platzieren. Solche Werbebanner setzen manchmal eigene Cookies. Wenn nun ein Anwender drei verschiedene Webseiten mit dem (zufällig) selben Werbebanner-Cookie besucht hat, kann die Werbeagentur theoretisch über ihren Cookie auslesen, welche drei Webseiten das waren. Sie enthält damit ein recht umfassendes Portfolio über das Surfverhalten einer Person. Cookies von Drittanbietern werden daher von Datenschützern als problematisch bewertet.

Quelle: Bundesamt für Sicherheit in der Informationstechnik
https://www.bsi-fuer-buerger.de/BSIFB/DE/Empfehlungen/EinrichtungSoftware/EinrichtungBrowser/GefahrenRisiken/Cookies/cookies_node.html
heruntergeladen am 03.05.2018