Es gibt keine sicheren Daten

Widerlegung des Mythos vom sicheren IT-System

Inhaltsverzeichnis

1. Um was geht es?

Die Erfassung, Speicherung und Konzentration sensibler Daten nimmt zu. Solche Datensammlungen stellen an sich bereits eine große Gefahr für Personen, Gesellschaft und Wirtschaft dar. Diese massiven Risiken werden im allgemeinen stark unterschätzt oder gar nicht erkannt.

Anhand einiger beispielhafter Fälle eines Berufshackers sowie an exemplarischen Datenskandalen verdeutlichen wir die tatsächliche Bedrohung.

2. Aus der Praxis eines Berufshackers

Die kommenden Kapitel handeln vom Bericht eines deutschen „Berufshackers“ - eines IT-Pentesters und Sicherheitsfachmanns, dessen Beruf es ist, im Auftrag großer Konzerne und Unternehmen in deren IT-Systeme einzudringen und damit Schwachstellen aufzudecken.

In seinem Bericht „Analyse: Aktueller Stand der IT-Sicherheit in der Praxis“ beschreibt er die heutzutage tatsächlich vorliegenden Verhältnisse in datenverarbeitenden Unternehmen und belegt sie mit praktischen Beispielen. Ungenügende Qualifikation der Verantwortlichen und Personalmangel bei Ermittlungsbehörden führen häufig dazu, dass Angriffe auf IT-Systeme gar nicht oder erst nach längerer Zeit (6 Monate und mehr) erkannt und gestoppt werden können.

Thesen des Berufshackers

Der Berufshacker steht mit uns in Verbindung – bei Bedarf können wir den Kontakt zu ihm vermitteln. Er stellt in seinem Bericht folgende Thesen auf:

1. Stand heute:
   - Ein angemessener Schutz höchst sensibler Daten ist nicht möglich.
   - Computersysteme können nicht vollständig abgesichert werden.
   - Ein gezielter Angriff mit höchster Erfolgswahrscheinlichkeit ist in überschaubar kurzer Zeit möglich.
   - Selbst der "Stand der Technik" zum Schutz von IT-Systemen weist Probleme auf.
2. Das an IT-Sicherheit Mögliche wird in der Regel nicht umgesetzt.
   - Die IT ist zu komplex, als dass man alle Bereiche überblicken könnte.
   - Technische Konzepte weichen oft aus pragmatischen Gründen von der Realität ab.
   - Die notwendige Trennung von IT-Systemen wird in der Regel nicht durchgehend vorgenommen.
   - Aus Gründen der Arbeitserleichterung neigt man in der IT dazu, bestehende Sicherheitsmechanismen zu umgehen.
3. Es gibt ein Kommunikationsproblem zwischen IT und Restpersonal.
   - Nicht-IT-Mitarbeiter nehmen in der Regel an, dass „alles in Ordnung“ ist.
   - Auf diese Weise kann jemand, der nur genügend kompetent und freundlich auftritt, schnell in sensible Bereiche eines Unternehmens vordringen und an geheime Informationen gelangen.
4. IT- Angriffe sind mit wenig Fachwissen möglich, das man schnell im Internet findet.
   - Die Verteidigung ist entgegen landläufiger Vorstellung sehr komplex und schwierig umzusetzen.
5. Die reine konsolidierte Speicherung höchst sensibler Daten ist ein Problem.
   - Die beiden Ziele, einerseits sicheren und berechtigten Zugriff zu erlauben und gleichzeitig Missbrauch zu verhindern, lassen sich auf Dauer nicht umsetzen.

Um was für Daten geht es?

Beispiele für personenbezogene sensible Daten:

- Einkommensdaten
- Arbeitnehmerdaten
- Mitgliedschaften in Gewerkschaften, Vereinen, Gruppierungen
- Bank- und Bezahldaten
- Konsumdaten
- Bewegungsprofile
- Verhaltensprofile
- Scoring
- Teilnahme an Zeugenschutzprogrammen
- Gesundheitsdaten, Patientenakten
- Steuer- und Finanzdaten
- sexuelle Vorlieben
- politische Einstellung

Beispiele für sensible Daten in Wirtschaft, Industrie und Forschung:

- Forschungsprojekte
- Finanzdaten
- Steuerdaten
- Umsatzstatistiken
- Arbeitnehmerdaten
- nicht-öffentliche Kommunikation
- Angebote, Kostenvoranschläge
- Kundendaten
- Strategiepapiere
- interne Memos

2.1. Allfinanz-Konzern

Tatort:

Großer deutscher Allfinanz-Konzern

Auftrag:

Security Assessment

Randbedingungen:

Die Administratoren waren nicht informiert.

Bericht:

Das Unternehmen war durch Zugangssysteme mit elektronischen Zugangskarten gesichert. Am Haupteingang wurden Besucher durch den Wachschutz geprüft. Wir folgten einer Gruppe von Mitarbeitern, die das Gebäude betraten, man hielt uns die Tür auf. Anschließend teilten wir uns auf.

Wir suchten einen freien Besprechungsraum und fragten freundlich nebenan, ob der Raum reserviert wäre und ob wir ihn für den Tag nutzen könnten. Wir erhielten daraufhin einen Schlüssel, damit wir die Notebooks während der Mittagspause einschließen konnten. Von dort begannen wir die Vor-Ort-Überprüfung (Onsite-Pentest). Da wir nicht auffallen sollten, gingen wir vorsichtig und langsam vor. Nach ca. 3 Stunden hatten wir durch Umleiten des Datenverkehrs im Netzwerk Zugriff auf eine Datenbank mit Mahnverfahren, einige Fileserver und eine Handvoll Passwörter. Gegen Abend hatten wir durch Schwachstellen auf einigen Endsystemen, über die wir in andere Benutzer springen konnten, bereits Administratoren-Rechte.

Am nächsten Tag knackten wir innerhalb von 45 Minuten die Passwörter aller Mitarbeiter der Zentrale bis auf ca. 100. Wir deckten eine Reihe von Schwachstellen auf. Auch war es möglich, Aktionen mittels der digitalen (Benutzer-) Identität der Mitarbeiter zu starten.

Bei einem echten Vorfall wäre der Fokus der Untersuchung vermutlich auf den Mitarbeiter gefallen. Am dritten Tag beschlossen wir, offensichtlicher zu agieren. Der Angriff fiel am Abend des dritten Tages auf, als wir den Virenscanner auf einem zentralen System deaktivierten. Trotz intensiver interner Untersuchungen fand das IT-Sicherheitsteam kaum Spuren. Man kam zu dem Schluss, dass jemand das Passwort eines Service-Accounts herausbekommen hatte.

Die zweite Gruppe durchwanderte das Gebäude unter dem Vorwand, im Auftrag der IT-Abteilung alle Geräte zu inventarisieren. Dabei installierte man Keylogger und Accesspoints und nahm auf dem Tisch liegende Unterlagen mit. Man nahm Fehlausdrucke vom Drucker mit und druckte Dokumente aus dem Zwischenspeicher (Speicherabruf) der Abteilungskopierer aus. Am Tag verließen und betraten meine Arbeitskollegen mehrfach das Gebäude. Das Team erhielt unter dem Vorwand, den Brandschutz zu prüfen, sogar Zugang zum Rechenzentrum. Am zweiten Tag wurde das Team von einem Mitarbeiter aufgehalten, der korrekterweise den Wachschutz informierte. Der Wachschutzmitarbeiter kam kurz darauf und bat die soeben Ertappten, ihm zum Wachschutzgebäude zu folgen. Auf dem Weg erklärte man ihm, dass man den Auftrag hätte, alle Rechner zu inventarisieren. Dies nahm der Wachschutzmitarbeiter zum Anlass, dem Team eine Generalzugangskarte auszuhändigen. Eine Rücksprache mit einem Vorgesetzten oder Ansprechpartner fand nicht statt.

Fazit:

- Zugang zum Gebäude trotz modernster Sicherheitshardware möglich
- Im Gebäude konnte man sich frei bewegen
- Mitarbeitersensibilisierung war unzureichend
- Zugriff auf kritische Daten nach 3 Stunden
- Administrativer Zugang schon am ersten Tag
- Passwörter waren zu einfach und technisch schlecht geschützt
- Massive Schwachstellen im Anwendungsbereich
- Nachforschungen des IT-Sicherheitsteams waren zu oberflächlich und brachten kaum Erkenntnisse

2.2. Verfahrenstechnik-Unternehmen

Tatort:

Internationaler Spezialist für industrielle Verfahrenstechnik

Auftrag:

Security Assessment, Onsite-Pentest

Randbedingungen:

Die Administratoren waren nicht informiert.

Bericht:

Der Zutritt zum Gebäude erfolgte durch den Haupteingang, eine Kontrolle fand nicht statt. Im Gebäude waren die verschiedenen Bürobereiche durch ein Zugangssystem mit kontaktlosem Zugangsverfahren (RFID) gesichert. Auch hier konnte man ungehindert in alle Bürobereiche gelangen, indem man einfach hinter den Angestellten durch die Tür schlüpfte. Die Mitarbeiter fragten zwar, wer wir seien und was wir machten, gaben sich aber mit einfachen Antworten wie "Kontrolle der Feuermelder" oder "Rechnerinventarisierung" zufrieden. Wir platzierten mehrere Accesspoints und Keylogger. In einigen Gesprächen entlockte mein Kollege den Mitarbeitern ihre Passwörter, während ich unter dem Tisch den Computer präparierte.

Gegen Abend, als die Reinigungsfirma ihre Arbeit verrichtete und der Haupteingang eigentlich bereits geschlossen war, klopften wir, bis ein Reinigungsmitarbeiter die Tür öffnete. Mit der Ausrede, wir müssten dringend ein Gerät installieren und hätten die Zugangskarte vergessen, baten wir um Einlass. Nachdem die Reinigungsfachkraft ihren Vorgesetzten angerufen hatte, durften wir in das Gebäude und das Gerät installieren. Einer der Geschäftsführer war noch im Haus. Mit der Ausrede, gerade etwas testen zu wollen, installierten wir noch eine Software (Dummy) auf seinem Rechner.

Beim Onsite-Pentest erhielten wir in kürzester Zeit Zugriff auf kritische Informationen und administrative Passwörter. Der Grund dafür war ein Fehler im Betriebssystem der Netzwerkkomponente eines namhaften Herstellers, welcher dafür sorgte, dass trotz der korrekt konfigurierten Trennung (durch VLANs) Daten anderer Netze oder Anschlüsse ohne Angriff zu sehen waren. Außerdem war es möglich, sich mit einfachen Mitteln in eines der angeblich physisch getrennten Netze (VLANs) einzubuchen. Das Forschungs- und Entwicklungsnetz durften wir nicht untersuchen.
Es war jedoch möglich, die Telefonate aller Anschlüsse am Standort (getestet an 2 Testanrufen) gezielt mitzuschneiden.

Am zweiten Tag kam ein Mitarbeiter der IT-Abteilung, der aufgrund von "Warnmeldungen" den Switch wegen eines Defekts austauschen sollte. Der von der Hardware erkannte Angriff wurde von den IT-Leuten zum Defekt erklärt.

Fazit:

- Zugang zum Gebäude trotz modernster Sicherheitshardware möglich
- Im Gebäude konnte man sich trotz modernster Sicherheitshardware frei bewegen
- Mitarbeitersensibilisierung war unzureichend
- Zugriff auf kritische Daten nach 3 Stunden
- Administrativer Zugang schon am ersten Tag
- Passwörter waren zu einfach und technisch schlecht geschützt
- Massive Schwachstellen im Anwendungsbereich

2.3. IT-Dienstleister

Tatort:

IT-Dienstleister in einem großen deutschen Produktions- und Handelskonzern

Auftrag:

Security Assessment, Offsite-Pentest, Phishing-Angriff, Onsite-Pentest, Social engineering

Randbedingungen:

Die Administratoren waren informiert.

Bericht:

Der Zugang zum Gebäude und allen Teilen waren problemlos möglich. Im Keller befand sich ein unverschlossener Archivraum mit allen Skizzen, Patenten, Bauplänen, Rechnungen und anderen Informationen der letzten 15 Jahre in gedruckter Form. Auch bei diesem Kunden war die Installation von Keyloggern und Accesspoints möglich. Sogar in der Forschungs- und Entwicklungsabteilung mit den höchsten Sicherheitsanforderungen konnten wir einen Accesspoint und einen Keylogger installieren. Ein Zugriff auf die Systeme über den angebrachten Accesspoint vor Ort inkl. SAP war binnen weniger Minuten möglich.
Die Hardware blieb noch für ca. zwei Wochen installiert. Die Mitarbeiter hatten zwar teilweise die Accesspoints gesehen, diese allerdings für Radios oder Teile der seit Ewigkeiten angekündigten neuen Telefoninstallation gehalten.

Beim Offsite-Assessment konnten wir diverse Möglichkeiten für SQL-Injections finden, welche es erlaubten, in das interne Netzwerk des Kunden zu gelangen. Uns fiel ebenfalls auf, dass in dem IP-Bereich des Kunden eine Webseite mit diversen Schwachstellen gehostet war, von deren Existenz die Administratoren keine Ahnung hatten.

Weiterhin führten wir einen Phishing-Angriff durch. Die Mitarbeiter wurden aufgefordert, sich an einem Portal anzumelden, um dort den Termin für die Weihnachtsfeier abzustimmen. Mehrere Antworten sind bereits in der ersten Minute eingetroffen. Die Phishing-Attacke wurde nach ca. 3,5 Stunden entdeckt.

Während der Vor-Ort-Überprüfung (Onsite Pentest) erlangten wir unter anderem Zugriff auf Produktions, Entwicklungs- und Finanzsysteme. Besonders interessant waren einige Wartungszugänge, mit denen man sich in die Netze der Kunden des Unternehmens einklinken konnte.

Fazit:

- Zugang zu Gebäude und Hochsicherheitstrakt war problemlos möglich
- Ungesichertes Papierarchiv ist ebenfalls ein Risiko
- Installation von Spionage-Hardware war möglich
- Installierte Spionage-Hardware ist innerhalb von 2 Wochen nicht gemeldet wurden
- Entdeckte Hardware ist nicht untersucht wurden
- Zugriff auf kritische Informationen in kürzester Zeit
- Zugriff war auch von außen möglich
- Zugriff auch auf Kundennetze
- Phishing innerhalb weniger Minuten erfolgreich

2.4. Medizinbereich-Dienstleister

Tatort:

Mittelständischer Softwareanbieter und Dienstleister im Medizinbereich. Der Kunde verarbeitet höchst sensible Patienten-Daten. In seiner Aufgabe hat der Softwareanbieter Zugriff auf die produktiv Systeme seiner Kunden.

Auftrag:

Security Assessment, Offsite-Pentest, Phishing-Angriff, Onsite-Pentest, Social engineering

Randbedingungen:

Die Administratoren waren informiert. Der Einsatz von Keyloggern und Accesspoints war nicht gewünscht.

Bericht:

Die Phishing-Attacke bestand aus zwei Wellen. Es war technisch unterbunden, von außen E-Mails mit internem Absender zu schicken. Daher verwendeten wir eine "Webmail"-Adresse mit dem Namen eines IT-Mitarbeiters. In der ersten Welle schrieben wir 32 Personen aus Geschäftsführung und IT an. In der Mail wiesen wir auf das neue Portal hin. Der erste Geschäftsführer hat sein Passwort nach ca. 30 Sekunden eingegeben, insgesamt haben 29 Mitarbeiter geantwortet. Danach sind die Mitarbeiter gewarnt worden.

Die zweite Welle wurde eine Woche später an dieselbe Zielgruppe mit demselben Absender verschickt und beinhaltete den Link auf ein vermeintliches Sicherheitsupdate und folgenden Text: "Aufgrund der Phishing-Attacke von letzter Woche bitten wir Sie, folgenden Patch zu installieren." In Wirklichkeit handelte es sich um einen Trojaner (Dummy, der lediglich einen Zähler betätigt). Der Zähler zählte wiederum 11 Personen, die den Trojaner geöffnet hatten. Mit einem echten Trojaner wäre nach dem Klick dauerhaft ein Zugang zum Netzwerk des Kunden möglich gewesen.

Beim Offsite-Assessment waren lediglich wenige Dienste im Internet verfügbar. Die meisten Dienste waren bei einem Dienstleister gehostet. Es gab einige niedrige Schwachstellen, die direkt behoben wurden.

Der Zugang zum Gebäude war mittels eines Wachschutzempfangs geschützt, der Gästen einen entsprechenden Ausweis ausstellte. Wir gingen mit einem freundlichen "Guten Morgen" an dem Wachschutzmitarbeiter vorbei.
Der Aufzug funktionierte nur mit RFID-Token. Also entschlossen wir uns, das Treppenhaus zu nutzen. Bis auf die vierte Etage waren alle Bürotrakte ebenfalls durch RFID-Tokens abgesichert. In der vierten Etage befand sich eine große Stahltür mit einer Kamera und einer Klingel. Nach dem Klingeln öffnete sich die Stahltür, und man kam in eine kleine Personenschleuse mit einer zweiten Stahltür am Ende der Schleuse. Diese war ebenfalls kameragesichert. Danach gelangte man an einen Empfang. Wir täuschten ein intensives Gespräch vor und gingen zielstrebig am Empfang vorbei. Wie wir nachher aus einem Gespräch erfuhren, war die Empfangsdame ein wenig irritiert. Wir seien so zielstrebig an ihr vorbeigegangen, dass sie nicht wusste, wie sie reagieren sollte. Mit einem böswilligen Angriff hatte sie allerdings nicht gerechnet. Wir suchten eine Reinigungsfachkraft und ließen uns von ihr einen der Fahrstühle für den fünften Stock freischalten.

Während der Vor-Ort-Überprüfung erlangten wir innerhalb von 3,5 Stunden Administratorenrechte und hatten damit Zugriff auf alle Systeme. Es konnten alle Passwörter bis auf 2 innerhalb von 30 Minuten geknackt werden.

Fazit:

- Trotz Vereinzelungsanlage und höchster Sicherheitsmaßnahmen war ein Zugang für Fremde möglich
- Das Empfangspersonal war nicht darauf vorbereitet, einfach ignoriert zu werden
- Ein großer Teil der Mitarbeiter (29 von 32) ist auf den Phishing-Angriff hereingefallen, darunter auch das fachlich qualifizierte Personal
- Auch nach der Warnung sind 11 Mitarbeiter erneut auf den Trojaner hereingefallen
- Auch hier gelang der Zugriff innerhalb eines halben Tages
- Die Passwörter waren ebenfalls zu einfach

2.5. Immobilien-Investor

Tatort:

Ein erfolgreicher Investor im deutschen Immobilienmarkt

Auftrag:

Security Assessment, Offsite-Pentest, Phishing-Angriff, Onsite-Pentest, Social engineering

Randbedingungen:

Die Administratoren waren nicht informiert.

Bericht:

Das Offsite-Assessment war, wie wir im Nachhinein erfuhren, unglücklicherweise genau während eines Wartungsfensters. Da die Systeme abgeschaltet waren, fanden wir keine Dienste im Internet, die wir hätten angreifen können.

Auf die Phishing-Attacke gaben 2 Mitarbeiter ihr Passwort an. Dies fand allerdings ebenfalls aufgrund des Wartungszeitraums erst am nächsten Tag statt.

Das erste Social Engineering mit Prüfung der physikalischen Sicherheit führten zwei meiner Kollegen durch. Sie waren in der Lage, in allen Bereichen Keylogger und Accesspoints zu installieren.

Im Verlauf der Vor-Ort-Überprüfung (Onsite-Pentest) schafften wir es innerhalb von 2 Stunden auf die komplette Mietdatenbank (Preise, Mieteranschriften, Zahlungsrückstände, …) zuzugreifen. Normalerweise erfolgte der Zugriff über ein Frontend, welches die Eingaben auf Plausibilität prüfte. Der direkte Zugriff auf die Datenbank erlaubte es, diese Prüfung zu umgehen (z.B. ohne Zahlungseingang Schulden zu tilgen, oder ohne Vermerk in der Historie die Mietpreise zu senken). Im Laufe des Tages erhielten wir ebenfalls Zugriff auf alle Kernapplikationen und Dateiablagen.

Der Einsatz war insbesondere deswegen interessant, weil die IT-Sicherheit des Unternehmens eine eigene Sicherheitsüberprüfung anhand der Dokumentationen und Policies durchgeführt hatte. Von dieser Seite waren viele Punkte eigentlich bereits erledigt, was wir aber in der realen technischen Umsetzung nicht nachvollziehen konnten.

Gegen Ende der Vor-Ort-Überprüfung führten wir ein zweites Social Engineering mit Untersuchung der physikalischen Sicherheit durch, um die bereits platzierte Ausrüstung wieder einzusammeln. Über vereinzelte Mitarbeiter oder das Reinigungspersonal war es trotz modernster elektronischer Zugangssysteme auch in der Zeit von 20 bis 22 Uhr möglich, in alle Bereiche einschließlich des Geschäftsführerbüros zu gelangen und dort Hardware mitzunehmen.

Fazit:

- Auch hier war ein Zugriff innerhalb kürzester Zeit möglich
- Auch hier war der Phishing-Angriff möglich
- Bewegung im Gebäude auch nach regulärer Arbeitszeit möglich

2.6. Großkonzern-Produktion

Tatort:

Produktionsfirma eines deutschen Konzerns

Auftrag:

Security Assessment, Offsite-Pentest, Social engineering

Randbedingungen:

Die Administratoren waren informiert. Der Einsatz von Keyloggern oder Accesspoints war nicht gewünscht.

Bericht:

Die Überprüfung über das Internet (Offsite Pentest) wurde als erstes durchgeführt. Ein Zugriff auf Kernsysteme war aus dem Internet möglich. Die Systeme waren nicht gehärtet. Nach 40 Minuten waren wir Administratoren auf den Systemen und hatten Zugriff auf das interne Netzwerk.

Die Vor-Ort-Überprüfung (Onsite Pentest) ergab, dass wegen mangelnder Netztrennung vollständiger Zugriff auf andere Konzernfirmen möglich war.

Bei Prüfung der physikalischen Sicherheit und des Social-Engineering war der Zugang zu allen Bereichen möglich. Wir nahmen Unterlagen und Datenträger mit.

Bei der Phishing-Attacke wurden 12 Benutzer angeschrieben. Nach zwei Minuten hatte der erste Benutzer sein Passwort angegeben. Acht von zwölf Benutzern haben geantwortet.

Fazit:

- Zugang zum Gebäude war möglich
- Zugriff auf kritische Systeme über das Internet binnen kürzester Zeit möglich
- Zugriff auf interne Systeme und andere Konzernteile durch mangelnde Netztrennung
- Phishing innerhalb kürzester Zeit erfolgreich

2.7. Medienkonzern

Tatort:

Ein großer deutscher Medienkonzern

Auftrag:

Prüfung eines Internet-Terminals im Eingangsbereich

Randbedingungen:

Das Terminal war angeblich physikalisch vom Unternehmensnetz getrennt

Bericht:

Ohne vorinstallierte Software schafften wir es innerhalb von 6 Minuten, Zugriff auf einen internen Terminal-Server zu erlangen. Der Wechsel zwischen den angemeldeten Identitäten war möglich. Nach ca. 45. Minuten hatten wir Administratorenrechte und Zugriff auf das Redaktionssystem sowie einen Server mit Finanzdaten.

Nach ca. 90 Minuten wurde der Einsatz als abgeschlossen erklärt, weil wir unser Ziel erreicht hatten.

Fazit:

- Zugriff auf das Unternehmensnetz in wenigen Minuten möglich
- Die vermeintliche Netztrennung war unzureichend, da einige Dienste wohl geroutet wurden
- Es waren keine besonderen Tools für einen Angriff nötig

2.8. Rüstungskonzern

Tatort:

Tochterunternehmen eines amerikanischen Rüstungskonzerns

Auftrag:

Security Assessment, Gezielte Überprüfung der Konfiguration vor Ort.

Randbedingungen:

Die Administratoren waren informiert.

Bericht:

Auch hier konnten vertrauliche Daten und Passwörter über das Netzwerk mitgelesen werden. Wir erhielten Zugriff auf alle primären Datenbanken und alle Serversysteme.

Zudem stellten wir fest, dass die Administratoren die Sicherheitsmaßnahmen, z.B. regelmäßigen Passwortwechsel, durch technische Tricks umgingen.

Im Unternehmen gab es ein striktes Antragsverfahren für Benutzerkonten. Dies wurde ebenfalls durch massive Mehrfachnutzung vorhandener Accounts ad absurdum geführt.

Fazit:

- Zugriff auch hier auf alle Daten möglich
- Aktuelle Sicherheitsmaßnahmen sind selbst von Administratoren umgangen wurden
- In einem Unternehmensnetzwerk lässt sich Software unbemerkt installieren

2.9. Sicherheitsanbieter

Tatort:

Ein Sicherheitsanbieter

Auftrag:

War nicht vorhanden - Lücke wurde bei der Nutzung des Internetportals per Zufall entdeckt.

Randbedingungen:

Keine definierten.

Bericht:

Die zufällig gefundene Sicherheitslücke erlaubte es, auf eine große Zahl von Kunden zuzugreifen - darunter diverse Großkonzerne, Banken und Regierungsinstitutionen verschiedener Länder.

Die Sicherheitslücke ließ sich allein mit einem Browser ausnutzen. Grundsätzlich ist die Empfehlung, sich nicht auf eine Sicherheitsmaßnahme zu verlassen, sondern immer mehrere Maßnahmen zu kombinieren. Allerdings wird dies in der Praxis nicht immer berücksichtigt. Daher wäre ein Zugriff auf viele der Kunden wahrscheinlich gewesen.

Der Hersteller hatte binnen weniger Stunden reagiert. Trotzdem hätte ein Angreifer mit bösen Absichten nicht abschätzbare Schäden herbei führen können.

Fazit:

- Auch Sicherheitsspezialisten haben Sicherheitslücken
- Einige Sicherheitslücken bei zentralen Anbietern erlauben die Beeinflussung vieler Systeme
- Auch wenn man selbst einiges für die Sicherheit tut, ist ein Angriff über Softwarehersteller, Dienstleister oder andere Schnittstellen möglich.
- angreifbare Daten

3. Datenmissbrauch ist möglich und findet statt

Datenmissbrauch findet täglich statt. Im Gegensatz zu klassischen Fällen kommt es im IT-Umfeld oft zum Verlust großer Datenmengen. Die folgenden Beispiele mit schwerwiegenden Vorfällen geben einen kleinen Einblick in das, was möglich ist und passiert.

Solche Missbrauchsfälle kommen oft nicht ans Licht. Die in der Vergangenheit bekannt gewordenen Fälle wurden oft nur deshalb publik, weil ein Insider Jahre nach den Vorfällen ausgepackt hat.

3.1. Deutsche Telekom

Tatort:

Deutschland, Deutsche Telekom, einer der führenden deutschen Telekommunikationsdienstleister

Tatzeit:

2006 bis 2008

Opfer:

Ca. 17 Millionen Kunden, kritische Journalisten

Bericht:

Im Jahr 2006 werden der Deutschen Telekom 17 Millionen Kundendatensätze gestohlen, darunter auch die Daten geheimer Telefonnummern von Ministern, Politikern, Ex-Bundespräsidenten, Wirtschaftsführern, Milliardären und Kirchenvertretern.

Die Deutsche Telekom beauftragt eine Detektei, Medienberichte auswerten zu lassen: Besonders kritische bzw. investigative Journalisten landen auf einer Liste, und die ersten fünf Journalisten dieser „Hitparade“ werden monatelang bespitzelt.

Außerdem überprüft die Telekom illegalerweise die Telekommunikations-Verbindungsdaten von etwa 60 Personen – dazu nutzt sie ihren selbst verwalteten Datenpool genau so, wie sie sich Verbindungsdaten von einem inländischen Konkurrenten sowie von einem weiteren ausländischen Unternehmen besorgt.

Im Mai 2008 wird der gesamte Skandal öffentlich. Fünf Manager und Mitarbeiter werden von den Aufgaben entbunden und in einen „Erholungsurlaub“ geschickt.

Fazit:

- Großflächiger und schwerwiegender Datenmissbrauch sensibler Verbindungsdaten durch führenden Provider Deutschlands
- Aufdeckung nur aufgrund des Whistleblowings einer einzelnen Person.

Quellen:
http://www.telekom.com/dtag/cms/contentblob/dt/de/812996/blobBinary/dt_open_book_abschlussbericht.pdf
http://www.zeit.de/online/2008/41/telekom-datenklau

3.2. Deutsche Bahn AG

Tatort:

Deutschland, Deutsche Bahn AG, ein (noch) staatseigenes Verkehrsunternehmen, das den beherrschenden Großteil des Schienenverkehrs in Deutschland betreibt.

Tatzeit:

2002 bis 2009

Opfer:

Ca. 173.000 Mitarbeiter, Gewerkschafter, Journalisten, ein Bundestagsabgeordneter

Bericht:

Anfang 2009 wurde (nur aufgrund investigativ arbeitender Journalisten) bekannt, dass die Deutsche Bahn in den Jahren 2002 und 2003 eine systematische Überwachung von etwa 70.000 bis 80.000 Mitarbeitern durchgeführt hat. Täglich wurden etwa 150.000 Mails kontrolliert. Erst im Oktober 2008 wurde diese Aktion gestoppt.

Die Bahn hatte Daten von 173.000 ihrer 240.000 Mitarbeiter an die Detektei "Network Deutschland" weitergegeben. Anhand von Adressdaten und Bankverbindungen sollten die Ermittler überprüfen, ob Mitarbeiter mit Scheinfirmen Geschäfte zu Lasten der Bahn abwickeln. Dazu waren die Daten mit denen von 80.000 Lieferanten abgeglichen worden.

Weiterhin hat die Deutsche Bahn wiederholt Stammdaten ihrer Mitarbeiter (u.a. Anschriften, Telefonnummern und Bankverbindungen) mit anderen Datenbanken abgeglichen.

Dabei ging es nicht mehr nur um fragwürdige Methoden zum Aufdecken von Korruption. Die Mailüberwachung sollte offenbar unerwünschten Informationsfluss unterbinden, beispielsweise Streikinformationen von Mitgliedern der Gewerkschaft Deutscher Lokführer (GDL).

So fiel GDL-Funktionären auf, dass ihre Mails bei den Adressaten nicht ankamen. Auch elektronische Post, die Bahnmitarbeiter an kritische Journalisten schickten, spürten die Mailwächter auf, ebenso Schreiben an Wissenschaftler und Verkehrsfachleute, darunter auch ein Bundestagsabgeordneter, der sich öffentlich mit Kritik an der Bahn zu Wort meldete.

Im weiteren Verlauf wurden Fälle bekannt, in denen Bankkonten, Privatkontakte und weitere persönliche Informationen eingeholt und ausgewertet wurden. So wurden beispielsweise Videoaufnahmen von Tankstellen besorgt, die Mitarbeiter ansteuerten.

Nach weiteren Recherchen seien in mehreren Fällen auch Daten der Mitarbeiter manipuliert worden. Diese Manipulationen seien anschließend unter anderem zur Kündigung von Kritikern des damaligen Bahnchefs Mehdorn und der Kapitalprivatisierung genutzt worden. Auch die Gewerkschaft Transnet hatte das Unternehmen mindestens zweimal um einen Abgleich der Mitglieder- mit der Mitarbeiterdatei gebeten, um die korrekte Zahlung von Beiträgen zu überprüfen.

In mindestens neun Fällen wurde ein Berliner "Recherchedienst" zur Überprüfung von Mitarbeitern, deren Ehepartnern, Lieferanten und sonstigen Vertragspartnern beauftragt.

Ende Mai 2009 wurde bekannt, dass der Leiter der Compliance im Januar 2009 Daten zur Vertuschung der Datenaffäre hatte vernichten lassen.

Fazit:

- Schwerwiegende Datenmissbräuche
- Aufdeckung nur schleppend und widerwillig
- „Erfolgreiche“ Vertuschung durch die Vernichtung von Daten

Quellen:
http://www.heise.de/newsticker/meldung/Bahn-soll-jahrelang-150-000-Mails-pro-Tag-gefiltert-haben-209988.html
http://www.heise.de/newsticker/meldung/Bahn-soll-Mitarbeiter-Mails-systematisch-durchforstet-haben-209878.html
http://www.heise.de/newsticker/meldung/Datenaffaere-Gewerkschaften-verlangen-von-Bahn-Chef-Entschuldigung-204214.html

3.3. Einwohnermeldeamt

Tatort:

Deutschland, mehrere Behörden

Tatzeit:

2008

Opfer:

Deutsche Einwohner aus 200 Städten und Gemeinden

Bericht:

In Deutschland ist jeder Einwohner dazu verpflichtet, sich im so genannten Meldeamt der Verwaltungsgemeinde anzumelden, in der er seinen Lebensmittelpunkt hat. Etliche persönliche Daten werden aufgenommen und dezentral gespeichert.

Diese zum Teil sehr intimen Daten waren aufgrund einer menschlich-technischen Panne im Potsdamer Meldeamt (nahe Berlin) für einige Wochen im Frühjahr 2008 schutzlos und für jeden zugänglich im Internet abrufbar.

Was war passiert?

Mitarbeiter hatten versäumt, nach der Installation der Software für das Melderegister das mitgelieferte Standardkennwort zu ändern. Das aber stand zu Demonstrationszwecken auch eine Weile auf der Internetseite des Softwareherstellers. So war es möglich, Zugriff auf den eigentlich streng geschützten Datenbestand zu erlangen. Nach Angaben des Softwareherstellers waren von der Datenpanne insgesamt 15 Kommunen betroffen.

Auch prominente Potsdamer wie der Fernsehmoderator Günther Jauch, die Schauspielerin Nadja Uhl oder das vom Modeschöpfer Wolfgang Joop entdeckte Model Franziska Knuppe hätten aufgrund der Panne ausgespäht werden können.

Fazit:

- Ein einfaches Missgeschick führt zu einer weitreichenden Gefährdung sensibler, nicht-öffentlicher Daten
- Aufdeckung des Skandals durch investigativen Journalismus

Quelle:
http://www.heise.de/newsticker/meldung/Gut-dass-es-passiert-ist-Datenpanne-zwingt-zum-Umdenken-216194.html

3.4. Polnischer Presseskandal

Tatort:

Polen, die Polizei und zwei große Geheimdienste

Tatzeit:

2005 bis 2007

Opfer:

Mindestens 10 bekannte und einflussreiche Journalisten sowie deren Kontakte

Bericht:

Die große polnische Tageszeitung "Gazeta Wyborcza" entdeckte im Oktober 2010, dass mindestens 10 einflussreiche Journalisten im Zeitraum von 2005 bis 2007 Opfer einer Überwachung wurden (damals regierte die konservative rechte Partei PiS). Die Polizei und zwei große Geheimdienste (Central Anticorruption Bureau und Internal Security Agency), veranlassten, dass die Kommunikationsdaten durch die Telekommunikationsanbieter gespeichert wurden (Inhalts- und Verbindungsdaten), um die Quellen der Journalisten aufzudecken. Der Zugriff auf die Daten durch Polizei und Geheimdienste erfolgte ohne gerichtlichen Beschluss oder eine andere Legitimierung, und die Ermittlungen waren nicht Teil eines laufenden Verfahrens. Es ist offensichtlich, dass die Nutzung des Datenverkehrs und der Verbindungsdaten nicht verfassungskonform war und ein erschreckendes Beispiel für Datamining und Missachtung der Pressefreiheit darstellt.

Als Resultat dieser Aktionen waren Polizei und Geheimdienste in der Lage, Quellen von Journalisten ausfindig zu machen. Wie man sagt, verloren einige Informanten aus der Verwaltung und der Polizei Ihren Job, weil sie an politisch strittigen Themen arbeiteten. Diese Entlassungen waren Anlass für die Staatsanwaltschaft, mögliche illegale Überwachungen zu untersuchen. Polizei und Geheimdienste bestritten eine Überwachung.

Die Untersuchung wurde aufgrund mangelnder Beweise eingestellt.

Einer der Journalisten forderte eine Wiedereröffnung der Untersuchung und gewann den Fall. Das Gericht ordnete eine detaillierte Untersuchung an.

Fazit:

- Vorratsdatenspeicherung wurde benutzt, um die Quellen von Journalisten zu identifizieren.
- Es gab keine rechtliche Legitimation.
- Polizei und Geheimdienste konnten erfolgreich die Quellen von Journalisten zurückverfolgen.
- Der Verstoß gegen das Recht auf Privatsphäre und das Pressegeheimnis führte zur Untersuchung durch die Staatsanwaltschaft
- Das Untersuchung wurde zunächst mangels Beweisen eingestellt und nur auf Nachdruck eines Journalisten neu eröffnet.

Quellen:
http://tvp.info/informacje/polska/inwigilacja-dziennikarzy-zamiatana-pod-dywan/3424956
http://wyborcza.pl/1,75478,8842563,Inwigilacja_dziennikarzy_badana_od_nowa.html

3.5. Operation Pecunia

Tatort:

USA, Großbritannien, Deutschland

Tatzeit:

1999 bis 2007

Opfer:

Mehrere zehntausend zu Unrecht Verdächtigte – diese Falschbeschuldigungen trieben 39 Menschen in den Selbstmord!

Bericht:

Ein junger Navy-General und 38 weitere Personen aus England nahmen sich das Leben, nachdem sie aufgrund von Datenspuren der Beschaffung kinderpornografischen Materials beschuldigt und teilweise verurteilt worden waren. Der junge Navy-General war vom Dienst suspendiert worden, obwohl sich die Vorwürfe gegen ihn in den vorherigen Ermittlungen nicht erhärtet hatten.

Die als „Operation Pecunia“ oder auch als “Operation Ore” betitelte große Polizeioperation begann 1999 in den USA und betraf viele Zehntausende angeblicher Konsumenten von Kinderpornographie.

Im April/Mai 2007 stellte sich heraus, dass ein großer Teil der 7.000 verdächtigten Briten Opfer von Kreditkartenbetrügern waren, darunter wohl auch mehrere der Menschen, die sich das Leben genommen hatten. Ihre Kreditkartendaten waren „gephisht“ und dann benutzt worden, um Zugriff auf Kinderporno-Seiten zu bezahlen. Ob überhaupt ein tatsächlicher Abruf von Bildern oder Videos stattfand oder es sich um reine Geldwäsche handelte, ist nicht geklärt.

Die Geschädigten wurden auf Basis völlig unzureichender Anhaltspunkte angeklagt und zum Teil auch verurteilt.

Fazit:

- Massenhafte Falschverdächtigungen mit tödlichen Folgen

Quelle:
http://oraclesyndicate.twoday.net/stories/4122817/
http://en.wikipedia.org/wiki/Operation_ore

3.6. Missbrauch von Vorratsdaten in den Niederlanden

Tatort:

Niederlande, Strafverfolgungsbehörden und Staatsanwalt

Tatzeit:

2009

Opfer:

Ein niederländischer Enthüllungsjournalist, ein niederländischer Sicherheitsexperte, sechs Freunde des Journalisten

Bericht:

Ein niederländischer Journalist deckte Sicherheitslücken im E-Mail-Zugang des Verteidigungsministers Jack de Vries auf. Dabei veröffentlichte der Journalist keine der sensiblen Daten, auf die er gestoßen war, sondern informierte die Behörden über die mögliche Gefährdung der nationalen Sicherheit. Später schrieb er einen Artikel im niederländischen Magazin "Nieuwe Revu". Doch statt sich darüber zu freuen, dass die Lücken durch einen wohlmeinenden Journalisten aufgedeckt wurden, reagierten die Behörden mit Strafverfolgung.

Im Verlauf des Gerichtsverfahrens fand der Journalist in den Akten seine kompletten Telekommunikationsdaten der vergangenen Zeit - einschließlich anonymer Quellen in Artikeln, die mit dem Gegenstand des Verfahrens nichts zu tun hatten. Er fand selbst die kompletten Telekommunikationsdaten seiner Freunde, die zufälligerweise den gleichen Vornamen wie der Sicherheitsexperte hatten, der ihm bei den Ermittlungen behilflich gewesen war. Sie wurden belauscht, obwohl der Name und der Arbeitgeber des Sicherheitsexperten im veröffentlichten Magazinbeitrag standen und man so auf andere und vor allem weniger zudringliche Art an die Identität des Mannes hätte gelangen können.

Das heißt, dass alle Vornamen aus dem Adressbuch des Journalisten durch die Behörden mit Hilfe der CIOT-Datenbank rekonstruiert wurden, einer nationalen Datenbank, in der die Daten aller Telekommunikationsteilnehmer in den Niederlanden gespeichert werden.

Zwar wurde der Journalist nicht verurteilt, aber er sagte uns, er habe Angst, in Zukunft Artikel dieser Art zu schreiben.

Fazit:

- Vorratsdatenspeicherung legte anonyme Quellen des Journalisten von Recherchen zu Artikeln offen, die keine Beziehung zum eigentlichen Verfahren hatten.
- Zugriff auf Telekommunikationsdaten wird nicht etwa verlangt, weil es nötig ist, sondern weil es leicht fällt.
- Durch Vorratsdatenspeicherung kann jeder im Verlauf einer Untersuchung allein dadurch zum Verdächtigen werden, dass er den gleichen Vornamen wie einer der Verdächtigen hat.

Quellen:
http://www.edri.org/files/Data_Retention_Conference_031210final.pdf

4. Komplexe IT-Systeme sind unbeherrschbar

4.1. Steuer-ID-System

Tatort:

Deutschland, überall

Tatzeit:

2007

Opfer:

Eine unbekannte Anzahl an Bürgern Deutschlands

Bericht:

Die Steuer-ID ist eine in Deutschland am 1. Juli 2007 eingeführte eineindeutige Identifikationsnummer im Zusammenhang für Steuerzwecke (TIN Tax Identification Number).

Diese Nummer ist unter Verfassungsrechtlern sehr umstritten, weil befürchtet wird, dass sie zu einer einheitlichen Personenkennziffer mutieren kann, deren Einführung vom Bundesverfassungsgericht eindeutig untersagt worden ist.

Bei der Ausgabe und Zuordnung der Steuernummern stellte sich heraus, dass nicht nur veraltete Daten eingespielt worden waren (alleine in Stuttgart konnten über 15.000 Briefe mit der Mitteilung der Steuer-ID nicht zugestellt werden).

Es wurde bekannt, dass das Datenverarbeitungssystem fehlerhaft war, was zu einem bundesweit großen Datenschlamassel führte:

Bürger wurden plötzlich mit falschen Geburtsnamen bedacht und in Ausländer verwandelt, ihre Geburtsorte kurzerhand verlegt. Besonders hoch war die Fehlerquote in Stade. "Gefühlte 100 Prozent der versandten Bescheide sind mit falschen Daten versehen", erklärte der Vize-Bürgermeister der niedersächsischen Kleinstadt Dirk Kraska gegenüber heise online. (…)

Kraska selbst stammt laut seinem Bescheid aus dem Libanon und hört auf den Geburtsnamen Solonin. Wie die Bild-Zeitung berichtet, heißt zudem etwa der Rentner William Jung jetzt mit Nachnamen "Ficken" und wurde in "Hamburg, Kasachstan" geboren. Astrid Brauer stammt demnach angeblich aus dem Iran, ihr Mann aus Russland und ihr Sohn aus Spanien.

"Wir sind ratlos, wo das Problem liegen könnte", führt Kraska weiter aus. Die Meldebehörde habe eine CD ans BZSt geschickt, so dass eine Veränderung der Daten beim Versand übers Internet ausgeschlossen werden könne.

Fazit:

- Massenhaft fehlerhafte Datenverarbeitung staatlicher Datenbanken in einem sensiblen Zusammenhang.
- Aufdeckung des Skandals nur aufgrund der Tatsache, dass die Bürger über einen Teil der über sie gespeicherten Daten initiativ informiert wurden.

Quelle:n
http://www.heise.de/newsticker/meldung/Kommunen-melden-grobe-Fehler-bei-Ausgabe-der-neuen-Steuernummer-195197.html
http://www.heise.de/newsticker/meldung/Bundesweit-Pannen-beim-Versand-der-neuen-Steuernummer-201607.html

4.2. Neuer elektronischer Personalausweis

Tatort:

Deutschland, überall

Tatzeit:

2010

Opfer:

Zahlreiche Bürger aus Deutschland

Bericht:

Mit dem 1.11.2010 wurde in Deutschland ein neues Ausweisdokument eingeführt: der elektronische Personalausweis „E-Perso“. Dieser Ausweis enthält einen RFID-Funkchip, der neben den Passdaten und dem biometrischen Merkmal des Gesichtes auch Fingerabdrücke sowie eine so genannte „qualifizierte elektronische Signatur“ enthalten kann.

Um die Akzeptanz der neuen Technik zu erhöhen, beschloss man, einigen Bürgern kostenlose Kartenlesegeräte (im Wert von mindestens etwa 16 Millionen Euro!) zur Verfügung zu stellen. Es stellte sich jedoch heraus, dass der Einsatz dieser Geräte an Heim-PCs zu ernsthaften Sicherheitsproblemen (inklusive des Diebstahls der Identität) führen kann.

Etwas später (kurz nach Einführung des Ausweises) fand ein IT-Experte (auf private Initiative!) heraus, dass die vom Bundesamt zur Verfügung gestellte Software in ihrem Update-Modul eine schwere Sicherheitslücke aufwies, durch die Trojaner hätten Zugang finden können.

Kurz danach kam es dann zu Datenpannen, wonach auf den hergestellten Ausweisdokumenten falsche Namen eingetragen waren.

Schließlich stellt sich Mitte Dezember 2010 heraus, dass einige der neuen Ausweise versehentlich mit leeren Funkchips ausgestattet worden sind. Außerdem funktionierte das Sperrkennwort nicht, mit dem im Normalfall die Weitergabe oder das Auslesen bestimmter Daten eingeschränkt werden soll.

Fazit:

- Zahlreiche Datenverarbeitungspannen in staatlich organisiertem IT-Projekt
- Aufdeckung durch betroffene Bürger, engagierte IT-Experten und einer NGO

Quellen:
http://www.heise.de/newsticker/meldung/Fehlerhafte-Personalausweise-in-Hessen-1141762.html
http://www.heise.de/newsticker/meldung/Stotterstart-des-neuen-Personalausweises-1145554.html
http://www.heise.de/ct/artikel/ePerso-Alltag-Vom-Foerdern-und-Fordern-Update-1147116.html
http://www.mdr.de/nachrichten/7979773.html

4.3. Elektronische Gesundheitskarte

Tatort:

Deutschland, überall

Tatzeit:

Seit 2004

Opfer:

Potenziell alle Bürger Deutschlands

Bericht:

Die elektronische Gesundheitskarte (kurz: eGK) soll als staatliches Großprojekt für eine vereinheitliche Erfassung persönlicher Gesundheitsdaten sorgen, diese verwalten und schnell und effizient den Menschen und den sie behandelnden Stellen zur Verfügung stellen. Abrechnung von Arztkosten, Datenverwaltung, Rezeptverschreibungen sollen vereinfacht und beschleunigt werden.

Dazu hat die deutsche Bundesregierung eigens eine Gesellschaft mit dem Namen „Gematik“ geschaffen, die dieses IT-Großprojekt organisieren und durchführen sollte.

Nachdem bereits im Jahr 2004 in einem Gesetz festgelegt worden war, dass die eGK zum 1.1.2006 eingeführt werden soll, ist dieses bis heute noch nicht geschehen.

Das Projekt hat bislang außer mehreren hundert Millionen Euro Kosten keine zufriedenstellende oder gar funktionierende Infrastruktur zu produzieren vermocht.

Mehrere „Feldtests“ liefen nicht unzufriedenstellend oder mussten gar abgebrochen werden. Die Akzeptanz unter Ärzten, Apothekern und Krankenkassen ist schlecht, die praktische Umsetzung der Technik hat sich vielfach als unpraktisch bis unmöglich erwiesen.

Dieses hatte zur Folge, dass die Anforderungen an die eGK immer weiter heruntergeschraubt wurden. Allerdings gibt es bis heute keinen politischen Mut zur Aufgabe des Projektes. Stattdessen soll die Karte mit Hilfe neuer Gesetzesverordnungen unter Zwang eingeführt werden.

Die datenschutzrechtlichen Aspekte der unzulänglichen Sicherheitsarchitektur und das mangelhafte Konzept der Datenverwaltung sollen an dieser Stelle völlig unbeachtet bleiben.

Fazit:

- Staatliches IT-Großprojekt, das praktisch gescheitert ist und dennoch durchgesetzt werden soll
- Versprechungen zu Leistungsumfang, Terminierung, Kosteneinsparungen und Datenschutz wurden nicht eingehalten
- Ignorieren von Sachkritik von IT-Experten und Datenschützern

Quellen:
http://www.heise.de/tp/r4/artikel/29/29895/1.html
http://www.heise.de/newsticker/meldung/Elektronische-Gesundheitskarte-Zwangsmassnahme-E-Card-21-1135915.html

4.4. Schengener Informationssystem SIS-II

Tatort:

Europäische Union

Tatzeit:

2001 bis 2010

Opfer:

Alle EU-Europäer

Bericht:

Ein weiteres Beispiel ist das europaweite Großprojekt zum Neuaufsetzen des Schengener Informationssystems SIS-II.

Im Jahr 2001 wurde der politische Wille manifestiert, das bisherige Informationssystem SIS zur EU-weiten polizeilichen Fahndungs- und Informationsarbeit grundsätzlich neu zu entwerfen. Diese Maßnahme hielt man für „unabdingbar“, und so wurde in 2004 der Auftrag zur Erfüllung dieser Arbeiten an ein internationales Konsortium von IT-Großunternehmen erteilt.

Die Bundesregierung sprach von zu erwartenden Kosten in Höhe von 14,6 Millionen Euro – die Fertigstellung wurde für 2006 anvisiert.

Um es kurz zu machen: Nach vielen Verzögerungen, Pannen und Problemen stellte man im Jahr 2009, also drei Jahre nach dem eigentlichen Fertigstellungstermin, fest, dass man SIS-II eigentlich doch gar nicht benötigen würde, weil das alte System SIS entgegen vorher geäußerten Behauptungen nun doch ausreichend erweitert werden konnte.

Trotzdem wollte die zuständige EU-Kommission nicht von SIS-II abrücken, bis dann endlich im Oktober 2010 durch das EU-Parlament die Notbremse gezogen und dem Projekt der Geldhahn zugedreht wurde: Alleine für das Jahr 2011 wurden 30 Millionen Euro veranschlagt, weitere 90 Millionen sollten bis zum Jahr 2013 folgen.

Die menschenrechtlichen Bedenken, die zweifelhafte staatsvertragliche Behandlung des SIS-II-Abkommens und die großen Datenschutzbedenken im Zusammenhang mit SIS sollen an dieser Stelle erst gar nicht angegangen werden.

Fazit:

- Misslingen eines europäischen IT-Großprojekts
- Fehleinschätzung von Technik und Kosten
- Nicht-Fähigkeit zum rechtzeitigen Abbrechen des Projekts
- (Außerdem: Verletzung der europäischer Menschenrechtskonvention)

Quellen:
http://www.heise.de/tp/r4/artikel/32/32490/1.html
http://www.heise.de/newsticker/meldung/EU-Parlament-dreht-SIS-II-den-Geldhahn-zu-1122320.html

5. Zusammenfassung und Fazit

Zusammengefasst:

- Daten sind nicht sicher – Missbrauch findet statt
- Vorfälle gelangen in aller Regel nicht an die Öffentlichkeit

Fazit

Digitale Daten haben die Eigenschaft, in ihrer Verbreitung und Langlebigkeit unbeherrschbar zu sein. Sie stellen damit ein für das Fortbestehen und die Weiterentwicklung demokratischer Gesellschaftsstrukturen bis dato nicht überschaubares Risiko dar.

Die konzentrierte Speicherung von sensiblen Daten ist mehr als grob fahrlässig.

Datensparsamkeit und die Vermeidung konzentrierter oder vereinheitlichter Informationen müssen sich zum unbedingten Gebot staatlichen Handelns entwickeln.

6. Glossar

Accesspoint ….... Komponente, die ein drahtloses Netzwerk bereitstellt bzw. mit einem physikalischen Netzwerk verbindet.

Accounts ….... Benutzerkonten zur Anmeldung bei einem Dienst oder System

Administrator …..... Person, welche für die Verwaltung der Computersysteme, Server oder Programme innerhalb einer Organisation/eines Netzwerks zuständig ist und in der Regel Zugriff auf alle Daten und Einstellungen hat.

Browser …..... Programm zum Herunterladen und Anzeigen von Webseiten.

BZSt …..... Bundeszentralamt für Steuern

Compliance …..... Einhaltung von Richtlinien oder gesetzlichen Vorgaben

Data Mining …..... Der Versuch der Mustererkennung in Datenbeständen anhand statistisch-mathematischer Verfahren.

Datenbank …..... Applikation oder ein System zur systematischen Speicherung großer Datenmengen.

Endsysteme …..... In einem Firmennetzwerk gibt es in der Regel verschiedene Systeme:

- Zentrale Systeme zur Speicherung und Verarbeitung der Serverdaten (Backend-Systeme, typisches Beispiel sind Datenbanken)
- Zentrale Systeme zur Anbindung für die Anwender (Frontend-Systeme, beispielsweise Webserver)
- Systeme der Mitarbeiter (Endsysteme, meist Schreibtischrechner, Notebooks oder Terminals)

Fileserver …..... Zentraler Computer zur Speicherung von Dateien

Frontend …..... Schnittstelle bzw. Systeme, die der Anwender sieht und mit denen er arbeitet. Diese Systeme greifen teilweise auf sogenannte Backend-Systeme zurück, die z.B. die eigentlichen Daten speichern, aber für den Anwender nicht sichtbar sind.

Härtung …..... Vorgang der Absicherung eines IT-Systems gegen Angriffe.

IT …..... Informationstechnologie. Umfasst die Branche der Computer und Technologie-Dienstleistungen.

Keylogger …..... Programm oder Gerät, mit dem man Tastatureingaben mitprotokollieren, überwachen und rekonstruieren kann.

Pentest …..... Sicherheitsüberprüfung, bei der durch einen simulierten Angriff Schwachstellen im Netzwerk erkannt werden. Beim Offsite-Pentest wird das Netzwerk von außen z.B. über das Internet angegriffen. Beim Onsite-Pentest vor Ort von einem Anschluss innerhalb der Räumlichkeiten des Angegriffenen.

Phishing …..... Methode, bei der Personen dazu bewegt werden, arglos Passwörter oder andere Informationen preiszugeben. Dies geschieht durch eine gefälschte Webseite, die zur Eingabe von Benutzernamen und Passwörtern auffordert und diese für einen unberechtigten Dritten speichert.

PNR …..... Passenger Name Records, Fluggastdaten (Die USA fordern detaillierte Datensätze über alle einreisenden Personen).

Policy …..... Richtlinie, Handlungsvorschrift mit verbindlichem Charakter.

Provider …..... Anbieter, in der Regel für Internetzugänge, Webseiten, E-Mail oder Telekommunikationsdienste.

RFID …..... Radio-Frequency IDentification, Kontaktloses Verfahren zur Übertragung von Informationen über Funkwellen. Die Daten eines Speichers (Karte, Etikett) werden dabei durch die Funkwellen eines Lesers berührungslos ausgelesen. Je nach System und Sendestärke beträgt der Abstand vom Leser zum Datenspeicher wenige Millimeter bis zu mehreren Metern. Verwendet in Zugangssystemen, Etiketten, Ausweisdokumenten und anderen Systemen. RFID-Chips befinden sich unter anderem im neuen Personalausweis, den Reisepässen vieler europäischer Staaten und in den Preisetiketten einiger Warenhäuser.

Scoring …..... Risikoeinschätzung anhand von Datenbeständen in Kombination mit Erfahrungswerten. Ein bekanntes Beispiel ist die Einschätzung der Kreditwürdigkeit eines Menschen aufgrund seines Wohnumfelds.

Security Asessment ..Sicherheitsüberprüfung

SIS …..... Schengener Informationssystem, nicht-öffentliche Datenbank, in der Personen und Sachen eingetragen sind, die im Schengenraum zur Fahndung, mit einer Einreisesperre oder als vermisst ausgeschrieben sind.

Social Engineering .. Zwischenmenschliche Beeinflussungen von Personen mit dem Ziel, unberechtigt an Informationen, Daten oder Dinge zu gelangen. Ein klassisches Beispiel ist der Anruf bei einem Mitarbeiter, bei dem sich jemand als neuer Kollege ausgibt, der dringende Wartungsarbeiten durchführen muss und "mal eben" das Passwort braucht.

SQL-Injection …..... Angriff, bei der durch die Eingabe bestimmter „Befehlsfolgen“ in einem Eingabefeld (z.B. auf einer Webseite) ein direkter Zugriff auf die Datenbank im Hintergrund erlangt werden kann.

Switch …..... Netzwerkverteiler

Trojaner …..... Programm, das unter Vorwand oder in einem anderen Programm versteckt an einen Computernutzer weitergegeben wird, um Kontrolle über das System auszuüben.

VLAN …..... Virtual Local Area Network, Technologie zur virtuellen Unterteilung von physikalischen Netzwerken in mehrere separate Netzwerke oder Sicherheitszonen.

Vorratsdaten- …..... Verdachtsunabhängige Speicherung aller
speicherung Verbindungsdaten für Telefon und Internet.

Whistleblowing …... Brisante Enthüllungen, die von einer Person aus selbstlosen Motiven an die Öffentlichkeit gebracht werden. Oftmals riskiert der Whistleblower dabei seine berufliche Existenz, mitunter sogar sein Leben. Plattformen wie Wikileaks wurden geschaffen, um dem Whistleblower die Möglichkeit zu geben, anonym zu veröffentlichen.

WLAN …..... Wireless Local Area Network, drahtlose Technologie zur Anbindung von Computern (insbesondere Notebooks) zur Verbindung mit dem Heimnetzwerk, Firmennetzwerk oder Internet.

Zensus …..... Volkszählung

7. Impressum

Herausgeber:

Arbeitskreis Vorratsdatenspeicherung, Deutschland
www.vorratsdatenspeicherung.de

Autoren:

Eine Menge netter Menschen aus dem „AK Vorrat“
Unter anderem: Pgamerx, JRS, Frank-DSR, Wurzellicht, Axel, Kasia, Roam, Vera, Freak, cwoehrl, Gero, Micha und noch einige weitere, namentlich ungenannte.

Idee und ViSdP:

Michael Ebeling, Kochstraße 6, 30451 Hannover
micha_ebeling@mail36.net

Arbeitskreis Vorratsdatenspeicherung
www.vorratsdatenspeicherung.de