Sicherheit-nach-Bedarf („Security by Desire“) in einer Zukunft ohne klassische Computer

Smartwatches sind der aktuelle Hype. Trotz neuer Modelle wie der iWatch ist diese Innovation nicht neu. Schon 1984 gab es von Casio mit der AT550 eine Art erste Smartwatch. 2009 präsentierte LG Electronics die LG-GD910, wobei nur noch ein Appstore gefehlt hat.

Der Trend geht klar in Richtung Internet der Dinge („Internet of Things“) und tragbarer Computersysteme („Wearables“). Wir wissen nicht mehr, was dabei mit unseren Informationen passiert.

Wie wird in der neuen verbundenen Welt die Sicherheit sichergestellt?

Die Entwicklung einer erfolgreichen Innovation durchläuft **drei Stufen**:

1. **Technologie funktioniert.** Wir sind über neue Möglichkeiten einfach froh, wie aktuell beim 3D-Drucker. Ein Aspekt wie Geschwindigkeit ist zweitrangig.
2. **Technologie funktioniert gut.** Für die breite Marktakzeptanz ist ein ausgereiftes Produkt notwendig. Für dieselben Funktionen wie z. B. Telefonieren und Surfen stehen inzwischen immer mehr Geräte (z. B. Smartphone, Smartwatch, interaktiver Fernseher etc.) jeweils als Einzelkanal zur Verfügung. Für den Nutzer besteht bei der zunehmenden Anzahl genutzter Geräte die Gefahr unnötiger Komplexität.
3. **Technologie funktioniert gut und erhöht den Wert anderer Technologien.** Ein einfaches Beispiel dafür ist die nahtlose Integration vom Handy im Auto: Ein Telefonat kann automatisch über die Freisprechanlage fortgesetzt werden. Aus Einzelkanälen wird Omnichannel. Symbiosen werden zum Standard und genau hier entstehen Sicherheitsrisiken.

Für den Nutzer, der alle Kanäle parallel in seinem persönlichen Kontext nutzen will, ist es irrelevant, mit welchen Computern er interagiert und so entsteht „Digitale Intelligenz“ über eine Rechnerallgegenwart („Ubiquitous Computing“ oder „Everyware“).

Fehlende Sicherheit kann dabei für den Nutzer eine Einschränkung des täglichen Lebens bedeuten. So verweigern viele Nutzer, die Google Glass außer Haus zu tragen. Die Gesellschaft akzeptiert diese Verletzung der Privatsphäre eines im Gesicht getragenen Gerätes nicht. Ohne Privacy-nach-Entwurf („privacy by design“) kann eine Innovation auf Stufe 1 zurückfallen!

Eine andere Gefahr ist, dass aus Symbiosen „Digitaler Parasitismus“ entsteht. Systeme könnten sich über einen koordinierten Angriff zu einem „Botnet der Dinge“ zusammenschließen. Kühlschränke versenden auf einmal Spam oder Router starten eine so genannte Dienstblockade („Denial of Service“).

Meine Empfehlung ist, Sicherheit-nach-Bedarf zu implementieren. Dies erfordert ein Vorausdenken und das Beheben von Sicherheitsschwächen direkt bei deren Entstehung. Da wir nicht alle Risiken vermeiden können, ist ein konsequent modularer Aufbau von Systemen erforderlich. Komponenten können dann durch sicherere ausgetauscht werden und so können wir auf übersehene oder nicht-vorhersehbare Sicherheitsrisiken mit Widerstandsfähigkeit („Resilience“) antworten.

Marinus Kuivenhoven ist Senior Security Spezialist bei Sogeti Niederlande.
E-Mail: marinus.kuivenhoven@sogeti.com