SICHERER UMGANG MIT SOZIALEN NETZWERKEN

Welches Problem wird gelöst?

- Durch Phishing gelangen Dritte an vertrauliche Zugangsdaten und nutzen diese Identität, um beispielsweise finanzielle Unterstützung von Freunden zu erbitten.
- Frei verfügbare Informationen werden genutzt, um Personen bloßzustellen und ihnen zu schaden (Cyber-Mobbing, Cyber-Stalking).
- Unternehmen kaufen Profildaten für unerwünschte Zwecke
- Potentielle Arbeitgeber können auf Einträge und Bilder stoßen, die nur für einen eingeschränkten Personenkreis bestimmt sind.

Wo gibt es gute Anleitungen im Netz?

- Das Internet-Archiv „Wayback Machine“ speichert Webseiten als Zeitdokumente dauerhaft ab: https://archive.org

Browser-Plugins

- HTTPS Everywhere: https://www.eff.org/https-everywhere
- Adblock Plus: https://adblockplus.org

Awareness-Kampagnen im Internet

- Verein zum Schutz der digitalen Identität - WakeUpInternet e.V.: http://www.wakeupinternet.com
- Die EU-Initiative für mehr Sicherheit im Netz: http://www.klicksafe.de

Wie heißt die Lösung?

- Awareness schaffen, Sensibilisierung von Mitarbeitern, Freunden und Familie.
- Vermeiden Sie identifizierende persönliche Angaben, wie Geburtsdatum, Postanschrift, etc.
- Browserinformationen zum Urheber und zur Sicherheit der Webseite beachten.

Browser-Plugins

- HTTPS Everywhere: Fordert Verbindungen zu Webseiten automatisch verschlüsselt an.
- Adblock Plus: Blockiert potentiell schadhafte Werbeanzeigen und Pop-ups.

Was sind die Grenzen der Lösung?

- Freizügige Veröffentlichung eigener personenbezogener Daten und Bilder durch Dritte.
- Fehlverhalten im Umgang mit persönlichen Daten kann nicht rückgängig gemacht werden.
- Datensammelwut von sozialen Netzwerken durch detaillierte Pflichtangaben.
- Notwendiges Vertrauen in die Autoren der Browser-Plugins und Browserhersteller.