Robert Luh

Sichere Internet-Identität in der e-Society

101- Complexity in Business: Insights and Solutions

Abstract

Der Austausch von sensiblen Informationen über das Internet ist ein unverzichtbarer Teil der modernen Gesellschaft wie auch der Geschäftswelt. Dabei stellt die Gewährleistung der Echtheit der Identität des Gegenübers nach wie vor eine Herausforderung dar – viele Kommunikationskanäle bieten Einfallstore für Identitätsdiebstahl oder sehen sich mit steigender Cyber-Kriminalität konfrontiert.
In diesem Dokument wird eine konzeptuelle Lösung vorgestellt, die sich mit der Implementierung eines internetweiten Identitätsmanagementsystems sowie dem Design eines zonenbasierten Wide-Area Netzwerks befasst, welches auf Software- und Identitäts-Trusts basiert. Die dem Konzept zugrundeliegende digitale ID erfüllt zwei essentielle Anforderungen: Einerseits erlaubt sie NetzteilnehmerInnen, die Identität bzw. Rechte eines Kommunikationspartners/einer Kommunikationspertnerin eindeutig zu ermitteln und so die Sicherheit des Systems maßgeblich zu erhöhen, auf der anderen Seite bietet sie mit „ID-Attribut-Entkoppelung“ einen Mechanismus, der die Privatsphäre der NutzerInnen aktiv schützt und verhindert, dass mehr personenbezogene Daten ausgetauscht werden als für eine Transaktion tatsächlich notwendig ist.

Keywords:

Identity Management; Kommunikation; Privatsphäre; Sicherheit

1. Einleitung

Die zunehmende Internet-Penetration hat in den letzten Jahren auch zu einem drastischen Anstieg der Cyber-Kriminalität geführt. Das organisierte Verbrechen nutzt das Internet bereits seit Jahren als Absatzkanal und Angriffsvektor, und auch Konzerne bzw. Nationen unterhalten großflächige Spionageprogramme. IT-Systeme und die darauf gespeicherten Daten stellen heutzutage die größten Werte und profitabelsten Ziele dar.

Eine Studie der Vereinten Nationen (Malby et al. 2013) identifiziert drei grundlegende Arten von IT-bezogenen Verbrechen: Angriffe auf die Geheimhaltung, Integrität oder Verfügbarkeit eines Systems, Angriffe auf die Persönlichkeitsrechte bzw. illegale Profitgenerierung sowie die Verbreitung illegaler Inhalte. Mit dem Aufkommen des Internets der Dinge (Heer et al. 2011) und der Zunahme der Interkonnektivität von Systemen und Geräten stieg insbesondere die Gefahr durch Angriffe auf die kritische Infrastruktur. Derartige Attacken auf z.B. Systeme eines nationalen Energielieferanten (zunehmend vernetzt dank Initiativen wie dem kommenden europaweiten ‚Smart Grid‘ (McLaughlin et al. 2010)) hätten das Potential, ein ganzes Land innerhalb weniger Tage ins Chaos zu stürzen (Deutscher Bundestag 2011).

Angesichts derartiger Bedrohungen drängt sich die Notwendigkeit auf, grundlegende legislative und technische Veränderungen an der Funktionsweise der heutigen Internet-Kommunikation anzustoßen. Gerade die Anonymität des weltweiten Netzes birgt zahlreiche Gefahren und ermöglicht es technisch versierten Kriminellen, über lange Zeit hinweg unentdeckt zu bleiben. Um dem entgegenzuwirken, müsste es zu einer Annäherung an existierende Identitätssysteme der physischen Welt (Reisepass, Führerschein) kommen, die es erlauben, sein Gegenüber eindeutig zu identifizieren.

In diesem Trend verbirgt sich jedoch ein Dilemma, das gerade in letzter Zeit an gesellschaftlicher Bedeutung gewonnen hat: Steht die Sicherheit von Systemen wie der kritischen Infrastruktur vor dem Recht auf Privatsphäre des Einzelnen oder sollte die „nationale Sicherheit“ kompromisslos vorangereiht werden?

Das in diesem Dokument vorgestellte Konzept soll zeigen, dass die Antwort auf diese Frage nicht zwangsläufig binär sein muss. Sollen großflächig akzeptierte Maßnahmen zu einer tatsächlichen Erhöhung der Sicherheit im Internet umgesetzt werden, dürfen fundamentale Privatheit-Prinzipien keinesfalls umgestoßen werden. Nachfolgend wird ein breites Systemkonzept skizziert, das je nach Anwendungsfall sowohl hohen Sicherheitsanforderungen im Umfeld heikler Systeme genügt als auch die Privatsphäre der Teilnehmer wahrt.

2. Hintergrund

2.1. Online-Identität

Bei einer Identität (ID) handelt es sich im Allgemeinen um einen Satz von Daten, der mit einer einzelnen Entität – etwa einer Person – assoziiert ist (Abelson et al. 1998). Eine Identität besteht aus einer Anzahl an Attributen, die neben den physischen Eigenschaften des Individuums auch die Herkunft, Gewohnheiten oder den Berufsstand beschreiben. In der digitalen Welt sind derartige Attribute meist synonym zu Konten (Accounts) und Rechten, die den Zugriff auf (Online-)Ressourcen steuern. Digitale IDs sind nicht zwangsläufig mit einer echten Person verknüpft; es gibt im Internet auch kein zuverlässiges System, das eine Person eindeutig identifizieren könnte.

Hier setzt das nachfolgend skizzierte Konzept an: Im Rahmen dieses Implementationsvorschlages eines Identitäts-Ökosystems (White House 2012) soll ein sicheres, ‚Echt-ID‘-gestütztes System aufgebaut werden, das etwa für Ende-zu-Ende Kommunikation von Personen und Geräten als auch zur Anmeldung an nationalen Bürgerdiensten genutzt werden kann.

2.2. Internet-Anonymität und Privatsphäre

Das Prinzip der ID-Attribut-Entkoppelung (Abelson et al. 1998) erhält dabei ein skalierbares Maß an Anonymität. Grundsätzlich beschreibt die Entkoppelung die Möglichkeit des Benutzers, gezielt nur die für eine bestimmte Transaktion minimal benötigten Attribute an das Zielsystem zu übermitteln. Je weniger Attribute dabei übertragen werden, desto höher bleibt der Grad der Anonymität und desto geringer das Missbrauchsrisiko. Abbildung 1 zeigt die verschiedenen Stärken von Attributen bei der Entkoppelung.

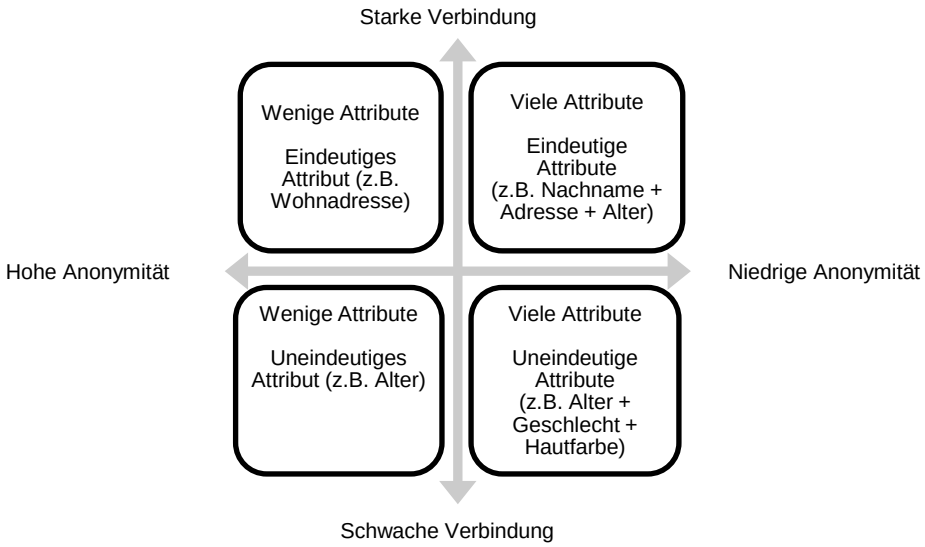


Abbildung 1: ID-Attribut-Entkopplung

Als Beispiel für mangelhafte Entkoppelung sei der Besuch eines Ab-18 Films im Kino genannt: Aktuell wird in der physischen Domäne der Personalausweis kontrolliert, um festzustellen, ob der Kunde oder die Kundin berechtigt ist, die Vorstellung zu besuchen. Obwohl für eine erfolgreiche Überprüfung nur das schwache Attribut ‚Alter' vonnöten wäre, hat der Kontrolleur dabei auch Zugriff auf den Namen und eventuell sogar die Wohnadresse des Individuums.

Im Internet wäre die feingranulare Überprüfung der Identität noch besser realisierbar. Einzeln zertifizierte Attribute könnten übermittelt werden, ohne dabei mehr als notwendig über die Person zu verraten.

3. Federated Internet

Um ein System zu schaffen, das echte Identitäten auf nationaler Ebene integrieren kann, müssen mehrere bekannte Verfahren in den neuen Kontext transportiert werden. Die Kernideen umfassen Active Directory Federations (Microsoft 2007) für die Abbildung von Vertrauensbeziehungen zwischen Teilnehmern sowie den verstärkten Einsatz von Ende-zu-Ende Kommunikation. Schlüsselmanagement würde über Public Key Infrastrukturen (PKI) gesteuert werden. Gewissermaßen ließe sich von einem „Federated Internet" (Jennings 2009) sprechen; im Gegensatz zum heutigen Netz müsste dieses neue, freiwillig genutzte System jedoch nicht alle Dienste umfassen, sondern lediglich jene Anwendungen abdecken, die besonders hohe Sicherheitsanforderungen haben.

3.1. Betriebsmodi

Im Kontext des Gesamtsystems werden zwei grundlegende Betriebsmodi unterschieden. Zum einen gibt es die *kontextunabhängige Einzeltransaktion:* Hier werden entkoppelte ID-Attribute an ein bestimmtes Zielsystem übermittelt, um für die Dauer einer Sitzung Zugriff zu erlangen. Einzeltransaktionen ermöglichen das größte Maß an Kontrolle über die eigene ID und dienen etwa der Authentifizierung gegenüber einem Dienstanbieter oder der Absicherung einer einzelnen

Datenübertragung. So kann das Verfahren problemlos auch in die physische Welt transportiert werden.

Zonenweites Single-Sign-On (Z-SSO) beschreibt hingegen die einmalige Anmeldung an einem vernetzten System, welches die anerkannte ID wiederum an untergeordnete Dienste weitergibt. Dadurch entfällt die Notwendigkeit der erneuten Anmeldung an jedem Teilsystem; die übergeordnete ID ist für das gesamte Netzwerk gültig. In Zusammenhang mit dem Konzept beschreibt Z-SSO die Verwendung eines Hochsicherheits-Netzwerks, das Web-Dienste an ´echte IDs´ koppelt. Auf diese Weise können etwa Bürgerdienste betrieben oder Zugriff auf besonders heikle Systeme gesteuert werden. Im Gegensatz zur Einzeltransaktion spielt die Entkoppelung hier eine untergeordnete Rolle: Der Fokus liegt auf der Erhöhung der Sicherheit.

3.2. Identitätssystem

Beiden Betriebsmodi liegt ein Identitätssystem zugrunde, dessen Funktionsweise in Abb. 2 erläutert wird.

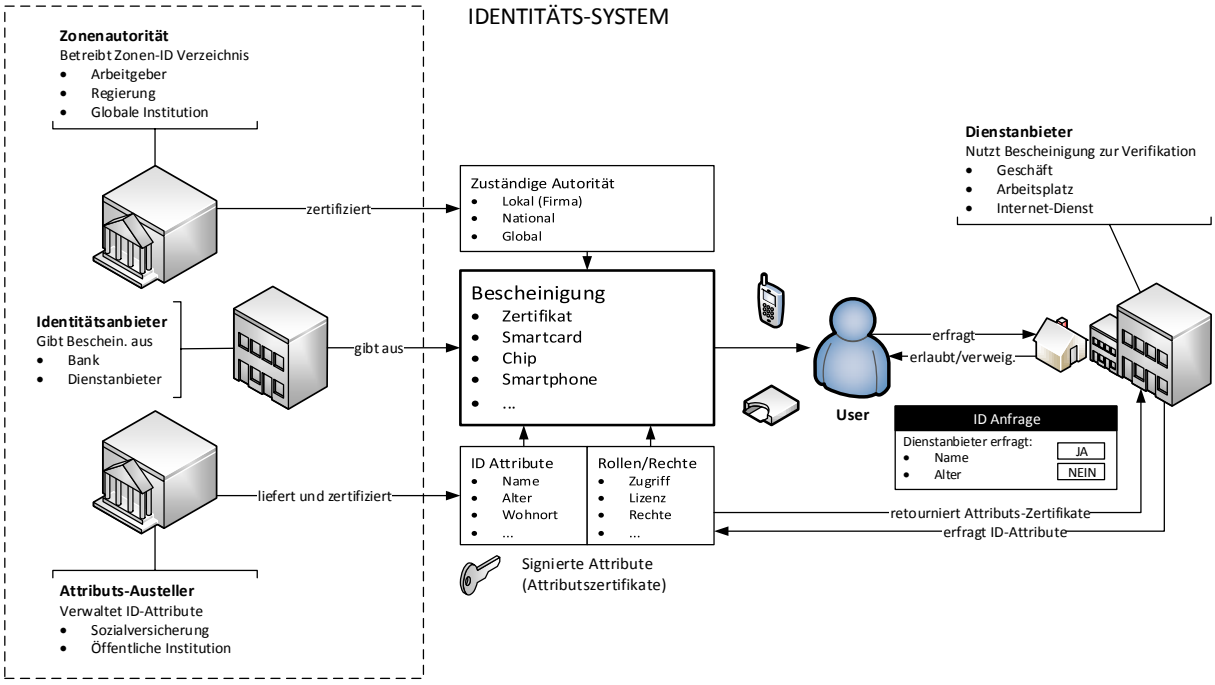


Abbildung 2: Identitätssystem

Das Identitätssystem setzt sich aus wenigsten 4 Typen von TeilnehmerInnen zusammen. Die *Zonenautorität* verwaltet die Identitäten in einem Sicherheitskontext. Sie ist gleichzeitig ein sogenannter Attributs-Aussteller, der in der Lage ist, bestimmte ID-Attribute einer Entität zu verifizieren.

Identitätsanbieter geben ID-Bescheinigungen an ein Individuum oder ein Gerät aus. Diese Bescheinigung kann die Form einer Smartcard, eines digitalen Zertifikats oder eines herkömmlichen Ausweises annehmen; der ID Provider ist üblicherweise der Dienstanbieter, der mit der Bescheinigung assoziiert ist.

Ein *Attributs-Austeller* ist eine Organisation die qualifiziert ist, bestimmte ID-Attribute zu verifizieren. Dies erfolgt in der Regel durch eine Verbindung in der physischen Domäne. Beispiele inkludieren eine Sozialversicherung, öffentliche Stellen oder den Arbeitgeber einer Person. Attributs-AustellerInnen können ebenso Identitätsanbieter und Zonenautoritäten sein.

Einer *Entität* (Benutzer, Gerät) wird eine ID ausgestellt, die sie bei der Anmeldung an einen Dienst innerhalb des Systems nutzen kann. Jede Entität verfügt über eine Zahl an Attributen, die von Attributs-AustellerInnen zur Verfügung gestellt und zertifiziert werden. Der Benutzer oder die Benutzerin übermittelt diese Attributszertifikate bei der Authentifizierung (unter Berücksichtigung des Prinzips der Entkoppelung).

DienstanbieterInnen sind TeilnehmerInnen am System, die einen bestimmten Dienst zur Verfügung stellen. Diese Parteien könnten Geschäfte (die etwa eine Altersverifikation erfragen), ArbeitgeberInnen (die Zugriffsrechte überprüfen) oder ein Internet-Dienst (der z.B. den Wohnort abruft) sein. Ein/e DienstanbieterIn erfragt eine Kombination aus Attributen, die von Attributs-AusstellerInnen zertifiziert sind. Wenn die Entität mit der Auswahl an Attributen einverstanden ist (Bestätigung über eine Anfrage auf z.B. dem Smartphone), kommt die Transaktion zustande.

Abbildung 3 zeigt den Prozess einer **ID-Ausstellung:** Als Bescheinigung kommt eine Smartcard zum Einsatz, die vom/von der ArbeitgeberIn ausgestellt und verifiziert wird.

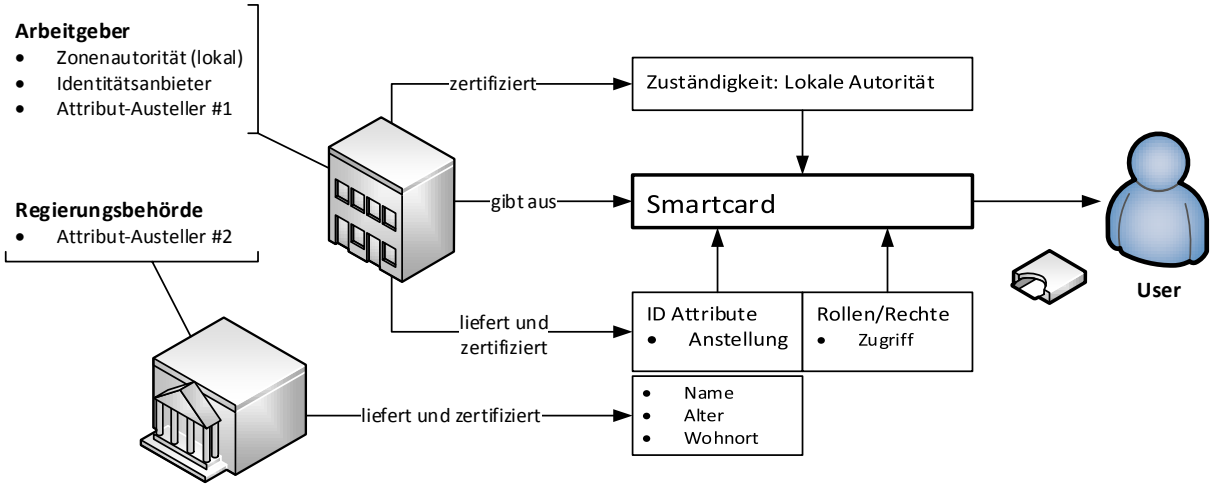


Abbildung 3: Ausgabe einer ID-Bescheinigung

Der Anhang zeigt das auf SSO basierende **Gesamtsystem** und erläutert beispielhafte Workflows. Die Sicherheit in diesem konzeptionellen Gesamtsystem wird durch folgende Ecksteine geschaffen:

- *Nichtabstreitbarkeit durch „Real-ID“* – Der Zugriff auf heikle Systeme ist nur nach Übermittlung einer Menge erforderlicher Attribute in Zusammenspiel mit z.B. biometrischen Daten möglich.
- *Isolierte und zertifizierte Softwareumgebung* – Der Rechner des Benutzers oder der Benutzerin muss den Richtlinien der aktuellen Zone (Sicherheitskontext, in dem der User oder die Userin tätig ist) entsprechen.

- *Gestufte Vertrauens-Zonen* – Eine Vielzahl an Sicherheitskontexten (Zonen; s.u.) erlaubt das selektive Etablieren von Vertrauensstellungen (Trusts) zwischen Individuen, Firmen oder gar Ländern. Trusts werden entweder vererbt oder über Whitelists manuell definiert.
- *Ende-zu-Ende Kommunikation* – Lokale Zonen und einzelne Knoten kommunizieren stets durch einen Tunnel – dies erlaubt zwei Parteien die sichere Kommunikation, selbst wenn die übergeordnete Zone (etwa die des Landes) keine Vertrauensbeziehung etabliert hat.

3.2.1. Vertrauensstellungen

Das Prinzip des Vertrauens (Trust) ist ein zentraler Bestandteil des Konzepts. Trusts definieren, dass ein/e TeilnehmerIn den Identitäten, Softwarezertifizierungen und/oder Datenbeständen einer/s anderen TeilnehmerIn/s vertraut. So muss die eigene Softwareumgebung den jeweiligen Sicherheitsvorgaben der Zone (siehe unten) entsprechen. Trusts müssen nicht alle diese Aspekte umfassen und können auch einseitig definiert werden. Theoretisch ist jede Kombination möglich. Um die Sicherheit des Systems zu gewährleisten, sind jedoch nur bestimmte Beziehungen sinnvoll:

	Lokal: Privat	Lokal: LAN	Lokal: Gerät	National	Global
Lokal: Privat	✓ Private Ende-zu-Ende Kommunikation	- Per Definition nicht mit lokalem Netz verbunden	✓ Gerät, welches auf ein privates System zugreifen darf	✓ Notwendig, um nationale Dienste zu nutzen (Person)	✓ Notwendig, um nationale Dienste zu nutzen (Person)
Lokal: LAN	✕ Lokaler Betreiber wird Privatperson selten vertrauen	✓ Firmen-Föderation	✓ Beschaffte oder produzierte Geräte	✓ Notwendig, um nationale Dienste zu nutzen (Firma)	✓ Notwendig, um globale Dienste zu nutzen (Firma)
Lokal: Gerät	✓ PC des Geräte-Besitzers	✓ Hersteller oder Nutzer	✓ Gerät-zu-Gerät Kommunikation	✕ Nur spezielle Geräte	✕ Nur spezielle Geräte
National	✕	✕ Nur denkbar für Dienstanbieter oder Partner	✕ Nischenszenario	✓ Vertrauen zwischen Nationen; Union	✓ Global standardisierte Apps/IDs
Global	✕	✕	✕	✓ Nationale IDs	- Globale Zone ist einzigartig

3.2.2. Sicherheitszonen

Zonen beschreiben den Kontext der jeweiligen Autorität. *Lokale Zonen* sind Firmennetzwerke, private Computer/Netzwerke und Geräte. Lokale Anwendungen sind mit privaten oder innerbetrieblichen Umgebungen vergleichbar, die sich selbst regulieren. *Nationale Zonen* definieren den Sicherheitskontext eines ganzen Landes und sollen dementsprechend nur von den eigenen BürgerInnen verwendet werden können. Die Authentifizierung erfolgt in der Regel durch den Personalausweis sowie einen zweiten Faktor. EndbenutzerInnen und lokale Zonen können beschließen, bestimmten Zonen das Vertrauen auszusprechen bzw. es abzuerkennen. Eine *globale Zone* könnte wiederum mehrere Staaten umfassen und würde vorhandene oder neu gegründete Verwaltungsbehörden als Autorität definieren (vergleichbar mit Root DNS oder einem TLD-Verwalter). Das Funktionsprinzip wäre dabei identisch zur nationalen Zone. Eine global gültige ID müsste jedoch erst implementiert werden.

4. Risiken und Herausforderungen

Die Einführung eines derartigen Systems ist nicht ohne Gefahren. Vier Aspekte sind von besonderer Bedeutung:

Vertrauen – Besonders im Falle des SSO-Systems muss den verwaltenden Autoritäten nahezu uneingeschränkt vertraut werden. Egal ob es sich dabei um eine Behörde oder eine/n private/n DienstleisterIn handelt – es ist insgesamt nur schwer auszuschließen, dass die Organisation nicht Ziel eines (erfolgreichen) Angriffs werden könnte oder mit staatlich sanktionierten Spionageprogrammen kooperiert. Regelmäßige Überprüfung durch eine unabhängige Institution (etwa eine Akkreditierungsstelle, die nach dem Multistakeholder-Prinzip (Hemmati 2002) arbeitet) könnte dieses Risiko jedoch maßgeblich reduzieren.

Single Point of Failure (SPoF) – Jede Zonenautorität kann als SPoF gesehen werden. Selbst wenn jeder Server über Backups verfügt, kann ein Gesamtausfall das System zum Stillstand bringen. Dies ist vergleichbar mit dem Ausfall des Root DNS Systems oder eines wichtigen Domänencontrollers. Durch geografisch verteilte Hot-Standby Backups und unterschiedliche Serverkonfigurationen kann dieser Gefahr entgegengewirkt werden. Einzeltransaktionen wären zusätzlich durch das ID-Zertifikats-Caching geschützt und funktionieren konzeptuell auch ohne permanente Internetverbindung.

Politische Einheit – Die möglicherweise größte Herausforderung für die Umsetzung eines solchen Systems ist die mangelnde politische Einheit bei Themen der Internetregulierung. Sowohl die regierungsdominierte International Telecommunications Union (ITU) der Vereinten Nationen als auch die U.S.-zentrische Internet Corporation for Assigned Names and Numbers (ICANN) folgen teilweise unterschiedlichen Agenden und sind sich bei vielen Fragen uneins (Ermert 2008, Chetty 2012, Taylor 2012). Zusätzlich gibt es eine Vielzahl an Organisationen, die sich für die unterschiedlichen Aspekte der Internet-Entwicklung (Technologien, IP und TLD-Management, Standards …) zuständig sehen (ICANN 2013). Erst ein wirklich demokratisches MultistakeholderInnen-Modell mit Beteiligung von Regierungen, Firmen, NGOs und den Vereinten Nationen könnte hier Abhilfe schaffen.

Migration – Im Falle einer erfolgreichen Einführung des Konzepts müsste man beachten, dass es durch die Migration von Diensten in das neue Netz nicht zu einem Abfall der Sicherheit kommt. Im schlimmsten Fall würden die aktuellen Probleme „mitgenommen“ werden und es gäbe langfristig nur noch wenige Vorteile. Auch dürfte es niemals zu einem Zwang kommen, das System zu benutzen: Gerade das SSO-System darf zu keiner Zeit als Ersatz für das heutige Internet gesehen werden.

5. Fazit

Sowohl die Allgegenwärtigkeit des Internets als auch die Cyberkriminalität wird in den nächsten Jahren und Jahrzehnten weiter zunehmen. Unsere Abhängigkeit vom weltweiten Netz steigt und steigt – sei es in der Geschäftswelt, der kritischen Infrastruktur oder auf privater Ebene. Der Schutz dieser Systeme sowie der persönlichen Daten ist eine Herausforderung, der es sich baldigst zu stellen gilt.

Das hier vorgestellte Gesamtkonzept für ein sicheres Internet auf Basis eines globalen Identitätssystems soll aufzeigen, dass weitreichende Veränderungen möglich sind, ohne unsere

Privatsphäre zu gefährden. Auch große Änderungen am existierenden System wären nicht erforderlich, da die notwendigen Technologien bereits weitgehend existieren.

Der Vorschlag basiert darauf, dass unsere echte Identität früher oder später den Weg in die digitale Welt finden muss – ein Vorgang, über den im unabhängigen Umfeld nachgedacht werden sollte, bevor uns die Entscheidung von einseitig denkenden (staatlichen) Organisationen abgenommen wird, die der Privatsphäre in der E-Society nicht den hohen Stellenwert einräumen, den sie verdient.

Literaturliste/Quellenverzeichnis:

Malby, Steven/Mace, Robyn/Holterhof, A./Brown, C./Kascherus, S/Ignatuschtschenko, E. (2013): Comprehensive study on cybercrime. United Nations Office on Drugs and Crime.

Heer, Tobias/Garcia-Morchon, Oscar/Hummen, René/Keoh, Sye Loong/Kumar, Sandeep S./Wehrle, Klaus (2011): Security Challenges in the IP-based Internet of Things. Wireless Personal Communications 61, no. 3.

McLaughlin, Stephen/Podkuiko, Dmitry/Miadzvezhanka, Sergei/Delozier, Adam/McDaniel, Patrick (2010): Multi-vendor penetration testing in the advanced metering infrastructure. In: Proceedings of the 26th Annual Computer Security Applications Conference.

Deutscher Bundestag (2011): Gefährdung und Verletzbarkeit moderner Gesellschaften – am Beispiel eines großräumigen und langandauernden Ausfalls der Stromversorgung.

Abelson, Hal/Lessig, Lawrence/Covell, Paul/Gordon, Steve/Hochberger, Alex/Kovacs, James (1998): Digital identity in cyberspace. White paper. Law of Cyberspace: Social Protocols.

White House (2012): National Strategy for Trusted Identities in Cyberspace: Enhancing Online Choice, Efficiency, Security, and Privacy.

Microsoft (2007): Active Directory Federation Services Overview. http://technet.microsoft.com/en-us/library/cc772593(v=ws.10).aspx, (27.01.2016).

Jennings, Brendan/Brennan, Rob/Donnelly, William/Foley, Simon N./Lewis, Dave/Sullivan, Declan O./Strassner, John/Van der Meer, Sven (2009): Challenges for federated, autonomic network management in the Future Internet. In: IFIP/IEEE International Symposium on Integrated Network Management-Workshops (IM'09), 87-92.

Hemmati, Minu (2002): Multi-stakeholder processes for governance and sustainability: Beyond deadlock and conflict. Routledge.

Ermert, Monika (2008): Controversy Over Internet Governance: ITU Families And ICANN Cosmetics? http://www.ip-watch.org/2008/11/18/controversy-over-internet-governance-itu-families-or-icann-cosmetics/, (27.12.2016).

Chetty, Lee-Roy (2012): A New Season of Cooperation between ICANN and ITU. http://itu4u.wordpress.com/2012/12/05/a-new-season-of-cooperation-between-icann-and-itu/, (27.12.2016).

Taylor, Keisha (2012): Is the U.N. really trying to take over the Internet? http://ssir.org/articles/entry/is_the_un_really_trying_to_take_over_the_internet, (27.12.2016).

Internet Corporation for Assigned Names and Numbers (2013): Who Runs the Internet? http://www.icann.org/sites/default/files/assets/governance-2500x1664-21mar13-en.png, (27.12.2016).

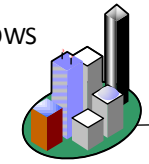
FEDERATED INTERNET

BEISPIEL-WORKFLOWS

LOKAL
Benutzer möchte sicheres Intranet nutzen: EFI Boot-Auswahl: „STREAMED OS (Firma)“
- Nutzer sendet Auth-Anfrage an lokale Zone: Firmen-Smarcard + PIN
- Lokaler Verzeichnisserver überprüft Daten und gewährt Zugriff
- Lokaler Datenspeicher streamt zertifiziertes (lokales) Betriebssystem und User-Anwendungen
- Nach dem Start werden die persönlichen lokalen Daten des Benutzers als Laufwerk hinzugefügt

NATIONAL
Lokal angemeldeter Benutzer möchte auf ein nationales Service zugreifen: Remote-Desktop: „NATION A OS“
- Nutzer sendet Auth-Anfrage an lokale Zone: Nationale Smartcard/Biometrie und PIN
- Lokales Verzeichnis sieht sich nicht zuständig und leitet Anfrage weiter (via Checkpoint)
- Nationaler Border Checkpoint identifiziert Paket als Auth-Anfrage and tunnelt sie zur Bearbeitung an die nationale Autorität
- Nationale Autorität überprüft Anmeldedaten und stellt einen Token an den Benutzer aus
- Nationaler Datenspeicher schaltet Remote-Betriebssystem frei und gewährt Zugriff auf seine Daten

ZONEN-TRUST & DATENVERKEHR
- Lokale Zonen vertrauen nationalen and globalen Zertifikaten, Nationale vertrauen der globalen Zone
- Lokale oder nationale Zonen (sowie Endnutzer) können selektive Trusts und Tunnels aufbauen
- Lokale/nationale/globale Services und Applicationen benötigen Zonen-Zertifikate zum Betrieb
- Datenaustausch ist per Default nur innerhalb der Zone erlaubt (Ausnahme: ID-Anfragen/Antworten)
- Produkte/Geräte sind werden von der lokalen Zone des Herstellers zertifiziert und vertraut (für Updates)



Globaler Dienstanbieter
z.B. Vereinte Nationen, Konzern-Präsenz

GLOBALE AUTORITÄT

Globaler Verzeichnisserver
- Globales User-Verzeichnis (globale IDs)
- Wie nationale Dienste
- Root DNS

Globaler Zertifizierungsserver
- Applikationszertifizierung
- Service/Domain Zertifizierung

Globaler Datenspeicher
- Daten für globale Nutzung
- Kein Zugriff auf nationale/lokale Daten
- Verzeichnis zertifizierter Apps

GLOBALE SICHERHEITSZONE

Zentralisiert, unabhängig, internationaler Trust-Broker
Benötigt global gültige ID

INTERNET 2.0

Hauptanwendungen
- Management der krit. Infrastruktur
- InternationalE Zusammenarbeit
- Bürgerdienste
- Gerätesicherheit
- Sicherer Datenaustausch

Prinzipien
- Nichtabstreitbarkeit durch „Real ID“
- Isolierte Softwareumgebung
- Gestaffelte Sicherheitszonen
- Trust Whitelisting

Kein Trust zu C (Zugriff verweigert)

Lokal<>lokal oder User<> User Trust ist möglich

NATIONALE SICHERHEITSZONE C

Nationale Infrastruktur
z.B. Kraftwerk

Geräte-APs

NATIONALE SICHERHEITSZONE A

Benötigt gültige ID von Nation A
oder vertraute ID einer anderen Zone

Gegenseitiger nationaler Trust (A<>B)

NATIONALE SICHERHEITSZONE B

John Doe
ID #113009823
Bürger von B

Zonen-Token: B, A, HomeNetwork, CompanyNetwork

LOKALE SICHERHEITSZONE

LOKALE AUTORITÄT

Lokaler Datenspeicher
- Benutzerdaten (Lokal; private Nutzung)
- Lokale Software/OS

Lokales Gerät
- Gestreamtes OS (EFI)
- Gestreamte Apps
- RAM verschlüsselt
- Keine lokalen Daten

Lokaler Border Checkpoint
- Überprüfung des eingehenden Verkehrs
- Intrusion Detection
- Tunnel Endpunkt

Apps können in unterschiedlichen Sicheheitskontexten betrieben werden

NEUTRALE ZONE

N. Border Checkpoint
Nation A Immigration

Authentifizierungs-Anfrage, Antwort

Nationale Autorität: Checkpoint
- Bearbeitet Auth-Anfragen
- Beantwortet ID-Anfragen (z.B. P2P Partner ID Check)

Nationaler Diensteanbieter
z.B. Finanzministerium

Lokaler Zert.-Server
- Applikationszertif.
- Servicezertifizierung
- Produktzertifizierung

Real ID

Benutzer-Authentifizierung
- Smartcard, PIN [, Biometrie]
- Globale ID
- Nationale ID
- [Firmen ID]

Lokaler Verzeichnisserver
- Benutzerverzeichnis und Auth (lokale/Firmen-ID)
- Liste der vertrauten Zonen

- Nationaler Datenspeicher (national zertifizierte Apps, Bürgerdaten)
- Nationaler Verzeichnisdienst (ID Verzeichnis)
- Nationaler Zert.-Server

NATIONALE AUTORITÄT

Hinweis: OS-Streaming benötigt eine hohe Bandbreite! Ein hohes Level der internationalen Zusammenarbeit (u.A. Standardisierung) ist erforderlich!