



CYBERSECURITY
LIECHTENSTEIN

Zuhause in der Cloud - geClaut?

Datenschutztag 2024



zu uns

Patrik Marxer

- Mitgründer und Präsident Cybersecurity Liechtenstein
- >20 Jahre in IT

Martin Möbes

- Mitgründer und Vizepräsident Cybersecurity Liechtenstein
- > 18 Jahre im Bereich IT Sicherheit
- > 25 Jahre in IT





Agenda

- Cybersecurity Liechtenstein
- Smart Home – Gerätedschungel
- Erfahrungsbericht – Ledvance
- Ist ein Smart Home sicher?
- Übernahme Smart Home Cloud Account
- Datenhunger von Smart Home Clouds
- Resümee - Tipps und Tricks



Wir sind eine Gruppe von IT Sicherheits-Experten welche in verschiedenen Unternehmen in Liechtenstein arbeiten.

Unsere Ziele

- Unterstützen und fördern von jungen Nachwuchstalenten der Region in IT Sicherheit Kompetenz, Bewusstsein und Verantwortung
- Veranstaltungen / Treffen für Interessierte
- Vernetzung
- Nationalteam - Teilnahme European Cyber Security Challenge
Düsseldorf 2016, Malaga 2017, London 2018, Bukarest 2019 und Wien 2022, Hamar 2023 (Norwegen) waren wir dabei

<https://cybersecurity.li>

Verein **CYBERSECURITY** LIECHTENSTEIN European Cyber Security Challenge



Hacker EM unter
Schirmherrschaft der ENSIA



Smart Home – Gerätedschungel



Sicherheit

Kameras
Türklingeln
Türschlösser
Fenster- und Türsensoren



Beleuchtung

Glühbirnen
Lichtschalter
Sensoren



Heizung, Lüftung, und Klima

Rollläden und Jalousien
Thermostate
Sensoren Temperatur, Feuchte, Co2



Sprachassistenten

Amazon Echo, Google Home, Apple HomePod

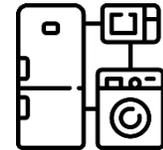
Unterhaltung

TV's
Lautsprecher



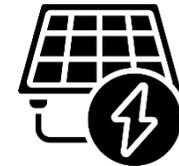
Haushaltsgeräte

Staubsauger
Kühlschränke
Waschmaschine
Trockner



Energie

PV-Wechselrichter
Smartmeter
WiFi-Steckdose
Wallbox



Automatisierungszentralen

Zentralisierte Steuerungseinheit



Aufbau Smart Home Cloud Account

- 1 Normale Glühbirne
- 1 Ledvance LED
- 1 Shelly – Wall Display
Schalter, Temperatur,
Luftfeuchte



Erfahrungsbericht – Ledvance I/II



Ledvance verkauft smarte Lampen und Leuchtmittel

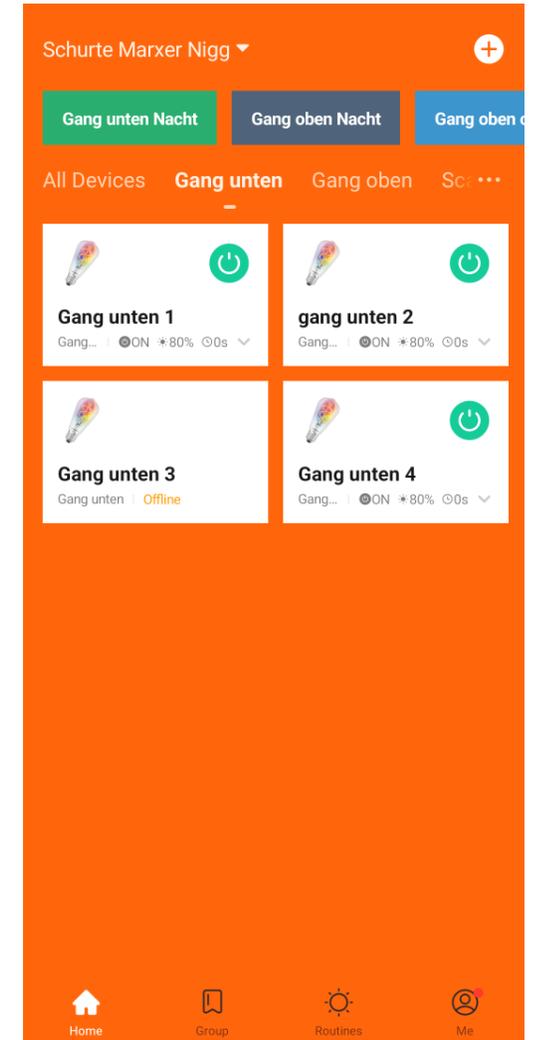
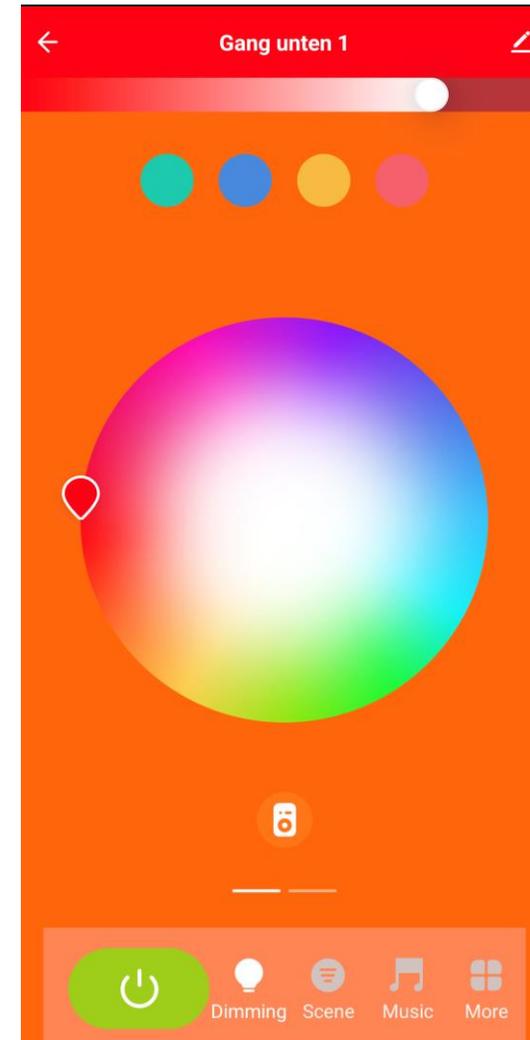
Hier unser Test mit einem LED-Leuchtmittel mit WIFI



Erfahrungsbericht – Ledvance II/II



- Gesteuert wird mit der Ledvance App
- Inbetriebnahme nur via App zwingend mit Cloud Account 
- Offline nur Standard Zustand (mit üblichem Stromschalter Ein/Aus)
- jegliche anderen Einstellungen nur via App/Cloud
- Kommunikation zwischen Leuchtmittel und Cloud sicher (TLS 1.2)





Ist ein Smart Home sicher?

Für die meisten Smart Home Geräte wird ein Cloud Account benötigt

Sind Username und Passwort sicher? → Wären Sie mit diesem Haustürschloss zufrieden?
→ für Online Banking schon lange nicht mehr
→ bei Apple und Google Zwei-Faktor-Authentifizierung fast zwingend nötig

Aber
→ bei den meisten Smart Home Anbietern ist eine „Zwei-Faktor-Authentifizierung“ nicht möglich



optional möglich:



→ Cloud Account nur so sicher wie Ihr Mail-Account



Email Account gehackt?

Wie kommt es dazu?

- Schwache Passwörter
- Phishing / Malware
- Unsichere Geräte
- Wiederverwendung von Passwörtern

Dienste wie <https://haveibeenpwned.com> zeigen, wenn Accounts zu der angegebenen Mailadresse in Leaks auftauchen. Dann heisst es: schleunigst Passwörter wechseln!

';--have i been pwned?
Check if your email address is in a data breach

pwned?

Oh no — pwned!
Pwned in 2 data breaches and found no pastes (subscribe to search sensitive breaches)

Recently added breaches

	70,840,771	Naz.API accounts
	4,670,080	Hathway accounts
	3,869,181	Legendas.TV accounts
	48,145	DC Health Link accounts
	13,405	InflateVids accounts
	3,901,179	Kaneva accounts
	4,563,166	Gemplex accounts

Übernahme Smart Home Cloud Account



1. Passwort vergessen
2. Mail mit Link im übernommenen Email Account
3. Neues Passwort und neue Email Adresse setzen...
4. und schon haben wir die volle Kontrolle

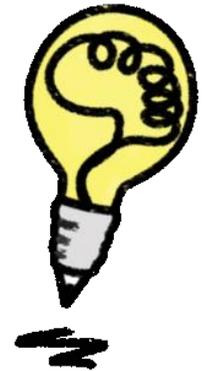


Demo Übernahme Smart Home Cloud Account

Fazit Übernahme Smart Home Cloud Account



- Da die Email Adresse geändert wurde gibt's keine Möglichkeit mehr, an den Account zu kommen
- Physische Geräte können nur auf Werkszustand zurückgesetzt werden
- und müssen wieder neu eingebunden werden





Smart Home Cloud Sicherheit

- Geschlossene Smart-Home-Systeme sind Vertrauenssache
- kein Einblick in die Firmware der Geräte und die Sicherheit der Cloud
- ...“Wochen, nachdem Hersteller über das Problem informiert wurde, lieferte die Netatmo-Cloud Einblicke in das fremde Haus“

Unerwünschte Einblicke: Fataler Fehler bei Netatmo-Sicherheitskameras UPDATE

| Stand: 15.12.2023 07:00 Uhr Ronald Eikenberg



Ein Leser hat uns eine Smart-Home-Kamera geschickt, die es so nicht geben darf: Sie erlaubt nämlich Einblicke in den Haushalt einer fremden Familie.

<https://www.heise.de/hintergrund/Unerwuenschte-Einblicke-Fataler-Fehler-bei-Netatmo-Sicherheitskameras-9568511.html?view=print>

Datenhunger von Smart Home Clouds



Daten sprechen Bände und alles geht in die Cloud



< Freitag, 09:00 AM

WLAN-

✓ Reinigung abgeschlossen!

Was machen solche Geräte im lokalen Netzwerk



Ziel der Geräte ist es, sich mit Gleichgesinnten zu verbinden,
um dem Nutzer eine einfache Inbetriebnahme zu ermöglichen
→ Geräte scannen das Netzwerk

Werden diese Netzwerkdaten in die Cloud zu den Anbieter gesendet?
(Welche Geräte Typen, Hersteller, Anzahl Geräte ...)



Resümee - Tipps und Tricks

- Insolvenz eines Cloud Geräte Anbieter bedeutet:
→ Geräte nicht mehr richtig funktionsfähig
- Viele Anbieter wollen Cloud Abos mit Zusatzdiensten verkaufen
- Schnittstellen zwischen Anbietern noch wenig standardisiert → grosse Anbieter forcieren Standards
- Sicherheit bei geschlossenen Systemen → Vertrauenssache
- Immer wenn möglich Multifaktor Authentifizierung aktivieren
- Passwort Manager nutzen: Keine Mehrfachverwendung von Passwörtern