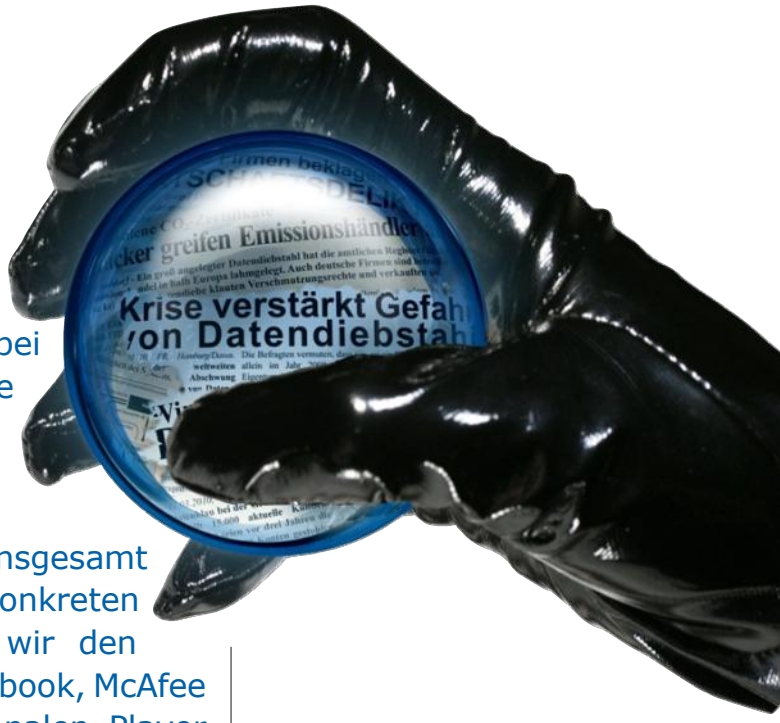
itWatch - Whitepaper

SNOWDEN, PATRIOT ACT, TEMPORA UND DIE ARGUMENTE, DIE NOCH FEHLEN



Die aktuelle Diskussion konzentriert sich vor allem auf drei Themen: Datenschutzaspekte bei Facebook, Google und Konsorten; die moralische Entrüstung, wenn sich Freunde ausspähen, und die Frage wer wann was gewusst hat. Viele der Kernfragen werden noch sehr undifferenziert diskutiert und insgesamt sehen bisher wenige Teilnehmer die konkreten Lösungen. In diesem Whitepaper wollen wir den Unterschied aufzeigen zwischen Google, Facebook, McAfee etc., den Blick für die Aufgaben der nationalen Player schärfen und die möglichen konkreten Handlungsfelder aufzeigen.

In den Diskussionen rund um die Enthüllungen von Edward Snowden wurden zunächst Spähprogramme und Vorratsdatenspeicherung durch die NSA und später auch des britischen Geheimdienstes thematisiert. Dabei lag der Fokus auf der organisierten und umfassenden Überwachung von Verbindungsdaten innerhalb und zu den USA (über Glasfaserkabel).

Die Rede war von „millionenfachem Abgreifen von Kommunikationsdaten deutscher Bürger durch die NSA und den Briten-Dienst GCHQ" (Spiegel Online[1]) – ein an sich pikantes aber keineswegs verwunderliches Thema. Der Auftrag der Nachrichtendienste liegt schließlich genau in diesen Tätigkeiten.

Dass eine unverschlüsselte E-Mail oder allgemeiner unverschlüsselter Datenverkehr über das Internet auch für Nicht-Profis relativ einfach abzuhören ist, ist überall bekannt. Wichtig ist es aber – egal ob man akzeptiert dass die Nachrichtendienste der Welt Daten abhören und sammeln – den konkreten Auftrag der nationalen Nachrichtendienste zu verstehen. Bei einer solchen Datensammlung sind nicht nur die Datenschutzrechte beeinträchtigt, viel wesentlicher ist, dass dieser Datenabfluss auch durch wirtschaftliche Interessen motiviert ist. Der Tagesspiegel[2] erläutert es sei lange bekannt, dass Ziel der US-Geheimdienste in Deutschland nicht nur die Terrorabwehr ist. Von versuchter Wirtschaftsspionage wird berichtet:

» *Dass US-Geheimdienste in Deutschland auch Wirtschaftsspionage betreiben, ist ebenfalls bekannt. In den 1990er Jahren sei ein CIA-Mann aufgefallen, der offenbar einen Mitarbeiter des Bundeswirtschaftsministeriums abschöpfen wollte. Das sei unterbunden worden, der CIA-Mann habe im Rahmen einer „stillen Lösung" die Bundesrepublik verlassen müssen, sagten Experten. Einige sprachen sogar von mehreren CIA-Leuten, die wegen mutmaßlicher Wirtschaftsspionage aus Deutschland hinauskomplimentiert worden seien….* «

Referenzen:

[1] Spiegel Online: US-Datenskandal - Amerikas millionenfacher Rechtsbruch, URL: http://www.spiegel.de/politik/deutschland/analyse-von-thomas-darnstaedt-wie-kriminell-ist-die-nsa-a-909013.html (Stand: 04.07.2013)

[2] Tagesspiegel: Bekannte Unbekannte, URL: http://www.tagesspiegel.de/politik/nsa-abhoeraffaere-bekannte-unbekannte/8466926.html (Stand: 16.07.2013)

Die Bedrohung für die Wirtschaft, die sich bis dato entlang der Berichte des Bundesamtes für Verfassungsschutz hauptsächlich von den Diensten aus China und Russland ausgespäht sah, wird angesichts der immer neuen Enthüllungen über den Auftrag der US- und UK-Dienste immer deutlicher.

Nicht nur die USA mit Patriot Act und Prism erweisen sich als interessierte Mithörer im Dienste der nationalen Wirtschaft, sondern beispielsweise auch die Briten mit dem Spähprogramm Tempora.

In der Zeit online[3] schreibt Patrick Beuth, dass einer der Gründe für den Einsatz von Tempora «enonomic well-being», das wirtschaftliche Wohlergehen, sei.

» *Die Formulierung «economic well-being» steht auch im Abschnitt 1 des Intelligence Service Act von 1994, dem britischen Gesetz, in dem die Aufgaben der Geheimdienste beschrieben werden.* «

Die Auswertung der gesammelten Daten zum Wohle der Nation stellt das potentiell viel größere Problem dar. Wichtig ist zu verstehen, dass solch wirtschaftliche Verquickung mit den gesammelten Daten der Dienste in Deutschland NICHT auf der Agenda der Dienste steht. Des Pudels Kern ist nicht das Sammeln der Daten, das jeder Dienst jedes Landes im Auftrag hat, sondern ob die gesammelten Daten zu wirtschaftlichen Zwecken eingesetzt werden, also zur Stärkung der eigenen nationalen Wirtschaft und damit billigend in Kauf genommen das Schwächen oder Vernichten ausländischer Unternehmen. Darin unterscheiden sich die handelnden Nationen ganz deutlich. USA und Großbritannien nutzen die Daten zur Stärkung der eigenen Wirtschaft.

Die Affäre spitzte sich zu, als zu den unverschlüsselten Daten, die an Netzknoten abgehört wurden, auch die durch den Patriot Act juristisch abgesicherte Möglichkeit des Zugriffs auf Daten von US-basierten Firmen – und natürlich deren ausländischen Niederlassungen – kam.

Auch das war für Kenner keine Verblüffung, denn viele hatten bereits frühzeitig darauf hingewiesen, dass durch den Patriot Act alle US-basierten Unternehmen und deren Auslandsniederlassungen verpflichtet sind, alle ihnen bekannten Daten an den US-Nachrichtendienst herauszugeben – ohne die Betroffenen oder die Dateneigner zu informieren.

Prof. Hornung[4] von der Universität Passau gab diesen Stand der Erkenntnisse z.B. auf dem Future Security Forum[5] der Fraunhofer am 04.09.2012 wieder. Man kann diese Datenweitergabe quasi als juristische Hintertüre ansehen, die genutzt werden kann, ohne dass Hintertüren in Software enthalten sind.

Peter Schaar[6], der Bundesdatenschutzbeauftragte, forderte im Interview mit dem Handelsblatt ein stärkeres Bewusstsein für die bestehenden Gefahren und entsprechende Handlungskonsequenzen:

» *Jede Firma hat es ein Stück weit selbst in der Hand, wer auf Daten zugreifen kann. Wer etwa Cloud-Diensten Informationen anvertraut, sollte wissen, wo die Daten gespeichert werden und an welche Rechtssprecher sich der Anbieter gebunden fühlt. Klar ist: Amerikanische Anbieter erlauben US-Behörden den Zugriff auf Daten sogar, wenn diese in Europa gespeichert werden.* «

Lassen Sie uns nun einen Blick darauf werfen, welche Daten dann weiter gegeben werden können. Klar ist, dass Facebook, Google, Amazon und andere Internetriesen sehr viele personenbezogene Daten besitzen und diese auch bereitwillig hergeben. Bereits der Fall einer Studentin, die als Touristin in die USA einreisen wollte und zurückgewiesen wurde, weil

Referenzen:

[3] Zeit online: Prism und Tempora - Massenhaftes Abhören soll der Wirtschaft dienen, URL: http://www.zeit.de/digital/datenschutz/2013-06/wirtschaftsspionage-prism-tempora (Stand: 16.07.2013)

[4] Prof. Dr. Gerrit Hornung, LL.M. (European Law), Lehrstuhl für Öffentliches Recht, Informationstechnologierecht und Rechtsinformatik,URL: http://www.jura.uni-passau.de/hornung.html (Stand: 12.07.2013)

[5] Konferenz Future Security 2012, URL:http://www.futuresecurity.fkie.fraunhofer.de/ (Stand: 16.07.2013)

[6] Schaar, Peter: Europäer sind ungeschützt – Der Bundesdatenschutzbeauftragte zum US-Datenskandal, In: Handelsblatt, 11.06.2013

Folgende Seite:

[7] Netzpolitik.org: USA - Beamte lesen Facebook-Nachrichten von Einreisenden, URL: https://netzpolitik.org/2013/usa-beamte-konnen-facebook-nachrichten-von-einreisenden-lesen/ (Stand: 16.07.2013)

[8] Süddeutsche.de: Tausende US-Firmen sollen Geheimdiensten helfen; URL: http://www.sueddeutsche.de/digital/skandal-um-weltweite-ueberwachung-tausende-us-firmen-sollen-geheimdiensten-helfen-1.1697261 (Stand: 12.07.2013)

[9] Focus Online, URL: http://www.focus.de/digital/internet/tid-31904/weltweite-datenspionage-durch-prism-so-schuetzen-sie-ihre-daten-vor-den-us-spionen-der-nsa_aid_1018356.html (Stand: 12.07.2013)

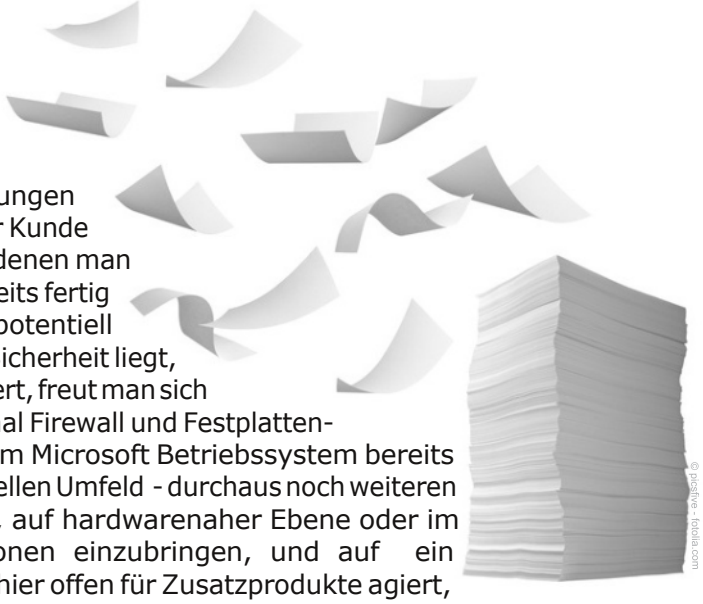
sie vorab in den sozialen Medien kommuniziert hatte, dass sie illegal als Au-Pair arbeiten möchte (siehe Netzpolitik.org[7]), zeigt, dass nicht nur die Nachrichtendienste Nutzen aus den Daten der sozialen Medien ziehen.

Neben diesen Unternehmen wurden z.B. Microsoft und McAfee (siehe Süddeutsche.de[8]) als Datenlieferanten der NSA genannt.
Aus Sicht der IT-Sicherheit fehlt deshalb gerade hier die Granularität in der Betrachtung und auch die Frage nach der Verantwortung, denn der Vergleich zwischen den unterschiedlichen „Datenschleudern" wie Facebook, Google, Microsoft oder McAfee ist nicht zulässig:

1. Im Fall von Facebook und Google…

… ist es meist ein Bürger, der seine Daten freiwillig und im Klartext unter möglicherweise nach deutschem Datenschutzgesetz fragwürdigen AGBs an eine Organisation übergibt. Zum großen Teil sind die angebotenen Services ohne Bezahlung - also kostenfrei für den privaten Nutzer – und finanzieren sich über Werbung und die Weitergabe der Daten. In Deutschland ist es trotz guten Datenschutzgesetzen bekannt, dass der Konsument gegen ein Versprechen von Gewinnchancen, Prämien oder Boni meist vollständig auf seine Datenschutzrechte verzichtet. Payback ist ein Standardbeispiel dafür. Die Lösung in diesem Fall liegt in der Sensibilisierung der Bürger und dem Aufzeigen von sicheren Handlungsweisen, die trotzdem den gewünschten Effekt möglichst genau erbringen (siehe beispielsweise Focus Online[9]).

2. Wie sieht es nun bei den in diesem Zusammenhang auch häufig genannten Firmen Apple oder Microsoft aus?



Deren Betriebssystem, Produkte und weiteren Lösungen werden nicht kostenfrei zur Nutzung angeboten. Der Kunde gibt hier sein Geld weitgehend für Themen aus, bei denen man sich zwar sehr freuen würde, wenn IT-Sicherheit bereits fertig eingebaut wäre, sich aber darüber klar ist, dass es potentiell Zusatzlösungen benötigt, da der Fokus nicht auf IT-Sicherheit liegt, sondern auf Stabilität, Komfort etc. Etwas lax formuliert, freut man sich also, dass die Mainstream-Themen Antivirus, Personal Firewall und Festplattenverschlüsselung quasi als kostenfreie Mehrwerte im Microsoft Betriebssystem bereits besetzt sind, sieht aber – insbesondere im professionellen Umfeld - durchaus noch weiteren Bedarf. Klar ist auch, dass Apple es nicht zulässt, auf hardwarenaher Ebene oder im Betriebssystemkern wirkliche Sicherheitsfunktionen einzubringen, und auf ein abgeschlossenes System setzt, während Microsoft hier offen für Zusatzprodukte agiert, diese auf jeder Ebene integrieren lässt und so dem Kunden einen echten, zusätzlichen Schutz ermöglicht.

3. Völlig anders ist die Situation bei IT-Sicherheitsprodukten.

Der Kunde kauft diese Produkte extra in der Absicht, die Schwachstellen in seinen IT-Systemen – auch Schwachstellen in Microsoft Betriebssystemen - zu schließen. Insbesondere bei DLP- und Labelling-Lösungen wird klar, dass der Kunde dem Produkt, welches er erworben hat, explizit alle vertraulichen Daten bekannt gibt und den Schutz dieser erwartet. Gerade wenn nun durch das Produkt kryptographischer Schutz angeboten wird, versteht man, dass es einfacher ist durch die Herausgabe der Schlüssel Zugriff auf die Daten zu bekommen anstatt einfach sämtliche Daten herausgeben zu lassen. Der Kunde investiert in der Absicht, dass kein unbefugter Dritter Zugriff auf von ihm als schützenswert erachtete Daten erhält. Bei einer solchen Betrachtung kann der Sachverhalt möglicherweise eher für eine Rückabwicklung oder Ablöse motivieren als zur Verlängerung der Wartungsverträge. Bevor man aber vorschnell handelt, sollte man sich seine Daten und die Situation in der internationalen Wirtschaft genauer betrachten. Die Historie zeigt, dass Intel zuerst die kryptographischen Beschleuniger auf die Chipsätze gebaut hat und dann McAfee gekauft hat, die kurz vorher mit SafeBoot einen Festplattenverschlüsseler gekauft hatten, der diese kryptographischen Module von Intel konstruktiv nutzen konnte.

Der dritte Punkt ist für Konzerne, deren zentrale, weil lebenswichtige Motivation der Schutz ihres intellektuellen Eigentums ist, besonders relevant – und seit längerem bekannt. So berichtete beispielsweise Günter Butschek, Produktionsvorstand bei der EADS-Tochter Airbus der Welt am Sonntag[10] , dass die IT-Sicherheit integraler Bestandteil ist:

» *Die Abwehr von Wirtschaftsspionage ist ein großes Thema für den deutsch-französischen EADS-Konzern. […]: «Wir sind ein begehrtes Ziel.» Das EADS-Management beschäftige sich nicht erst seit dem US-Abhörskandal mit dem Thema. «Praktisch jedes zweite Meeting des Gesamtvorstands beschäftigt sich mit dem Thema IT-Sicherheit», erklärte Butschek.* «

An Airbus wird die Situation besonders deutlich, da der Hauptwettbewerb in den USA sitzt und es viele direkte Wettbewerbssituationen gerade auch im amerikanischen und europäischen Markt – jeweils für einen der Player ein „Heimatmarkt" – gibt.

Referenzen:

[10] Welt online: Abwehr von Wirtschaftsspionage großes Thema für EADS, URL: http://www.welt.de/newsticker/dpa_nt/infoline_nt/wirtschaft_nt/article117806299/Abwehr-von-Wirtschaftsspionage-grosses-Thema-fuer-EADS.html (Stand: 12.07.2013)

[11] vgl. Weichert, Thilo: Prism, Tempora, Snowden: Analysen und Perspektiven; URL: http://www.vocer.org/de/artikel/do/detail/id/496/prism-tempora-snowden-analysen-und-perspektiven.html (Stand: 12.07.2013)

[12] ebd.

[13] golem.de; URL: http://www.golem.de/news/prism-skandal-furcht-vor-hintertueren-in-us-software-und-hardware-1306-100012.html (Stand: 04.07.2013)

Was sind nun die Handlungsoptionen für die einzelnen Player in Deutschland und Europa?

Datenschützer und IT-Sicherheitsexperten wissen seit Jahren, dass die technischen Möglichkeiten der Datenermittlung, -speicherung und –auswertung ausgenutzt werden – mit welchen Zielen auch immer – insbesondere wenn kein unabhängiges Kontrollorgan den Einsatz dieser Möglichkeiten reglementiert[11]. Weil es keine Kontrollorgane mit Zuständigkeit für das weltweite Internet gibt und die in der Grau- oder illegalen Zone Handelnden immer wieder ein Land finden werden, in welchem die Rechtsverfolgung für ihre Straftaten im Internet de facto nicht stattfindet, kann man in diesem Sinne durchaus verstehen, dass Frau Bundeskanzlerin Merkel das Internet als Neuland bezeichnet. Es ist zweifelhaft, ob das weitere Forcieren von nationalen Gesetzen ohne eine weltweit stabile Rechtsverfolgung und weitere Schritte als begleitende Maßnahmen zielführend ist, oder ob sich das weitere Forcieren der nationalen Gesetze nicht sogar durch die strikteren Auflagen ungewollt gegen die heimische Wirtschaft richtet.

Die Alternativen sieht Dr.Thilo Weichert, Verfasser des Artikels „Prism, Tempora, Snowden: Analysen und Perspektiven"[12] in erhöhter Wachsamkeit:

» *Die selbstverständlichste Reaktion Europas sollte es sein, die US-amerikanischen Datensauger à la Google, Facebook, Apple, Amazon u. a. zumindest soweit zur Beachtung des europäischen Rechts zu zwingen, wie diese in Europa aktiv sind. Hierzu können die Verbraucherinnen und Verbraucher einen wichtigen Beitrag leisten. Das ist zudem eine kollektive Aufgabe der europäischen Datenschutzaufsichtsbehörden. Dies kann durch eine von der US-Lobby unbeeinflusste Verabschiedung einer grundrechtsfreundlichen Europäischen Datenschutzgrundverordnung forciert werden….* «

Der Bundesverband IT-Mittelstand (BITMi) hat eine explizite Warnung in diese Richtung ausgesprochen (golem.de[13]):

» *Der Bundesverband IT-Mittelstand (BITMi) warnt nach Prism und Tempora vor Informationstechnologie aus den USA. «Deutschland ist besonders anfällig für solche Spionageaktionen. Unsere Wirtschaft ist sehr stark von ausländischen Technologien abhängig und wir wissen nicht, ob und welche Hintertüren noch in häufig benutzten Soft- und Hardwareprodukten eingebaut sind», sagte Michaela Merz, IT-Sicherheitsexpertin des Verbandes.* «

Diese Position wird auch von deutschen Politikern unterstrichen. Der sächsische Ministerpräsident Stanislaw Tillich beispielsweise fordert im Handelsblatt vom 09.07.2013:

» *Wir müssen es schaffen, dass Europa seinen Bedarf an Soft- und Hardware aus eigener Kraft, mit eigener Technologie und eigenen Produkten deckt.*«

Dies sei unerlässlich, um Privatpersonen, Geschäftsleute und Amtsträger besser vor dem Ausspähen ihrer Daten zu schützen. Tillich hebt dabei nicht nur das Recht auf informationelle Selbstbestimmung hervor, sondern untermauert auch die Notwendigkeit einer staatlichen Unterstützung beim Aufbau eines eigenen Industriezweiges:

» *Die außeruniversitäre Forschungslandschaft, die Universitäten und die Vielzahl kreativer KMU am Standort Dresden oder München wie die kreative IT-Szene wie in Berlin geben diesen Bemühen eine stabile Basis.[…] Voraussetzung ist, dass wir*

Europäer dies wollen – und fördern. Unser Ziel muss es sein, die gesamte Wertschöpfungskette, einschließlich Produktion, in Europa abzubilden.«

Schauen wir uns den Bedarf der einzelnen Organisationen an. Jedes Unternehmen, welches seine eigenen Produkte erstellt und vertreibt ohne Daten und Geschäftsgeheimnisse von Dritten zu verwalten, kann für sich entscheiden, wie es um die IT-Sicherheit steht, weil durch das Handeln keine Dritten gefährdet sind.

In einem Verbund von mehreren Unternehmen und in den Datenschutz- und Datensicherheitsvereinbarungen zwischen Unternehmen und Organisationen sollte man in die Betrachtung der Mechanismusstärke des Schutzes spätestens nach Auswertung der Snowden-Enthüllungen diese Aspekte mit in die Metrik einbeziehen.

Besonders kritisch ist die Verwaltung von wirtschaftlich wesentlichen Daten durch Dritte zu sehen – den Behörden kommt dabei eine besondere Schutzaufgabe zu - insbesondere, wenn sie die Daten hoheitlich verwalten oder sogar entlang ihrer gesetzlichen Zuständigkeit erheben. Nehmen wir hier als Beispiel den Patentstreit zwischen Apple und Samsung. Was wäre, wenn die beteiligten Anwaltskanzleien und die Gerichte über Hintertüren in der Sicherheitssoftware indirekt dem Verfahrensgegner Zugriff auf die Details geben würden?
Weitergedacht erscheint es eine valide Forderung der Unternehmen zu sein, ihre Daten, Strategien etc. im gesamten Verfahren über Anwaltskanzleien bis hin zum Richter geeignet zu schützen. Als Konsequenz sollten Außenprüfer der Finanzämter, die innere Sicherheit und deren Ermittler, Justiz- und Innenministerin von Bund und Ländern und viele weitere öffentliche Auftraggeber ihre IT-Security möglichst kurzfristig national besetzen.

Nachdem die Erkenntnisse rund um die Enthüllungen von Snowden leider meistens kein zusätzliches Budget frei geben, hat die itWatch, als nationaler Anbieter von innovativer IT-Sicherheit „made in Germany" aus diesem aktuellen Anlass eine Kampagne „Abwrackprämie für Datenschleudern" gestartet, mit der sie interessierten Anwendern den Umstieg auf eine garantiert hintertürfreie Lösung leicht macht.

itWatch steht für innovative IT-Sicherheit „made in Germany"

itWatch steht für innovative Softwareprodukte mit dem Fokus auf dem Schutz vor Datenklau - Data Loss Prevention (DLP), Endgeräte Sicherheit (Endpoint Security), Verschlüsselung, kostensenkende Mehrwerte im Betrieb und die einfache Nutzung von Sicherheitslösungen durch Anwender.

Bei der Entwicklung der Produkte steht die Kosteneffizienz für den Kunden im Vordergrund. Die Produkte der itWatch unterstützen immer die bereits etablierten Kundenprozesse - eine Veränderung der Prozesse ist deshalb nicht nötig.

Alle Produkte werden mehrsprachig angeboten und ohne Zukauf im Haus der itWatch in Deutschland frei von Hintertüren hergestellt und weltweit über Partner angeboten.

Möchten Sie Ihr bisheriges ausländisches System in den Ruhestand schicken und abwracken und haben Interesse an der „Abwrackprämie für Datenschleudern" der itWatch GmbH?

Gerne stehen wir Ihnen unter AWP@itwatch.de für alle Ihre Fragen zur Verfügung.