



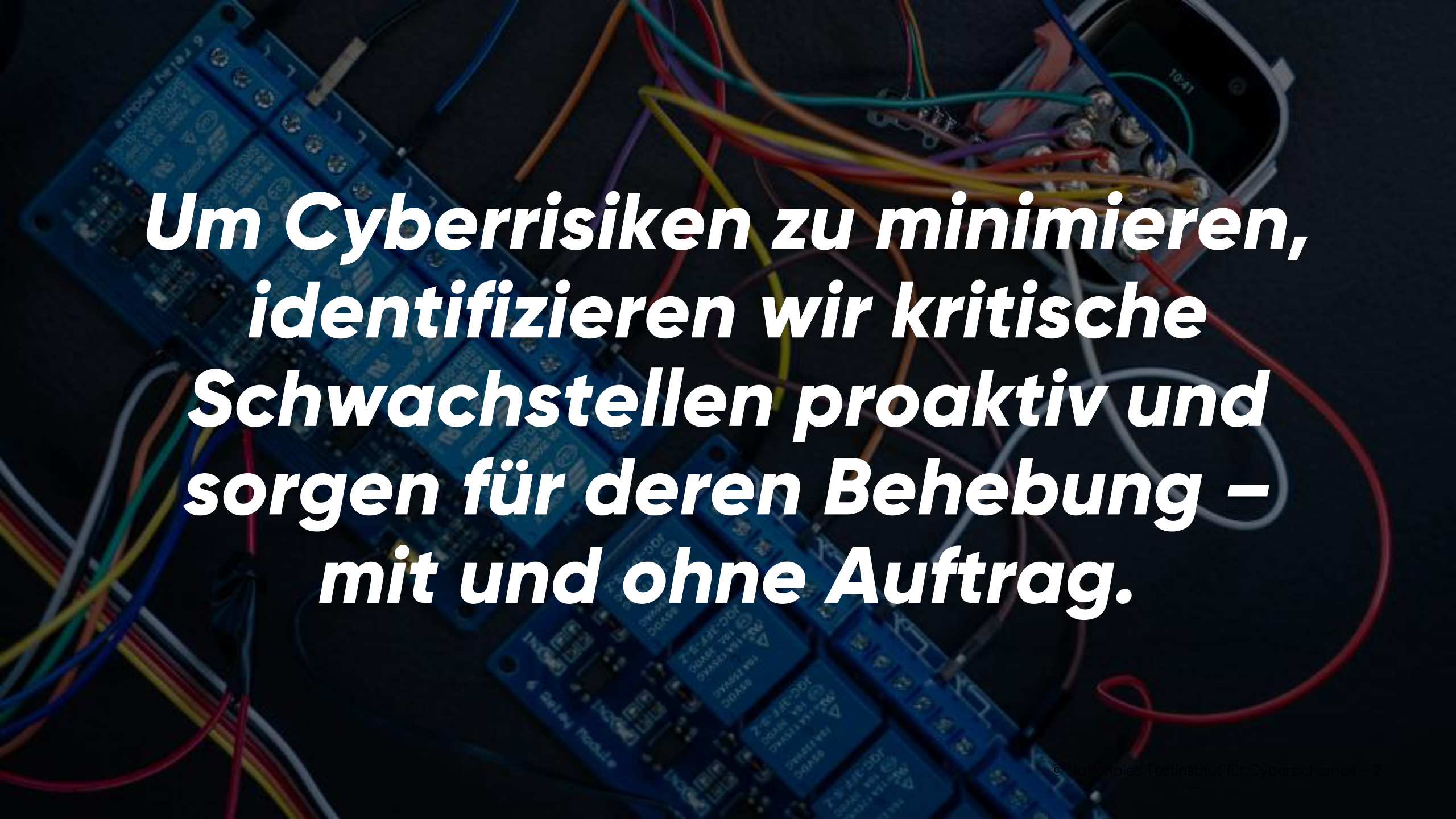
Tobias Castagna

Leiter Testexperten

Nationales Testinstitut
für Cybersicherheit

Verborgene Angriffsfläche: Wie übersehene Schwachstellen die Schweiz Cyberangriffen aussetzen

TEFO, 05. November 2026

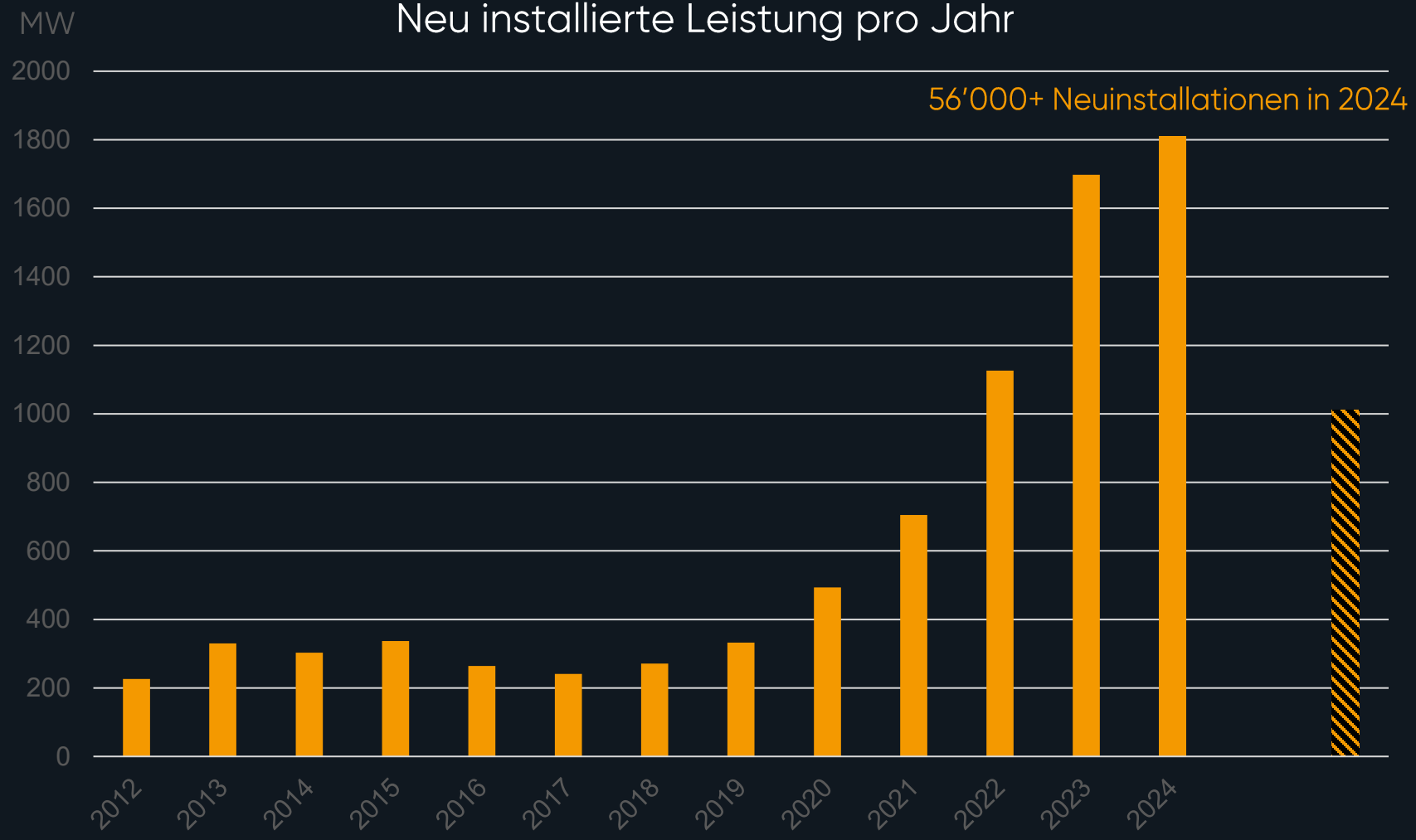


© Nationales Testinstitut für Cybersicherheit – 2


Wir testen was sonst
nicht getestet wird.


>14%
des Schweizer
Strombedarfs werden
durch Solarenergie
gedeckt

Neu installierte Leistung pro Jahr



Nationales Testinstitut für Cybersicherheit

Quelle: https://www.swissolar.ch/de/angebot/news-und-medien/fakten-und-zahlen/infografiken
Quelle: https://www.kkg.ch/de/wissen/strom-kernenergie/schweizer-kernkraftwerke.html

Warum werden so wenige Tests durchgeführt?

Anlagenbetreiber: „Hacking ist kein Problem! Ich beziehe meinen Strom einfach aus dem Netz.“

Netzbetreiber: „Wir können nichts tun, da wir die Anlagen nicht selbst betreiben.“

© Nationales Testinstitut für Cybersicherheit

MaDIoT

Manipulation of Demand via IoT Devices

© Nationales Testinstitut für Cybersicherheit



Stromausfall in Spanien und Portugal

Netzbetreiber schließt Cyberattacke aus

Stand: 29.04.2025 15:42 Uhr

Nach dem Stromausfall auf der Iberischen Halbinsel ist die Versorgung wiederhergestellt. Die Ursache ist weiter unklar - doch weder der spanische Netzbetreiber noch die

GOBIERNO DE ESPAÑA | CONSEJO DE SEGURIDAD NACIONAL | COMITÉ PARA EL ANÁLISIS DE LAS CIRCUNSTANCIAS QUE CONCURRIERON EN LA CRISIS DE ELECTRICIDAD DEL 28 DE ABRIL DE 2025

Versión no confidencial del informe del comité para el análisis de las circunstancias que concurrieron en la crisis de electricidad del 28 de abril de 2025

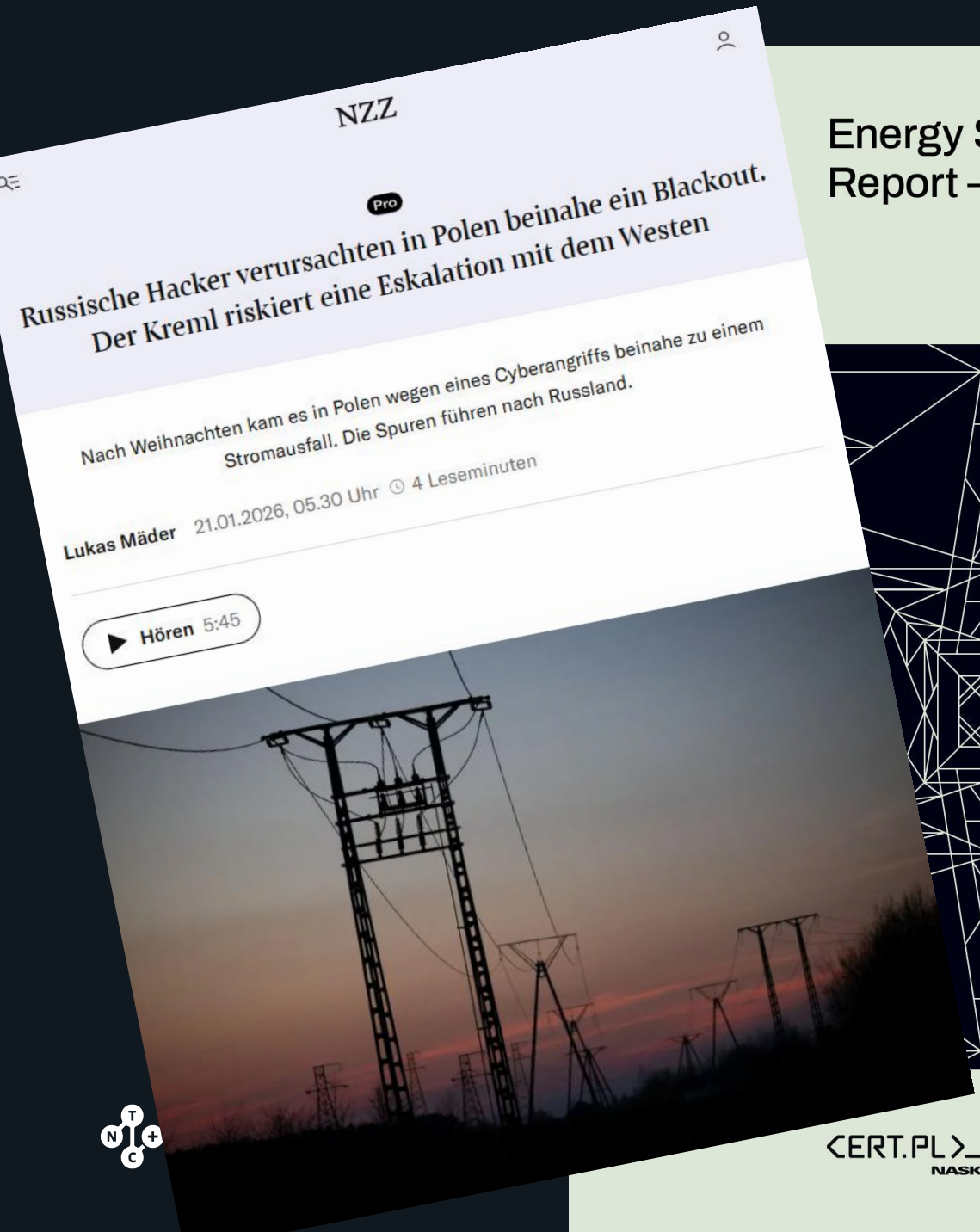
» Grid Incident in Spain and Portugal on 28 April 2025

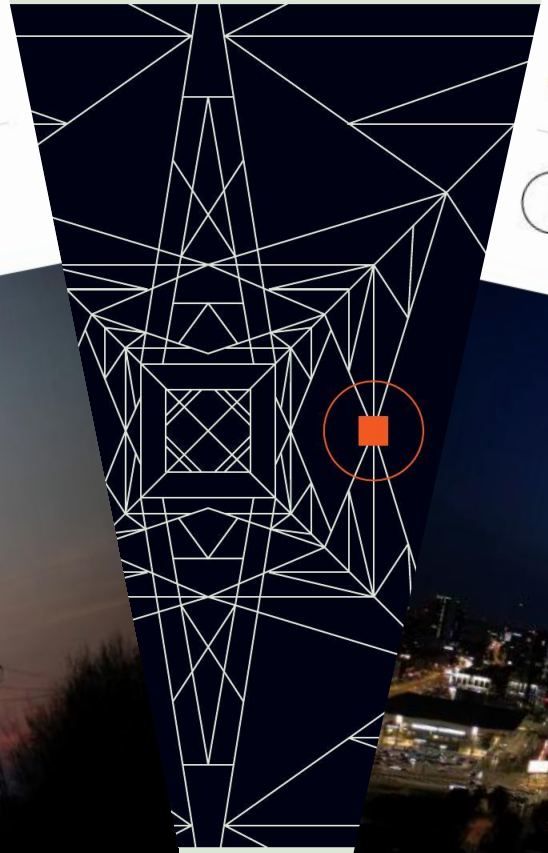
ICS Investigation Expert Panel
Final Report

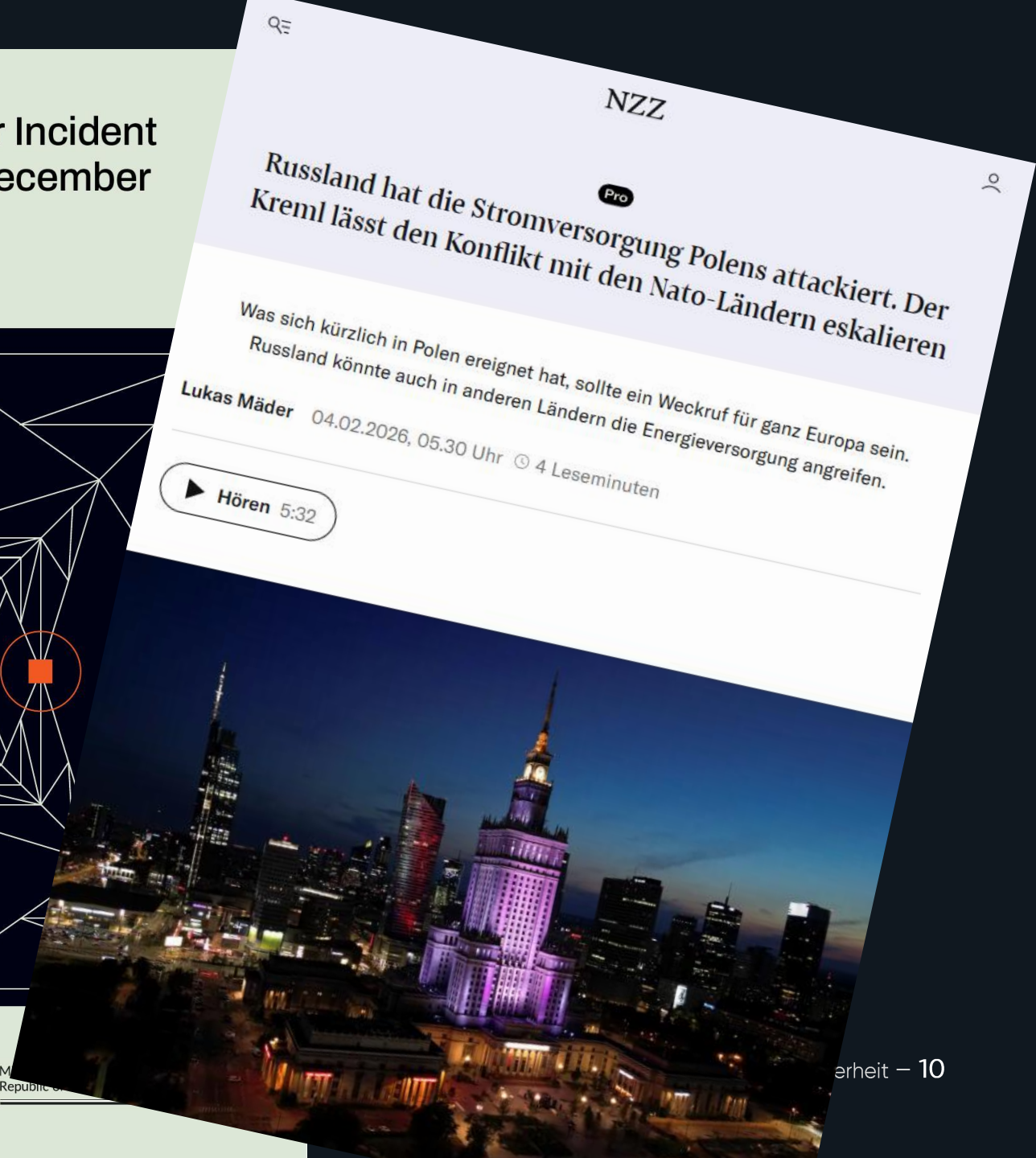


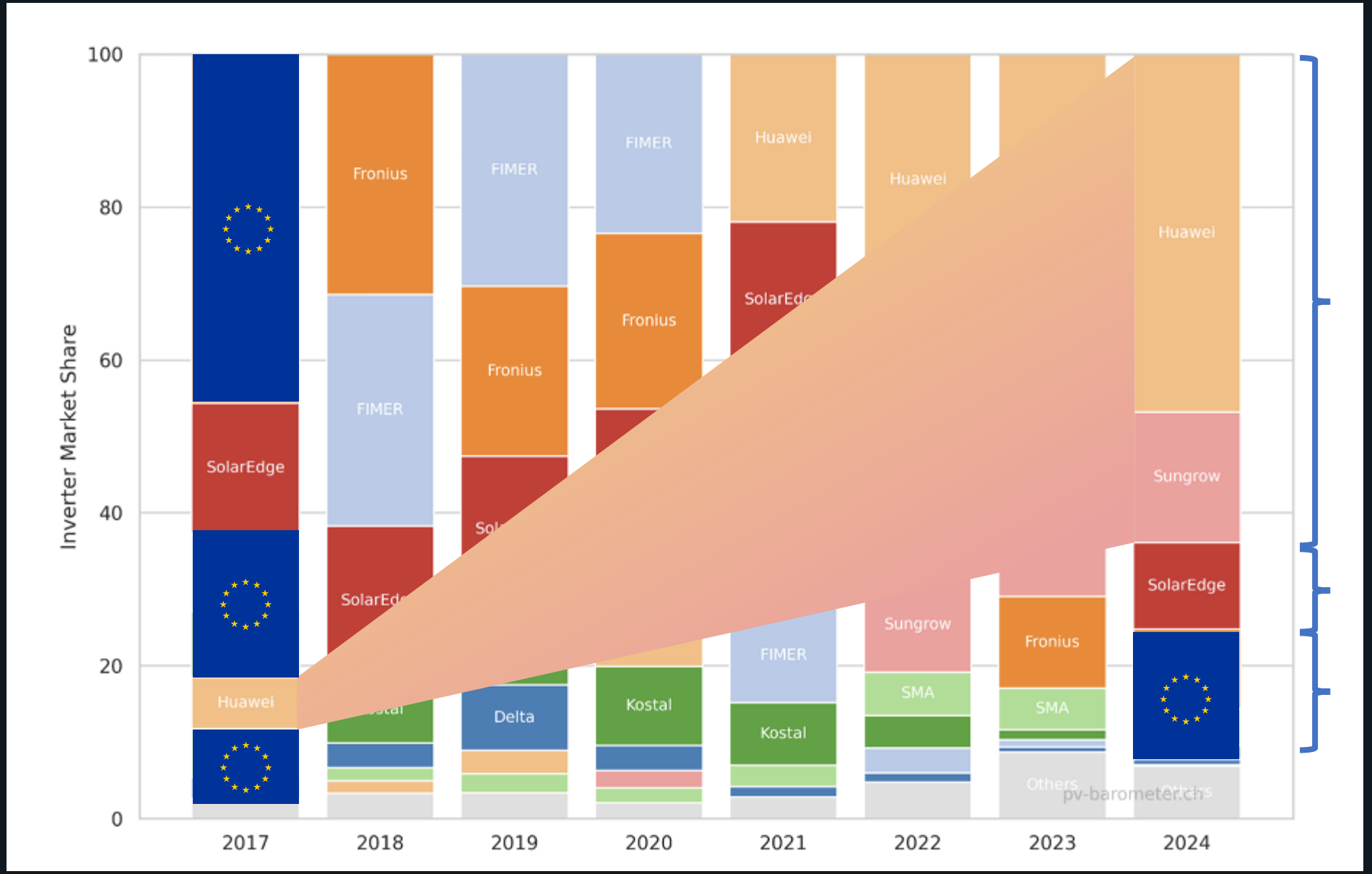
20 March 2026

Energy Sector Incident Report – 29 December









Nationales Testinstitut für Cybersicherheit

Quelle: https://www.pv-barometer.ch/

Nationales Testinstitut für Cybersicherheit

Cybersicherheit von Photovoltaikanlagen

Erkenntnisse und Empfehlungen

Version	1.0
Datum	17. September 2026
Klassifikation	Öffentlich
Autoren	Tobias Castagna, Stefan Gloor, Andreas Leisib Raphael M. Reischuk, Lukas Sohrmann, Fabio Zu
Verantwortlich	Tobias Castagna

Mit Unterstützung von | energieschweiz



DIE ZEIT

Z+ Hackerangriff auf Solaranlagen

Deutschland war nur einen Knopfdruck vom Superblackout entfernt

Ein Hacker hätte Hunderttausende Solaranlagen abschalten und so einen großflächigen Stromausfall verursachen können. Zum Glück war es einer von den Guten. Dieses Mal.

Von Gregor Aisch und Eva Wolfangel

7. Oktober 2026, 5:32 Uhr

Verschenken Zusammenfassen

Wenn jemand diese Anlagen fernsteuern könnte, würde aus ihnen eine vernichtende Waffe werden. Denn wenn dem Stromnetz plötzlich mehr als drei Gigawatt Leistung entzogen oder zugeführt werden, kann es zu großflächigen und tagelangen Stromausfällen kommen. Vor diesem Szenario warnen Fachleute seit Jahren. Ende August wäre es beinahe Realität geworden: Unbefugte hatten Zugriff auf die Steuerung von genau jenen 470.000 Solaranlagen in Europa, darunter 250.000 in Deutschland, die mehrheitlich von Privatpersonen betrieben werden. Die ZEIT konnte das nachvollziehen und verifizieren. Mit wenigen Klicks wäre es möglich gewesen, diese Anlagen gleichzeitig abzuschalten. Und damit in Deutschland und möglicherweise großen Teilen Europas die Lichter ausgehen zu lassen.

Golem

Abo testen Anmelden

DEALS KARRIEREWELT (SECURITY) (USA) (WIRTSCHAFT) (ENERGIE & KLIMA) (WISSE

ENERGIEWENDE

BSI warnt vor Fernabschaltung von PV-Anlagen aus China

Die Koalition will die Fernsteuerung von PV-Anlagen erleichtern. Doch das BSI sieht schon jetzt "erhebliches Gefährdungspotenzial".

Aktualisiert am 20. Januar 2025 um 17:35, veröffentlicht am 20. Januar 2025 um 14:30 Uhr / Von Friedhelm Greis

102 News folgen Teilen



Zu viel Solarstrom kann das Stromnetz überlasten.

Reuters

World Business Markets Sustainability Legal Commentary Technology Investigations

Rogue communication devices found in Chinese solar power inverters

By **Sarah Mcfarlane**

May 14, 2025 6:55 PM GMT+2 · Updated May 15, 2025



[1/4] Solar panels are arrayed on Earth Day in Northfield, Massachusetts, U.S., April 22, 2022. Picture taken with a drone. REUTERS/Brian Snyder/File Photo Purchase Licensing Rights


TAURO
TAURO


F26
FASSI
HAIR STYLE
welti-furrer
Zürich
Luzern
Spital
Herti
Bossard Arena
Polizei




HACKRF One
GREAT SCOTT GADGETS
PHILIPS AVENT
Arenti
Alecto
MENU
OK
PHILIPS AVENT
Alecto
DBX-85 ECO

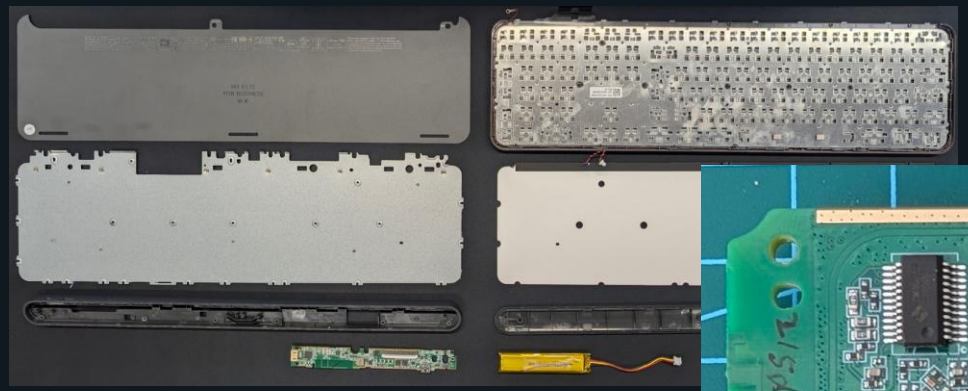
Peripheriegeräte

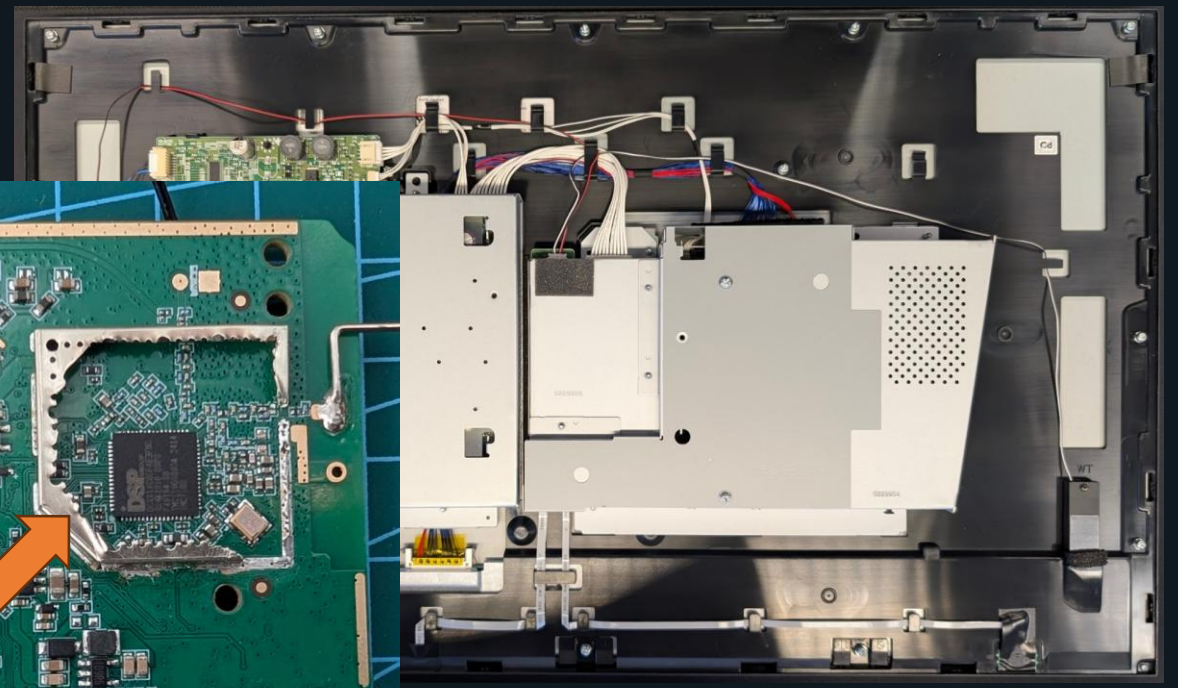




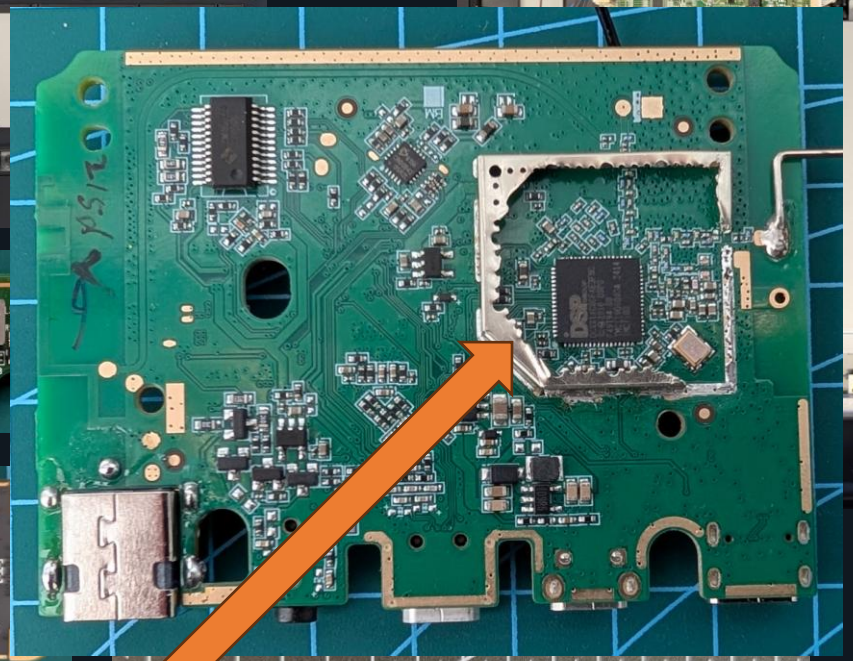


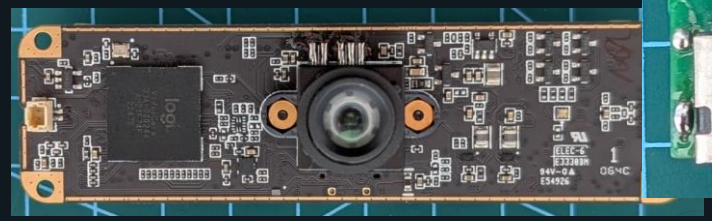


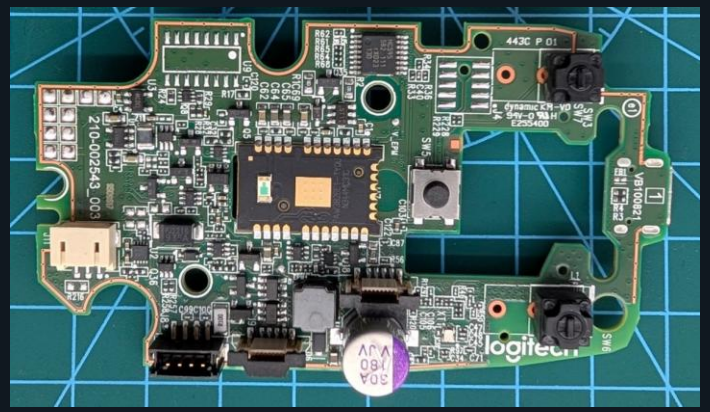


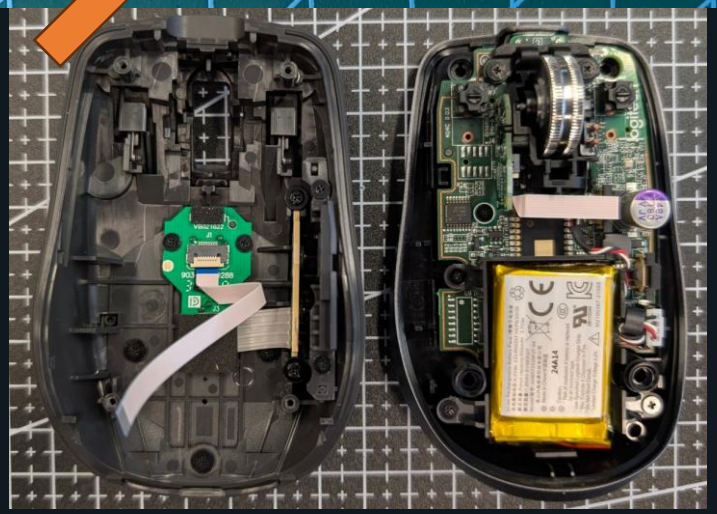


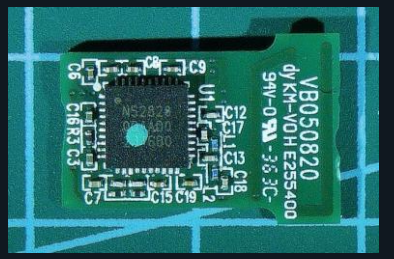








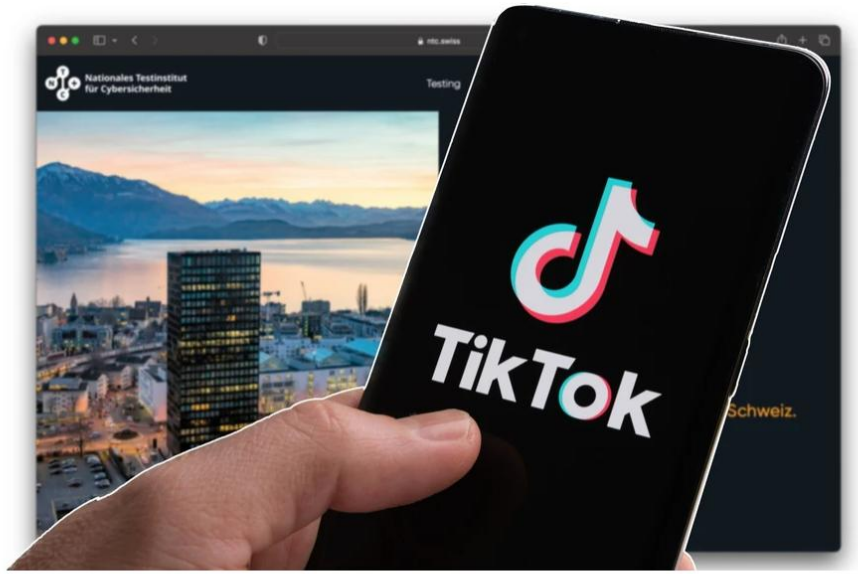






Nationales Testinstitut für Cybersicherheit

© Nationale



Die auch in der Schweiz populäre TikTok-App gibt Grund zur Sorge.
bild: watson

Die Cyber-Empa hat die TikTok-App geprüft – und warnt nun Firmen und Behörden

Unabhängige Schweizer IT-Sicherheitsexperten haben die China-App unter die Lupe genommen und empfehlen Firmen und Behörden, ihren Gebrauch kritisch zu hinterfragen.

75
News folgen

18.04.2023, 19:59 19.04.2023, 12:42

NZZ

Spioniert Temu seine Nutzer aus? Ein Schweizer Unternehmen hat die Sicherheit der chinesischen Shopping-App getestet

Temu ist so beliebt wie umstritten. Nun haben Experten für Cybersicherheit herausgefunden, wo die App tatsächlich Schwächen hat – und wo die Konkurrenz schlechter abschneidet.

Lukas Mäder, Janique Weder
05.12.2024, 08.00 Uhr 4 min

Hören Merken Drucken Teilen



Fehlende Anreize

Anlagenbetreiber: „Hacking ist kein Problem! Ich beziehe meinen Strom einfach aus dem Netz.“

Netzbetreiber: „Wir können nichts tun, da wir die Anlagen nicht selbst betreiben.“

© Nationales Testinstitut für Cybersicherheit

Verantwortungsdiffusion

Verantwortungsdiffusion bezeichnet das Phänomen, dass eine Aufgabe, die offensichtlich erledigt werden müsste, nicht ausgeführt wird – obwohl genügend fähige Personen vorhanden wären. Die Beteiligten hoffen bewusst oder unbewusst darauf, dass jemand anderes zum richtigen Zeitpunkt einspringt.

KIS =  jedes Spitals

© Nationales Testinstitut für Cybersicherheit

- Schwerwiegende Schwachstellen in allen KIS
  - 40+ mittlere bis schwerwiegende Schwachstellen
  - 3 Schwachstellen höchster Kritikalität

  } Zugang zu Patientendaten innert Stunden

- Tests in Zusammenarbeit mit den Spitälern durchgeführt

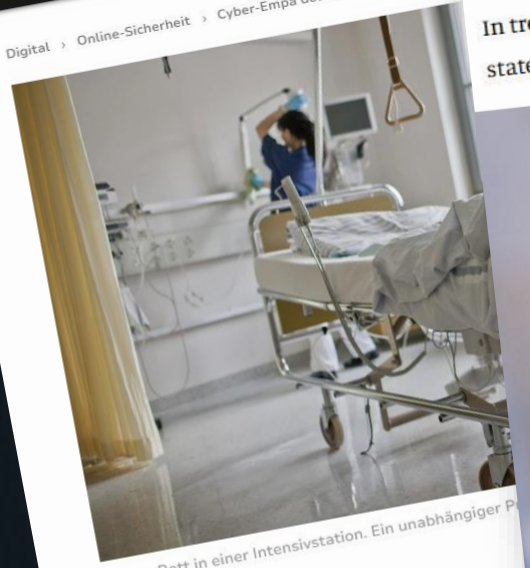
- Mehrheit der Schwachstellen wurde behoben
  - Einige erfordern eine grundlegende Neugestaltung der Softwarearchitektur

© Nationales Testinstitut für Cybersicherheit

watson

Schweiz International Wirtschaft Sport Leben Spass

Digital › Online-Sicherheit › Cyber-Empa deckt schwere Sicherheit



Leeres Bett in einer Intensivstation. Ein unabhängiger P
Mängel.
bild: keystone

«Cyber-Empa»
schwere Siche
bei Schweizer

Eine aktuelle Untersuchung de
bersicherheit (NTC) lässt aufh
hängigen Prüfer sind – vorsich

News folgen

CORRIERE DEL TICINO

Svizzera «Gravi lacune» nella sicur
sistemi d'informazione clinica degl

In tre dei sistemi analizz
state individuate più di



©Chiara Zocchetti

ATS
23.01.2025 09:57

I sistemi d'i
lacune nell
per la cibe
moderate

SRF

SRF news



Bericht zeigt IT-Sicherheitslücke

Aus Tagesschau vom 23.01.2025

News › Wirtschaft ›

Cybersicherheit in Spitäler

Schweizer Sp

NZZ

Patientendate
Bericht deckt
schwere Män

Schweizer Spitäler kü
ihrer Systeme. Das z

Lukas Mäder
23.01.2025, 08.00 Uhr



Die Rechner in S

LE TEMPS

ACCUEIL › CYBER Réservé aux abonnés

La cybersécurité des hôpitaux suisses est
dangereusement défaillante, alertent des
experts

L'Institut national de test pour la cybersécurité NTC a analysé trois systèmes d'information hospitaliers couramment utilisés en Suisse. Des risques très importants ont été mis en avant



- Cybersicherheit by Design und by Default
- Schwachstellentests und -behandlung
- Sicherheitsupdates während dem Produktlebenszyklus
- Meldung von Schwachstellen und Sicherheitsvorfällen

RED, CRA, NIS2, ...

© Nationales Testinstitut für Cybersicherheit –

Fehlende Anreize

Verantwortungsdiffusion



Tobias Castagna

Head of Test Experts at NTC,
#gerneperDu

tobias.castagna@ntc.swiss