



SIELING

RECHTSANWALTSKANZLEI

RECHTSANWALTSKANZLEI

NSA Affäre - datenschutzrechtliche Risiken und
mögliche Vorkehrungen

www.kanzlei-sieling.de

- ... ein ganz normaler Arbeitsplatz



Ausgangssituation

- NSA Definition (Quelle: Wikipedia)
- „Die National Security Agency (englisch für Nationale Sicherheitsbehörde), abgekürzt NSA, ist der größte und finanziell am besten ausgestattete Auslandsgeheimdienst der Vereinigten Staaten. Die NSA ist für die weltweite Überwachung, Entschlüsselung und Auswertung elektronischer Kommunikation zuständig und in dieser Funktion ein Teil der Intelligence Community, in der sämtliche Nachrichtendienste der USA zusammengefasst sind. Die NSA arbeitet mit Geheimdiensten befreundeter Staaten zusammen.“
- Edward Snowden enthüllt im Juni 2013 die Totalüberwachung

Risiken

- Sicherheitsrisiken, vor allem außerhalb des Firmennetzwerkes, Verlust von Geschäftsgeheimnissen oder von personenbezogenen Daten
- (strafbare) Datenschutzverletzung bei sog. Berufsgeheimnisträgern
- „Wir weisen darauf hin, dass bei der Kommunikation per E-Mail, soweit nicht auf ausdrücklichen Wunsch des Mandanten die Verschlüsselung gewünscht wird, sowohl diese als auch Anhangdateien grundsätzlich unverschlüsselt an den Mandanten oder Dritten (z.B. Rechtsschutzversicherern, Gerichten, Gegnern) übersandt werden. Sprechen Sie uns bitte an, wenn Sie eine verschlüsselte E-Mail Kommunikation wünschen.
- ☐ Die Kanzlei ist berechtigt die Korrespondenz im Rahmen des Mandatsverhältnisses mit dem Mandanten und Dritten per E-Mail zu führen. Diesbezüglich entbindet der Mandant die Kanzlei von der berufsrechtlichen Schweigepflicht. (Bitte ankreuzen, wenn Sie die Kommunikation via E-Mail wünschen)“

Risiken

- E-Mail Kommunikation
- Telefon und Fax
- Clouddienste
- WLAN (firmeneigenes und fremdes)
- Internetkommunikation
 - skype und co.
 - instant messenger

Lösungen

- Kommunikation im Unternehmen möglichst Inhouse-Lösungen
- Kommunikation verschlüsseln
 - S/MIME
 - PGP
- qualifizierte elektronische Signatur nach dem SigG
- Ziele:
 - Vertraulichkeit
 - Authentisierung
 - Unverfälschtheit

Lösungen

- Anonyme, werbefreie, sichere Postfächer auf Servern in Deutschland bietet posteo.de (kostenpflichtig)
- Das Verschlüsseln von E-Mails ist – abhängig vom verwendeten Mail-Programm – mit etwas Aufwand verbunden. Ein nützliches Werkzeug mit deutschsprachiger Oberfläche und Dokumentation ist z.B. GPG4win
- Truecrypt ist ein umfangreiches Programm zum Verschlüsseln von Dateien, Ordnern, Festplatten (englisch);
- kostenloser Leitfaden zur Verschlüsselung von E-Mails
 - <https://www.sicher-im-netz.de/files/documents/unternehmen/Leitfaden-E-Mail-Verschlueselung.pdf>
 - <https://www.bsi-fuer-buerger.de>

Webseite

Meldung vom 26.06.2013

„Fehlstart der neuen Website der Stiftung Datenschutz – wo sind die Datenschutzhinweise?“

- Informationspflicht gem. § 13 TMG
- Analysedienste
- Einbindung von social Plug-ins
- Übermittlung von Daten ins EU-Ausland
- Verschlüsselte Übertragung (https) anbieten

unerkannt surfen

- Es gibt zahlreiche Browser-Plugins, die es Website-Betreibern erschweren, Daten über ihre Besucher zu sammeln;
- z.B.: HTTPS Everywhere, das – wenn technisch möglich – eine https-verschlüsselte Verbindung zwischen Internet-Browser und dem Server erzwingt
- Tor maskiert die eigenen IP-Adresse, verlangsamt aber auch den Datenaustausch.

anonym suchen

- MetaGer ist eine Metasuchmaschine, besonders geeignet für deutschsprachige Inhalte, die keine Nutzerdaten speichert.
- Duckduckgo und ixquick lassen suchen, ohne zu speichern.
- Startpage kombiniert die Suchergebnisse von Google mit dem Datenschutz von ixquick.

Soziale Netzwerke

- Gefahren:
 - Offenlegung privater und firmeninterner Informationen durch z.B. Nutzung von Chatfunktionen
 - Phishing
 - Identitätsdiebstahl
 - Verbreitung von Schadsoftware

Soziale Netzwerke

- Lösungen:
 - Sicherheitseinstellungen ständig überprüfen
 - Mitarbeiter briefen
 - MyPermissions.org ermöglicht die Verwaltung von Diensten, die Zugang zum eigenen Facebook-Account haben.
 - Friend Inspector ist eine Browser-App, die am Lehrstuhl der Universität Regensburg entwickelt wurde. Hier kann man in spielerischer Weise Interessantes über das eigenen Facebook-Profil und die Privatsphäre-Einstellungen herausfinden.

Lösungsansätze

- was bleibt? Stichwort: Metadaten
- oder doch besser:
- alles per Schneckenpost und persönlich regeln?

Vielen Dank für Ihre Aufmerksamkeit!