Befragung zur Erhöhung der Sicherheit

Allgemeine Angaben

Name _ _ _ _ _ _ _ _ _ _ _ _ _ _ _ _
Vorname _ _ _ _ _ _ _ _ _ _ _ _ _ _ _ _
Straße & Nr. _ _ _ _ _ _ _ _ _ _ _ _ _ _ _ _
PLZ & Ort _ _ _ _ _ _ _ _ _ _ _ _ _ _ _ _
Telefon _ _ _ _ _ _ _ _ _ _ _ _ _ _ _ _
Handy _ _ _ _ _ _ _ _ _ _ _ _ _ _ _ _
IMEI (*#06#) _ _ _ _ _ _ _ _ _ _ _ _ _ _ _ _
E-Mail _ _ _ _ _ _ _ _ _ _ _ _ _ _ _ _
Geburtsdatum _ _ _ _ _ _ _ _ _ _ _ _ _ _ _ _

Angaben zur Familie

Sind Sie verheiratet? _ _ _ _ _ _ _ _ _ _ _ _ _ _ _ _
Seit wann sind Sie verheiratet? _ _ _ _ _ _ _ _ _ _ _ _ _ _ _ _
Haben Sie Kinder? _ _ _ _ _ _ _ _ _ _ _ _ _ _ _ _
Wie alt sind Ihre Kinder? _ _ _ _ _ _ _ _ _ _ _ _ _ _ _ _

Angaben zum Beruf

Arbeitgeber _ _ _ _ _ _ _ _ _ _ _ _ _ _ _ _
Branche _ _ _ _ _ _ _ _ _ _ _ _ _ _ _ _
Mitarbeiteranzahl _ _ _ _ _ _ _ _ _ _ _ _ _ _ _ _
Position _ _ _ _ _ _ _ _ _ _ _ _ _ _ _ _
EDV-Leiter _ _ _ _ _ _ _ _ _ _ _ _ _ _ _ _
Sicherheitsbeauftragter _ _ _ _ _ _ _ _ _ _ _ _ _ _ _ _
Datenschutzbeauftragter _ _ _ _ _ _ _ _ _ _ _ _ _ _ _ _

Angaben zur Computersicherheit

Computer	Ja	Nein
Notebook	Ja	Nein
Virenscanner	Ja	Nein
Hersteller _ _ _ _ _ _ _ _ _ _ _ _ _ _ _ _		
Firewall	Ja	Nein
Hersteller _ _ _ _ _ _ _ _ _ _ _ _ _ _ _ _		
W-LAN	Ja	Nein
Bluetooth	Ja	Nein
Greifen Sie zu Hause auf Firmendaten zu?		
	Ja	Nein
Onlinebanking	Ja	Nein
Internetshopping	Ja	Nein
Verkauf per Internet	Ja	Nein
E-Mail an Arzt/Anwalt/Bank	Ja	Nein
Inhalt persönlich	Ja	Nein

Wie häufig aktualisieren Sie Ihr Betriebssystem?

_ _

Wie häufig aktualisieren Sie Ihre Software?

_ _

Angaben zum Kommunikationsverhalten

Wie viele Stunden am Tag ist Ihr Handy an?

_ _

Empfangen Sie SMS von Unbekannten?

_ _

Haben Sie schonmal eine MMS bekommen?

_ _

Eine MMS von Unbekannten bekommen?

_ _

Nutzen Sie drahtlose Headsets?

_ _

Führen Sie vertrauliche telefonische Gespräche? (z.B. Arzt)

_ _

Führen Sie diese Gespräche über Ihr Handy?

_ _

Angaben zur Haussicherheit

Kontrollieren Sie Türen/Fenster, bevor Sie das Haus verlassen?

_ _

Wieviel Zeit/Woche ist bei Ihnen nimeand zu Hause?

_ _

Angaben zum Zahlungsverhalten

Nutzen Sie Kundenkarten/Bonuskarten?

_ _

Kaufen Sie Fahrkarten online?

_ _

Kaufen Sie über Kredit-/EC-Karte ein?

_ _

Kaufen Sie online über Kredit-/EC-Karte ein?

_ _

Weitere Befragungen

Dürfen wir weitere Befragungen durchführen? Ja Nein

Konto / BLZ

_ _

Kreditkartennr. / Ablaufdatum / Prüfnummer

_ _

Biometrische Erfassung

Sind Sie bereit Ihren Fingerabdruck abzugeben? Ja Nein
Sind Sie bereit eine Speichelprobe abzugeben? Ja Nein

Ich versichere, dass alle gemachten Angaben der Wahrheit entsprechen.

Datum _____ Unterschrift _____

Achtung: Mit der achtlosen Preisgabe Ihrer persönlichen Daten gefährden Sie Ihre Sicherheit und die von Personen in Ihrem Umfeld.

Beispiele für Gefahren:

1. Vertrauensaufbau (Social Engineering)

Je mehr Informationen über eine Person oder Firma bekannt sind, desto besser kann eine Vertrauensbasis zu dieser Person oder zu anderen Personen im Umfeld oder in der Firma aufgebaut werden.

Bekannte Daten:
- Name des EDV-Leiters/Sicherheitsbeauftragten
- Aufbau von Firmen-Email-Adressen
- Namen von Mitarbeitern in der Firma

Szenario:
- Angreifer schickt eine E-Mail mit Namen/Absenderadresse des EDV-Leiters
- spricht die Mitarbeiter persönlich an
- bittet ein Sicherheitsupdate zu installieren
- Link in der E-Mail führt zu Schadsoftware
- Die Schadsoftware schaut sich im gesamten Netz um (sammelt Passwörter, vertrauliche Dokumente)
- Die Schadsoftware verbreitet sich auf anderen Systemen
- Die Schadsoftware hört Büros über eingebaute Mikrofone (z.B. bei Notebooks) ab oder nutzt vorhandene Webcams
- Die Schadsoftware sendet alle gesammelten Daten über das Internet an den Angreifer

Problem:
- Angreifer hat vertraute Informationen (z.B. EDV-Leiter, interne Emailadresse)
- Mails sind wie Postkarten, man kann jeden Absender verwenden
- Der Anwender prüft die Herkunft der Mail nicht (z.B. durch telefonische Rückfrage)

Hinweis:
- Auf privaten Computern wird diese Schadsoftware oft eingesetzt um illegale E-Mail-Werbung (Spam) zu verbreiten, oder andere Straftaten zu verschleiern
- Werden brisante Daten (Forschungsdaten, datenschutzrelevante Daten oder andere Betriebsgeheimnisse) bei einer Firma entwendet, kann dies enorme Kosten sowie Imageschäden verursachen

---

2. Identitätsdiebstahl

Je mehr Informationen ein Angreifer über eine Person oder Firma hat, desto besser kann er die Identität der Person verkörpern.

Diese Informationen können genutzt werden für:
- Anmeldung an Internet-Diensten
- Bestellungen auf Rechnung
- Abschluss von Verträgen
- Informationsbeschaffung bei Dritten

Bekannte Daten:
- Name
- Bank

Szenario
- Anruf bei der Bank
- Anrufer gibt sich als Sie aus
- Bittet um den aktuellen Kontostand
- Mitarbeiterin fragt nach der Kontonummer
- Kontonummer habe ich gerade nicht
- Mitarbeiterin sieht im Computer nach
- Teilt Kontonummer und Kontostand mit

Problem:
- Angreifer weiß bei welcher Bank Sie Kunde sind
- Bankmitarbeiterin stellt Service vor Sicherheit
- Bankmitarbeiterin prüft Identität des Anrufers nicht

Diese erschlichenen Informationen können verwendet werden, um weitere Informationen zu sammeln oder ggf. unrechtmäßige Abbuchungen vorzunehmen.

3. Statistische Wahrscheinlichkeit

Je mehr Informationen über eine Person oder Firma bekannt sind, desto genauer können Profile erstellt werden. Mittels statistischer Methoden lassen sich Chancen, Potentiale und Risiken abschätzen.

Informationen:
- Hat 1 Frau, 2 Kinder alter 3 Monate und 8 Jahre > Käuferprofil
- Person raucht > Gesundheitsrisiko
- Person macht keinen Sport > Gesundheitsrisiko
- Isst gern Fastfood > Gesundheitsrisiko
- Hört Gewalt verherrlichende Musik > potentieller Vandale
- Macht Kampfsport > potentieller Vandale
- Name klingt islamisch > potentieller Terrorist
- Kontakt zu islamischen Ausländern > potentieller Terrorist

Folgen:

Die gesammelten Daten werden oft mit statistischen Daten verglichen, um so zu entscheiden wer ein Risiko darstellt, wer für was kauffreudig ist und um Vorurteile zu bilden.

- Käuferpotential > gezielte Werbeangebote
- Gesundheitsrisiko > schlechtere Berufschancen > schlechtere Versicherungsbedingungen oder sogar Versicherungsablehnung
- Potentieller Vandale > muss überwacht werden > schlechtere Berufschancen > schlechtere Glaubwürdigkeit vor Gericht
- Potentieller Terrorist > Einreiseverweigerung (z.B. in die USA) > schlechtere Berufschancen > muss überwacht werden > schlechtere Glaubwürdigkeit vor Gericht

4. Konfigurationsprofile

Je mehr Informationen über die eingesetzte Software/Hardware einer Person oder Firma bekannt sind, desto genauer können Angriffsprofile erstellt werden.

Informationen:
- Verwendete Softwareprodukte
- Aktualisierungszyklus der Endanwender
- E-Mail-Adresse

Szenario:
- Angreifer sammelt Softwareprofile von einer Vielzahl von Anwendern
- Angreifer wartet bis für eines der verwendeten Produkte eine Sicherheitslücke bekannt wird
- Angreifer nutzt Sicherheitslücke, um Schadsoftware bei allen angreifbaren Endanwender zu installieren
- Die Schadsoftware unterdrückt Virenscanner/ Desktopfirewall und andere Schutzsoftware

Problem
- Opfer war bereits angreifbar
- die Preis gegebenen Informationen wurden vom Angreifer gesammelt
- Der gezielte Angriff konnte in der Zeit zwischen der Entdeckung der Schwachstelle und der Aktualisierung durch den Endanwender erfolgen

Folgen:

Die Schwachstellenangriffe sind zeitkritisch, da damit zu rechnen ist, dass der Endanwender die entsprechenden Aktualisierungen irgendwann einspielen wird. Weiß aber ein Angreifer über die Systeme der Opfer Bescheid, so kann er sich eine langwierige Suche sparen. Ist ein System erst mal infiziert, können Angreifer diverse Schadsoftware nachinstallieren, sowie die Funktionsweise von Schutzsoftware (z.B. Virenscanner, Desktopfirewall) beeinflussen. Schadsoftware, die speziell für einzelne Angriffe entwickelt wurde, wird von Virenscannern in der Regel nicht entdeckt.

5. Bewegungsprofile

Informationen:
- Identifikationsnummer (IMEI) des Handys einer Person

Szenario:
- Person geht dem legalen Alltagsleben nach
- In einem Umkreis von wenigen Kilometern wird ein Verbrechen begangen
- Einige Wochen später bekommt die Person einen Brief mit Fragen darüber, was sie in der entsprechenden Nacht gemacht hat und ob es dafür Zeugen gibt
- Die Person kann sich nach der langen Zeit nicht mehr erinnern, verstrickt in Widersprüche
- Die Person wird damit vom Zeugen zum Tatverdächtigen

Problem:
- Der Standort von Handys wird mitprotokolliert
- Die deutschen Behörden und Ämter arbeiten langsam und sorgfältig > erfassen zu spät zu viele Daten

Hinweise:

Der Einsatz von IMSI-Catchern (Handyortung) ist in Deutschland derzeit nicht erlaubt. Allerdings lässt sich die deutsche Exekutive in vielen Fällen von den Einschränkungen ihrer Befugnisse nicht beeindrucken oder versucht, diese abzuschaffen. Mit entsprechenden Geräten können auch Angreifer, welche nicht dem Staat oder der TK-Gesellschaft angehören Handys orten oder abhören.

6. Zusätzliche Informationen

Zusätzlich zu den Informationen durch Ihre Antworten können bei Interviews oder Telefonumfragen Informationen über Stimmlage, Reaktionszeiten und Gesichtsausdruck erlangt werden.

7. Vorratsdatenspeicherung

Neben dem Fragebogen gibt es noch viele andere Möglichkeiten, Daten zu sammeln (Kundenkarten, Kreditkartendaten, Videokameras, …). Eine solche Möglichkeit ist z.B. die Erhebung und Speicherung von so genannten Nutzungs- und Verkehrsdaten.

Die Bundesregierung plant, diese Daten für sechs Monate auf Vorrat zu speichern. Mit diesen Daten soll unter anderem nachvollzogen werden, wer wann mit wem Kontakt hatte, wo sich Personen zu welchem Zeitpunkt aufgehalten haben und wann sie welche Internetseite besucht haben. Dies ist insbesondere für Journalisten, Anwälte, Ärzte und die Seelsorge ein Problem, da die Anonymität von Informanten, Mandanten, Patienten und Hilfsbedürftigen nicht mehr gewährleistet werden kann. Aber auch für jeden einzelnen Bürger und jede Firma kann dies zu einer Bedrohung werden. Neben den staatlichen Befugnissen soll ebenfalls ausländischen Geheimdiensten und Rechteinhabern (z.B. Musikindustrie) der Zugriff auf diese Daten gestattet werden. Zudem kann die Sicherheit der Daten nicht gewährleistet werden, wenn sogar Kreditkartenunternehmen gehackt und bestohlen werden. Es ist bekannt, dass es bei ausländischen Geheimdiensten üblich ist, Unternehmen im eigenen Land mit wirtschaftlich interessanten Informationen zu fördern. Zudem werden die Daten nicht vom Staat unter kontrollierten Bedingungen gesammelt, sondern durch die Anbieter von Internet-Zugängen unter der Last großer Kosten. Das organisatorische und rechtliche Chaos wird in vielen Fällen ebenfalls unberechtigte Zugriffe auf die Daten vereinfachen.

- Die Vorratsdatenspeicherung kehrt die Unschuldsvermutung um
- Die Vorratsdatenspeicherung ist verfassungswidrig
- Die Vorratsdatenspeicherung schränkt Grundrechte ein
- Die Vorratsdatenspeicherung ist teuer
- Die Vorratsdatenspeicherung ist von Kriminellen und Terroristen leicht zu umgehen
- Die Wirksamkeit der Maßnahme ist umstritten

Dieser Fragebogen ist eine Aktion des
Arbeitskreis Vorratsdatenspeicherung (AK Vorrat)
Der AK Vorrat ist ein bundesweiter Zusammenschluss von Bürgerrechtlern, Datenschützern und Internet-Nutzern, der die Arbeit gegen die geplante Vollprotokollierung der Telekommunikation koordiniert.

Weitere Informationen finden Sie unter
www.vorratsdatenspeicherung.de