Medienmiteilung 27.11.2019

EU Cybersecurity Act: Warum die geplanten Verordnungen wenig Erfolg haben werden

Angriffe von Cyberkriminellen bedrohen nicht nur die Wirtschaft, sondern jeden von uns. Die geplante EU-Verordnung zur Standardisierung von Cybersicherheit soll die Sicherheit von Onlinediensten und vernetzen Geräten verbessern. „Das Problem der unsicheren Produkte wächst schneller als die Bürokratie nachkommt", kommentiert Mirko Ross und warnt vor einer zahnlosen Verordnung.

Bei der Konferenz „EU Cybersecurity Act" in Brüssel beschäftigten sich Experten jetzt mit dem aktuellen Stand der Umsetzung des Gesetzes. Ein Kernthema war dabei die Sicherheit von Produkten im Internet der Dinge (IoT). Konferenzteilnehmer Mirko Ross, bekannter IoT- & Cybersecurity-Experte, Entrepreneur und Influencer, erklärt im Interview, warum uns die Zeit davon läuft und weshalb die Experten nachbessern müssen.

Frage: Herr Ross, können wir uns zurücklehnen und darauf vertrauen, dass der Gesetzgeber uns zukünftig vor Cyberattacken schützen wird?

Mirko Ross: Schön wär's! Fakt ist, dass wir dringend Regeln brauchen, aber der bürokratische Prozess der EU viel zu langsam verläuft. Bis entsprechende Verordnungen in Kraft treten, haben Cyberkriminelle ungehindert Zugriff auf IoT-Geräte – die Folgen lassen sich nicht abschätzen, können jedoch verheerend sein. So hatte bereits vor drei Jahren das Mirai Botnet hunderttausende von billigen, unsicheren Web-Kameras gekapert und damit eine Cyberwaffe zum Mieten aufgebaut. Mit Cyberwaffen kann man Staaten, Unternehmen oder öffentliche Infrastruktureinrichtungen angreifen – ich überlasse es der Fantasie des Einzelnen, sich auszumalen, was das für jeden von uns bedeuten kann.

Frage: Sie warnen davor, dass die geplante Verordnung zahnlos ist. Was genau meinen Sie damit?

Mirko Ross: Wenn man die Sicherheit von IoT-Geräten verbessern will, muss man die Hersteller, also die Industrie, in die Pflicht nehmen. Es muss Vorgaben geben, um zu unterbinden, dass beispielsweise in IoT-Geräten ungesicherte Wifi-Module verbaut sind, die nicht mit Updates versorgt werden. Denn dadurch lädt man Angreifer sozusagen mit einer offenstehenden Tür ein. Mit den bisher vorgesehenen Regelungen wird das nicht wirklich möglich sein.

asvin GmbH
Schulze-Delitzsch-Str. 16
70565 Stuttgart
T 0711 2204093 0
F 0711 2240493 44

contact@asvin.io
www.asvin.io

@asvin_io

IBAN: DE64 6117 0024 0043 2245 00
BIC: DEUTDEDB611

Sitz Stuttgart
HRB 76700, Amtsgericht Stuttgart

Frage: Können Sie das genauer erläutern?

Mirko Ross: Um die Cybersicherheit von Produkten im Internet der Dinge zu erhöhen, ist ein freiwilliges Gütesiegel für Produkte vorgesehen. Damit setzt man auf die Eigenverantwortlichkeit der Industrie und auf bewusste Verbraucher. Die unfassbar große Zahl der unsicheren Geräte, die momentan in Betrieb sind, sprechen für sich: Verbraucher und Industrie sind schon aktuell mit diesen Rollen überfordert. Denkbar ist aber, dass fehlende verbindliche Vorschriften durch Regelungen im europäischen Verbraucherschutz ergänzt werden, so dass wir dann ein kompliziertes Konstrukt hätten, das schließlich doch eine höhere Sicherheit für Consumer Products vorschreibt.

Frage: Wäre denn ein solches mehr oder weniger verbindliches Sicherheitssiegel tatsächlich die optimale Lösung?

Mirko Ross: Eher nicht: Einer meiner Kritikpunkte an der Zertifizierung ist die Skalierbarkeit dieses Ansatzes: Um eine sorgfältige Zertifizierung sicherzustellen, braucht man Menschen, die sie durchführen. Das Potenzial an verfügbaren Mitarbeitern in Unternehmen ist aber begrenzt und damit die Zahl der durchführbaren Zertifizierungen. Das Internet der Dinge wächst dagegen exponentiell – die Kapazitäten beim Zertifizieren sind damit schnell überschritten. Diese beiden Welten passen deshalb nicht zusammen.

Frage: Was wäre Ihrer Einschätzung nach ein besserer Ansatz, um die Sicherheit nachhaltig zu optimieren?

Mirko Ross: Es müssen mehr verpflichtende Regeln zur Absicherung der Produkte vorgegeben werden, ähnlich wie beim Datenschutz: Dort hat die DGSVO sehr deutliche Vorgaben gemacht, die von Unternehmen beim Umgang mit personenbezogenen Daten eingehalten werden müssen. Bei Produkten im Internet der Dinge muss der Hersteller verbindlich verpflichtet werden, während der Produktlaufzeit für eine ausreichende Sicherheit zu sorgen. Produkte dürfen nicht mit bekannten Sicherheitslücken in Verkehr gebracht werden; Sicherheitslücken, die sich später ergeben, müssen vom Hersteller für eine angemessenen Laufzeit über Updates und Patches geschlossen werden. Schließlich ist die Haftung ein starkes Instrument: Nur wenn Hersteller für unsichere Produkte in Haftung genommen werden können, haben sie ein Interesse daran, ihre Produkte sicherer zu gestalten. Vorher leider nicht.

Herr Ross, wir danken für das Gespräch!

Abdruck honorarfrei, Beleg (Print, Scan) oder Link erbeten.

Mirko Ross ist iX-Autor und Gründer sowie CEO des Start-ups asvin und der digital worx GmbH. Für die Sicherheit im IoT engagiert er sich als Mitglied der Expertengruppe für Sicherheit im Internet der Dinge der Europäischen Agentur für Netzwerk- und Informationssicherheit ENISA. Darüber hinaus ist er Mitglied des Internet Of Things Council, einem weltweiten IoT-Think-Tank, und Projektkoordinator im eHealth-Forschungsprojekt MITASSIST.

asvin GmbH
Schulze-Delitzsch-Str. 16
70565 Stuttgart
T 0711 2204093 0
F 0711 2240493 44

contact@asvin.io
www.asvin.io

@asvin_io

IBAN: DE64 6117 0024 0043 2245 00
BIC: DEUTDEDB611

Sitz Stuttgart
HRB 76700, Amtsgericht Stuttgart

Image

Kontakt
seidel. agentur für kommunikation
Brunnengasse 3
73650 Winterbach (Stuttgart)
T: +49 7181 / 26 29 376
E: medien@seidel-kommunikation.de