HORIZON 2020

KEEPING YOUR CONNECTED SMART DEVICES PROTECTED AGAINST HACKERS AND CYBER ATTACKS

Ergebnisse in Kürze

IoT-Geräte durch die Abschaffung statischer Anmeldedaten sichern

Millionen veralteter Geräte für das Internet der Dinge können jetzt gesichert werden. Die Lösung baut auf einer „3 Tier Security Shell“ (Sicherheitsarchitektur mit drei Ebenen) auf, schafft feste Passwörter ab und führt selbst auf einfachen Chips eine Verschlüsselungs- und Authentifizierungs-Software aus. Die Selbstreparatur, die auf künstlicher Intelligenz basiert, sorgt für zuverlässige und sichere Systeme für das Internet der Dinge.

DIGITALE WIRTSCHAFT

SICHERHEIT

© elenabsl, Shutterstock

Das Internet der Dinge (IoT) ist kein separates Internet, sondern stellt Internetverbindungen her, über die einfache Geräte Daten austauschen. Beispiele für solche Geräte sind intelligente Fabrikanlagen, drahtlose Bestands-Tracker, intelligente Haushaltsgeräte und biometrische Cybersicherheitsscanner.

Die Vernetzung solcher Geräte mit dem Internet hat zu riesigen unvorhergesehenen Sicherheitsschwachstellen geführt. Mit dem Internet der Dinge verbundene Geräte sind bekanntermaßen für Hacking anfällig. Zusätzlich zu einer langen Liste an Schwachstellen, die sie mit Internetservern gemein haben, macht diesen Geräten auch eine schlechte Geräteauthentifizierung zu

schaffen, da mit gehackten Einheiten andere Geräte gehackt werden können. Dieses Problem wird als Zombie-Botnets bezeichnet und führt häufig zu Dienstleistungsverhinderungsangriffen. Eine zweite wesentliche Schwachstelle von Geräten für das Internet der Dinge ist, dass diese von der Rechenleistung her zu simpel sind, um Verteidigungs-Software mit Verschlüsselung auszuführen. Bis vor Kurzem hatten solche Geräte im Wesentlichen gar keinen Schutz.

Angriffe gehen auf Kosten der Gesellschaft

Fast die Hälfte aller Unternehmen, die Geräte für das Internet der Dinge anbieten, haben schwere Sicherheitsverletzungen erlitten, die sich auf den Umsatz auswirken. Da solche Sicherheitsverletzungen mittlerweile pro Jahr Verluste in der Höhe von mehr als 5 Billionen EUR verursachen, hat die IT-Branche damit begonnen, das Problem ernst zu nehmen. Ferner hat die Europäische Kommission die Datenschutz-Grundverordnung (DSGVO) verabschiedet, die nicht konforme Unternehmen seit 2018 mit schweren Bußgeldern belegt. Doch um wirkliche Sicherheit herzustellen, bedarf es mehr, als allein einer finanziellen Abschreckung.

Das EU-finanzierte Projekt ELIoT Pro entwickelte eine zuverlässige Lösung, indem eine wichtige Schwachstelle im Internet der Dinge – feste Passwörter – durch ein Einmalpasswort ersetzt wird, das im IoT-Systemadministrator-Authentifizierungsprotokoll auch bei der Authentifizierung und Verschlüsselung von Gerät zu Gerät verwendet wird. Diese Protokolle sind dazu auf eine sehr leichte Rechenleistung ausgelegt, die selbst für einfache mit dem Internet der Dinge vernetzte Geräte geeignet ist.

Statische Anmeldedaten sind passé

„Passwörter und andere statische Anmeldedaten – wie biometrische Daten, falls diese nicht richtig gehandhabt werden – sind gemeinhin bekannte und weitläufig ausgenutzte Schwachstellen“, erklärt Projektkoordinator Jack Wolosewicz. „80 Prozent aller Hacks beinhalten die Nutzung solcher Anmeldedaten.“ Um dies zu verhindern, schafft das Projektteam die Erfordernis solcher Anmeldedaten, sowie die damit verbundene Verletzlichkeit, ab, da diese durch einmalige Transaktions-Tokens ersetzt werden, die nach 200 ms ablaufen. Keine Passwörter bedeuten, dass es für Hackerinnen und Hacker nichts zu stehlen gibt. Hierdurch werden die Gefahren von Phishing- oder Man-in-the-Middle-Angriffen neutralisiert. Allein dadurch werden 80 % aller Bedrohungen für die Kommunikation zwischen Mensch und Maschine beseitigt, was etwa bei der Kommunikation zwischen Systemadministrator und Bedienungstafeln im Internet der Dinge der Fall sein kann.

Das Verschlüsselungsprotokoll des Projekts beseitigt die restlichen 20 % an Bedrohungen. Das Protokoll bietet eine starke Verschlüsselung, die dennoch auf

sehr schlichten Geräten ausgeführt werden kann. Dies wird mithilfe einer Software-Lösung erreicht, welche die Datenübertragung und die Geräteauthentifizierung für die Kommunikation zwischen Maschine und Maschine sichert.

Ein weiterer Faktor des ELIoT-Pro-Systems ist die Selbstreparatur, die durch eine prädiktive Analyse mit künstlicher Intelligenz erreicht wird. Somit kann das System anomale Aktivitäten wie etwa Cyberangriffe detektieren und gleichzeitig Geräte- oder Systemfehler vorhersehen.

„Das Konzept von ELIoT Pro macht es zu einer Universallösung für die Vernetzung über das Internet der Dinge“, merkt Wolosewicz an, „und zwar branchenunabhängig. Unser System wird für Anwendungen im Bereich des industriellen Internets des Dinge, intelligenter Gebäude, intelligenter häuslicher Umgebungen und intelligenter Städte verwendet. Unsere Lösung schließt alles ein und ist unvergleichlich.“ Daher schloss das Team Vereinbarungen mit großen Unternehmen in diesen Sektoren. Die Forscherinnen und Forscher versuchen als nächstes, weitere Vereinbarungen abzuschließen und parallel dazu die Verkaufs- und Vermarktungsstellen des Projekts auszubauen.

Schlüsselbegriffe

ELIoT Pro | IoT | Verschlüsselung | Passwörter | statische Anmeldedaten | Sicherheit | Internet der Dinge | Einmalpasswort | Transaktions-Token | künstliche Intelligenz | Selbstheilung.

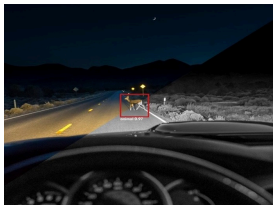
Entdecken Sie Artikel in demselben Anwendungsbereich

Digitalisierung des Wassersektors

7 Oktober 2022

Neue Sicherheitsscanner zur sicheren Erkennung von Bedrohungen durch sich in Bewegung befindende Personen

5 Oktober 2018



Kostengünstige Wärmebildtechnik unterstützt sichere automatisierte Mobilität

31 März 2023

Optimal für medizinische Umgebungen geeignete mobile Mehrzweckroboter

3 März 2023

Projektinformationen

ELIoT Pro

ID Finanzhilfevereinbarung: 822641

Projektwebsite

DOI
10.3030/822641

Projekt abgeschlossen

EK-Unterschriftsdatum
13 September 2018

Finanziert unter
INDUSTRIAL LEADERSHIP - Innovation In SMEs

Startdatum
1 Juni 2018

Enddatum
31 Mai 2020

Gesamtkosten
€ 2 827 625,00

EU-Beitrag
€ 1 979 337,50

Koordiniert durch
CYBERUS LABS
Poland

Letzte Aktualisierung: 30 Oktober 2020

Permalink: https://cordis.europa.eu/article/id/422562-iot-devices-secured-by-removing-static-credentials/de

European Union, 2025