Stiftung Neue Verantwortung

Workshop-Protokoll: IT-Sicherheit durch Mindeststandards?

Mittwoch, 13. Dezember 2016, Stiftung Neue Verantwortung
(Chatham-House Regeln)

Das Projekt *IT-Sicherheit im Internet der Dinge* der SNV geht zunächst von zwei Arbeitshypothesen aus: (1) Bei IoT-Sicherheit mangelt es nicht an technischen Lösungen sondern es fehlen ökonomische Anreize vorhandene Lösungen umzusetzen. (2) Um daher IoT-Sicherheit nachhaltig zu stärken, muss man ökonomische Anreize für IoT-Hersteller schaffen, um schon bei der Entwicklung auf Sicherheit zu achten. In einer Reihe von Workshops untersucht das Projekt daher verschiedene Ansätze, um solche ökonomischen Anreize für IoT-Hersteller zu setzen: verpflichtende Mindeststandards, Ausweitung der Produkthaftung auf Software und ein Gütesiegel für Verbraucher. Der Fokus dieses Workshops lag auf verpflichtenden Mindeststandards.

Im Workshop wurden zunächst grundsätzliche Fragen zu verbindlichen Mindeststandards und IoT-Sicherheit diskutiert.

- **Standard und Gütesiegel:** Ein verbindlicher Mindeststandard als Marktzutrittsbedingung würde den kleinsten gemeinsamen Nenner im Sinne einer Basissicherheit darstellen. Ein Gütesiegel für den Verbraucher würde darauf aufbauen und signalisieren, dass durch den Hersteller mehr als die Basissicherheit umgesetzt wurde.

- **Ziel und Detailgrad des Standards:** Je enger das Schutzziel und je genauer die Vorgaben, desto höher der tatsächliche Schutz für das Gerät. Beispiel: Ein verbindlicher Mindeststandard für Internetrouter zum Schutz gegen Botnetze könnte beispielsweise den Einsatz bestimmter Softwarebibliotheken zur Verschlüsselung und Authentifizierung vorschreiben. Nachteil dieses Vorgehens wäre das schnelle „Altern“ des Standards und die potenzielle Vielfalt kleinteiliger Standards für unterschiedliche IoT-Geräte. Alternativ könnte der Standard technikneutral lediglich bestimmte Eigenschaften vorschreiben, z.B. „starke Verschlüsselung“ oder „2-Faktor Authentifizierung“ und die Implementierung den Herstellern überlassen. Hier kann der Hersteller jedoch eklatante Fehler bei der Umsetzung und Implementierung machen – was genau bedeutet „starke Verschlüsselung“? Ebenso wurde diskutiert, ob ein solcher Mindeststandard auch (Management)Prozesse berücksichtigen sollte.

- **Skalierung von Standards:** (1) Ist der Mindeststandard schlank genug, um auch von kleinen Unternehmen umgesetzt werden zu können? (2) Skaliert die Durchsetzung und Überprüfung (Zertifizierung) des Mindeststandards mit dem Wachstum im Internet der Dinge?

- **Rolle von Distributoren / Inverkehrbringern:** Eine strittig diskutierte Möglichkeit, damit (vor allem) ausländische OEM-Hersteller stärker auf Security-by-Design setzen, wäre die Distributoren bzw. Inverkehrbringer zur Verantwortung für Sicherheitsmängel zu ziehen.

- **Negative und positive Anreize schaffen:** Es wurde mehrfach betont, dass nicht nur Fehlverhalten / Nichteinhaltung eines Standards bestraft werden sollte, sondern dass auch positive Anreize gesetzt werden müssten: Indem es (gerade für kleinere Unternehmen) leichter und günstiger wird, auf Security-by-Design zu achten.

Frage 1. Unterscheidung zwischen Consumer IoT und Industrial IoT?

- Hinsichtlich verbindlicher Mindeststandards sollte zwischen Consumer IoT und Industrial IoT unterschieden werden. Eingesetzte Technologien und Gefährdungslage sind zwar u.U. ähnlich, rechtliche Rahmenbedingungen sind jedoch grundsätzlich verschieden.

- Eventuell ist eine weitere branchenspezifische Unterscheidung notwendig: Medical IoT, Connected Car, Industrial IoT? Gleichzeitig wurden Trends wie BYOD als Problem für die Trennschärfe zwischen IIoT und CIoT gesehen.

- Ebenso gibt es unterschiedliche Anforderungen zwischen CIoT und IIoT: Während bei CIoT Verfügbarkeit, Integrität und Vertraulichkeit ähnlich wichtig sind, hat im IIoT oft Verfügbarkeit höchste Priorität — auch dies spricht für eine Unterscheidung bei der Standardentwicklung.

- Da der Konsument vom CIoT-Hersteller stark abhängig ist, wurde diskutiert inwieweit CIoT-Standards strikter und deterministischer sein müssen.

Frage 2. Wie könnten verbindliche Mindeststandards überprüft werden?

- Möglichkeiten zur Überprüfung: Self-Assessment durch das Unternehmen oder Audit durch externe Experten (vom Unternehmen bezahlt) ähnlich der Jahresabschlussprüfung. Diskutiert wurde, ob der Ansatz einer externen Auditierung genügend skaliert, um die Anzahl an IoT-Herstellern und Produkten wirklich abzudecken.

- Öffentliche Überprüfung: Unternehmen verpflichtet sich zur Einhaltung der Standards und schafft Anreize für Community, Produkte zu analysieren (Open Source, Bug Bounty-Programme). Falls Standards nachweislich nicht eingehalten wurden, direkte Konsequenzen für Hersteller. Gleichzeitig wird eine Vorfalldatenbank aufgebaut (siehe CVE).

- Weiterhin wurde diskutiert, ob entsprechende verpflichtende Mindeststandards sektor-spezifisch und in mehreren Stufen eingeführt werden sollten.

- Ebenso war unklar, wie „tief“ eine solche Überprüfung sein kann, um sowohl die Masse neuer IoT-Produkte abdecken zu können, als auch genügend Aussagekraft zu haben. (Was wären adäquate Nachweise / Prüfartefakte?)

- Es wurde auch angemerkt, dass die diskutierten Vorschläge rein reaktiv seien statt präventiv und die Gefahr des White-Washing bestünde.

Frage 3. Wie komme ich von *heute* zu einer Welt mit angewendeten Standards?

- Da es keine „Silver Bullet“ für IoT-Sicherheit gibt und es noch einige Jahre dauern wird (im besten Fall), bis ein verpflichtender Mindeststandard für IoT-Geräte durchgesetzt wird, stellt sich die Frage, was ergänzende Ansätze wären.

- Einrichtung eines IoT-CERT (Computer Emergency Response Team), wie z.B. in Südkorea.

- Ausweitung der Möglichkeiten und Rechtssicherheit für Netzbetreiber / IT-Sicherheitsforscher um Netzwerk-/Port-Scans durchzuführen.

- Schaffung und Konsolidierung von Best Practices für IoT-Security (siehe Online Trust Alliance, GSMA Security Framework, OWASP Security Guidelines, etc.)

- Da die meisten IoT-Produkte durch OEMs hergestellt und dann durch andere auf den Markt gebracht werden, wurde diskutiert, ob Inverkehrbringer von IoT-Produkten (Media Markt, etc.) einen Single Point of Contact für Sicherheitsmängel bei IoT-Produkten zur Verfügung stellen müssen und rechtliche Konsequenzen drohen, falls sie dies nicht machen. Dies hätte potenziell negative Auswirkungen auf den IoT-Markt, könnte jedoch die Durchsetzung „sicherer“ IoT-Produkte fördern.

Frage 4. Wie sind verpflichtende Mindeststandards zu definieren, damit sie möglichst lange Gültigkeit behalten?

- Definition verbindlicher Mindeststandards (im Sinne einer Basisabsicherung) sollte auf abstrakter Ebene bleiben und eher im Sinne von Prinzipien formuliert werden und einen modularen Aufbau besitzen. (Beispiel: Es muss einen Update-Mechanismus geben) Konkrete Implementierungen werden dann in Umsetzungshinweisen ausgearbeitet und konstant aktualisiert (aktueller Stand der Technik)

- Spezifische Sicherheitsanforderungen einzelner Sektoren würden dann auf dem verbindlichen Mindeststandard aufbauen und diesen jedoch sektor-spezifisch anpassen und ausweiten.

- Es wurde diskutiert, dass Standards für CIoT deutlich stärker und ausdifferenzierter sein müssten, als für IIoT.

- Es wurde betont, dass ein verbindlicher Mindeststandard interdisziplinär und nicht nur durch die Industrie festgelegt werden muss.
- Auf Datenschutzgrundverordnung (Privacy-by-Design Regelung und Sanktionen bei Verstoß) ließe sich aufbauen, da sich die Unternehmen damit sowieso auseinandersetzen müssen.