IFA
Institut für Arbeitsschutz der
Deutschen Gesetzlichen Unfallversicherung

Gefahrbringende Angriffe auf vernetzte Industriesteuerungen

Fachtagung: Sicherheit und Gesundheit in der Warenlogistik

Jonas.Stein@dguv.de Dresden, 2021-09-15

Vernetzte Industriesteuerungen in Schlagzeilen

17.12.2014 15:58 Uhr | Security

BSI-Sicherheitsbericht: Erfolgreiche Cyber-Attacke auf deutsches Stahlwerk

07.08.2015 15:22 Uhr | Security

Scada-Sicherheit: Siemens-PLC wird zum Einbruchswerkzeug

Alert! 04.05.2018 11:10 Uhr | Security

ICS-Systeme von Schneider Electric: Angreifer könnten Fabriken übernehmen

Quelle: Oxygenstahlwerk, Bild 16 in DGUV Regel 109-601

ICS = Industrial Control System
PLC = Programmable Logic Controller

Schlagzeilen aus der Warenlogistik

Hacker blockieren Coop-Kassen für sechs Tage

Lebensmittelzeitung, 15. Juli 2021

Stress

ABB IRB 140, Industrieroboter: Hardcoded default credentials on IRC 5 OPC Server; 15.07.2020 Alias Robotics, CVE-2020-10287

böswillige Steuerung

WLAN-KAMERAS AUSGEKNIPST

Wer hat die Winkekatze geklaut?

Weg ist die Winkekatze - und keine unserer vier Überwachungskameras hat den Dieb gesehen. Denn WLAN-Cams von Abus, Nest, Yi Technology und Arlo lassen sich ganz einfach ausschalten.

Moritz Tremmel, veröffentlicht am 2. Oktober 2019 golem.de

Überfall

Beispiel: Funkfernsteuerungen

Sicherheitsanalyse von Industriekrananlagen ergab [1]:

Nicht autorisierte Fernsteuerung war

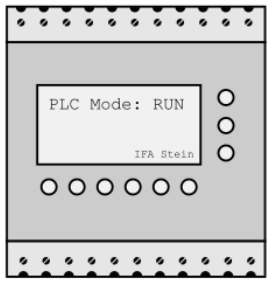
- sehr einfach
- sogar trotz Not-Halt möglich

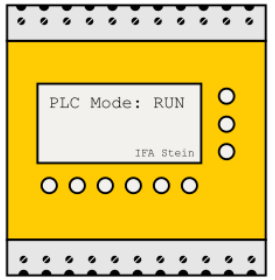
[1] Andersson et al., A Security Analysis of Radio Remote Controllers for Industrial Applications, Trend Micro Research, 2019

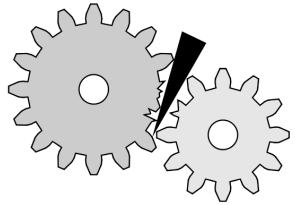
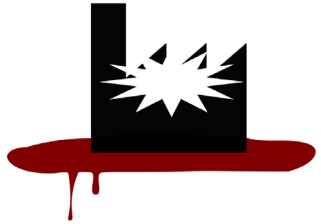
Safety & Security

Safety:	Ereignis ohne Absicht; Unfall
Security:	Ereignis mit Absicht; Angriff

Meilensteine der Schadsoftware für Industriesteuerungen

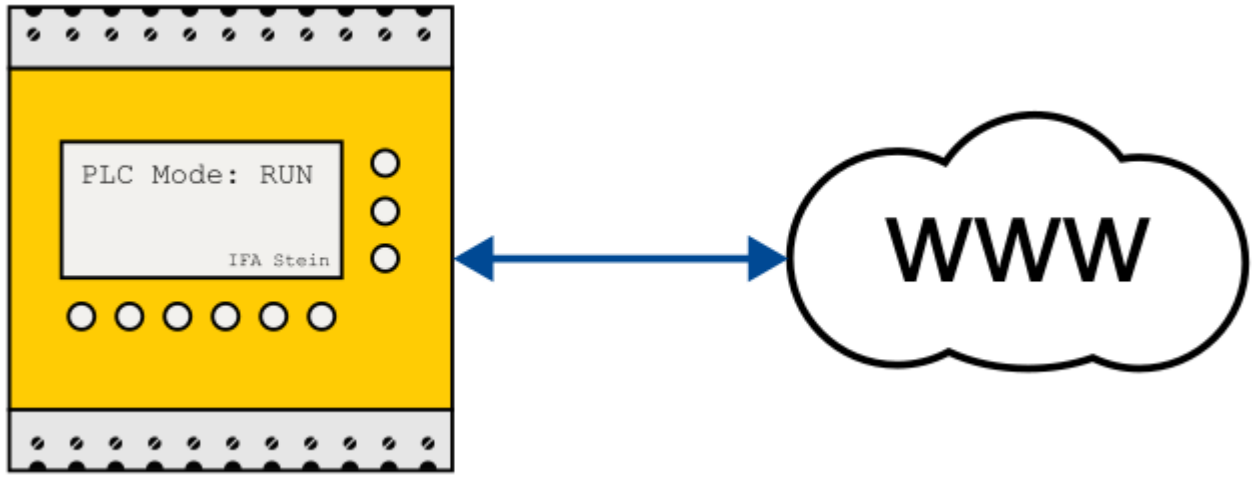




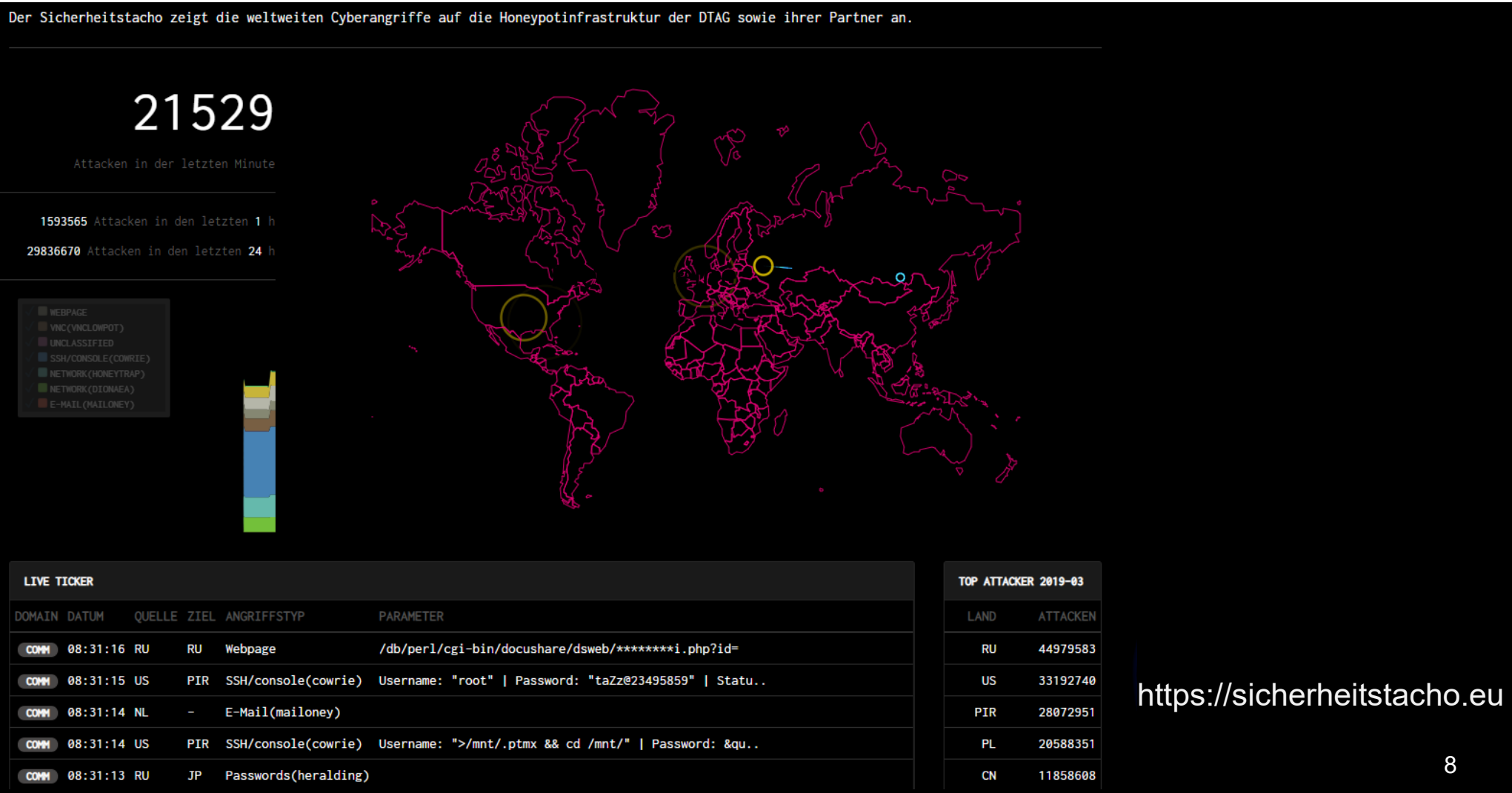



Jahr der Entdeckung	Name	SPS Für SPS programmiert	Safety SPS Für Safety-SPS programmiert	Absicht: Produktionsstopp	Absicht: Zerstörung
2010	Stuxnet	X		X	(X)
2010	Blackenergy2	X			
2014	Havex/Backdoor.Oldrea	X			
2015	Industroyer/Crashoverride	X		X	
2017	Trisis/Triton/Hatman		X	X	X

Szenario 1: System ist mit dem Internet verbunden

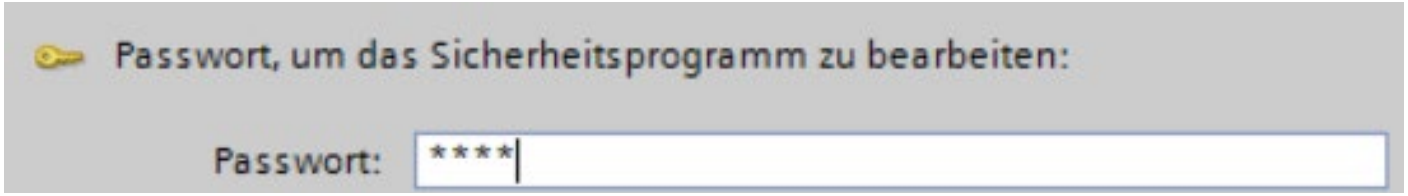


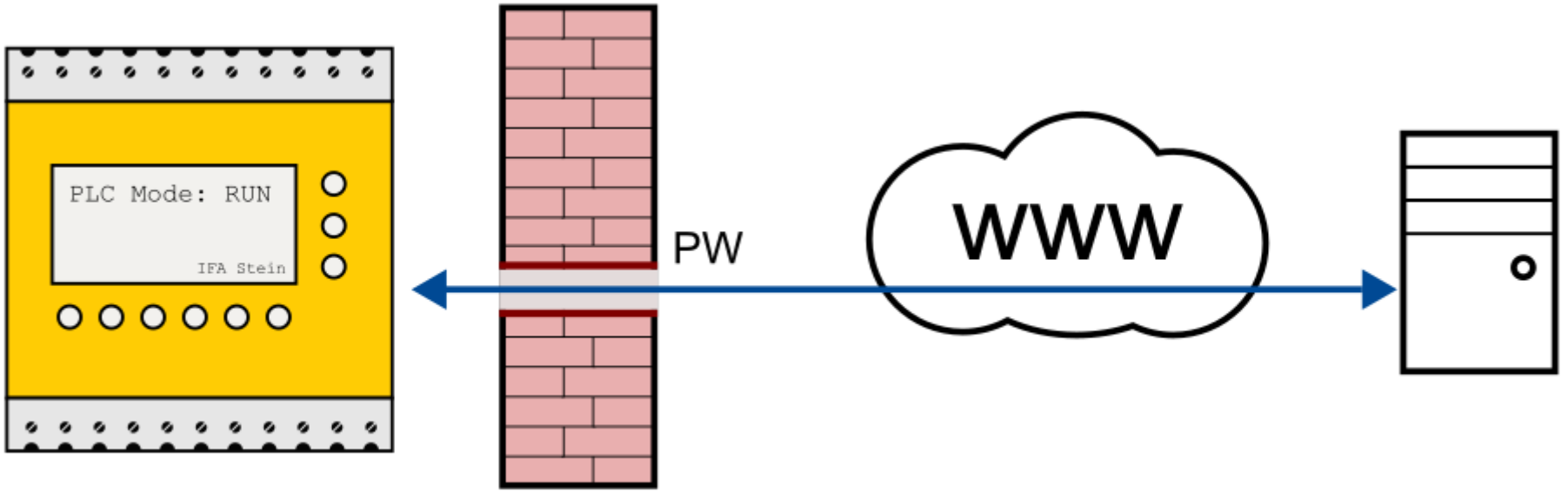
Aktuelle Angriffsversuche auf ein Honeypotnetzwerk



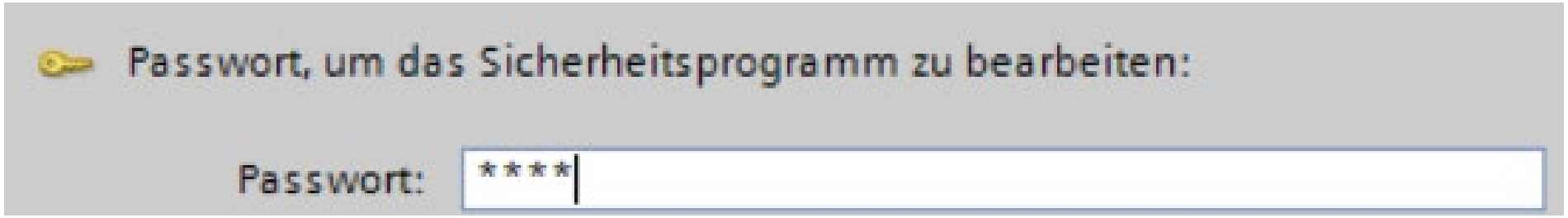
https://sicherheitstacho.eu

Szenario 2: Steuerung durch Passwort geschützt





Steuerungen oft nur durch ein Passwort geschützt



Beispiel	Problematik
Passwort vom Hersteller voreingestellt	Betreiber behält admin:123456
… und ist nicht änderbar	Backdoor in Produktserie (ICS-ALERT-11-204-01B)
Passwort wurde nach Dienstaustritt beibehalten	Passwörter verlassen Betrieb
Steuerung ausgemustert, Daten auslesbar	Passwort im Klartext

Bewertung von Passwörtern

Was ist ein unsicheres Passwort?

4242

Achtung Experiment!
Rein subjektiv.
Es gibt keine richtige,
oder falsche Antwort

Bewertung von Passwörtern

Was ist ein unsicheres Passwort?

Cologne1

Bewertung von Passwörtern

Was ist ein unsicheres Passwort?

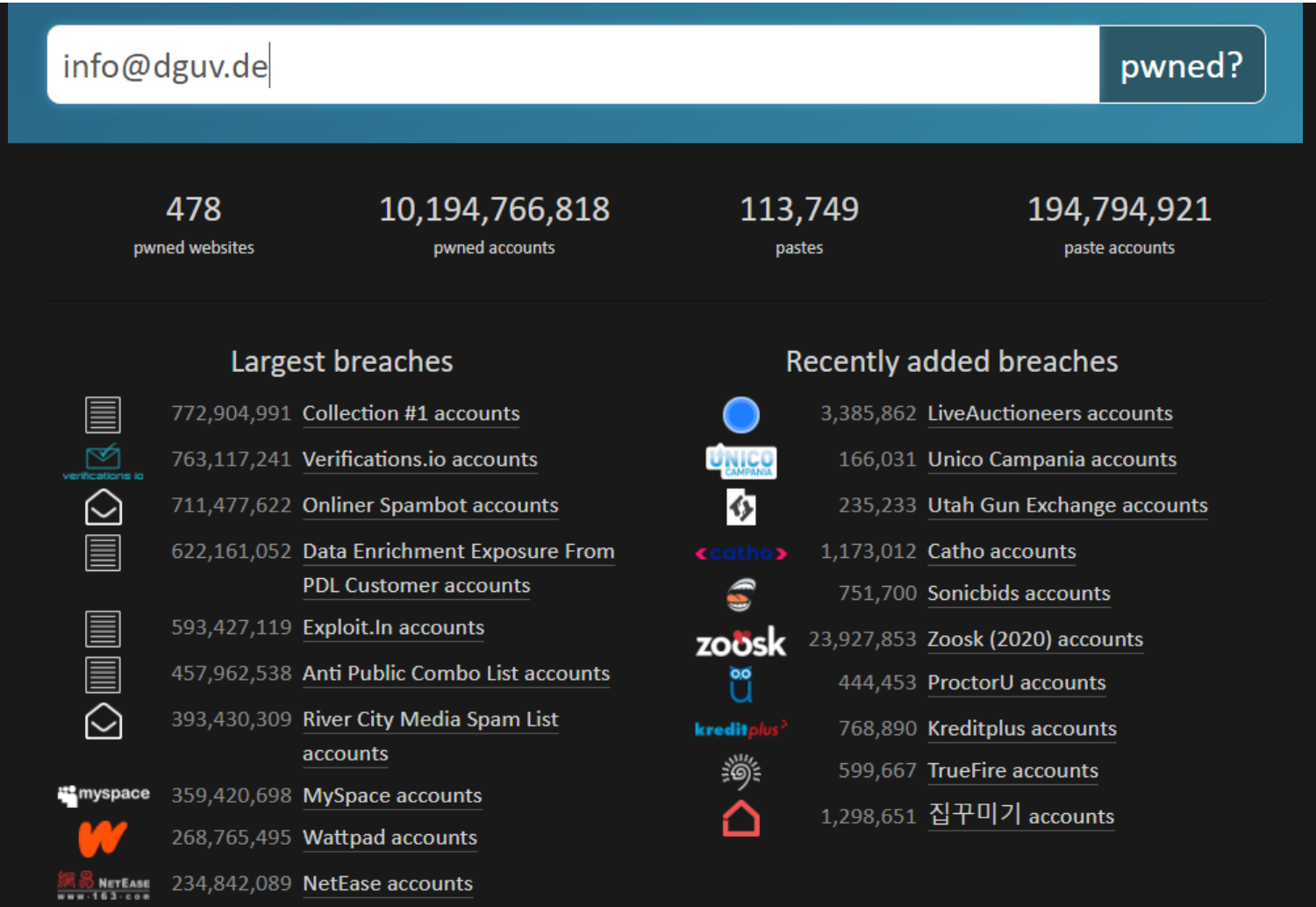
6NuH4Yp&se3upifa#z

Bewertung von Passwörtern

Was ist ein unsicheres Passwort?

6NuH4Yp&se3upifa#z
6NuH4Yp&se3upebay#z
6NuH4Yp&se3upgmail#z
6NuH4Yp&se3uplastfm#z
6NuH4Yp&se3upplc#z

Zugangsdaten, die öffentlich wurden



https://haveibeenpwned.com/

Welche Daten wurden öffentlich? Vier Beispiele

Adobe — 152 Millionen Datensätze

In October 2013, 153 million Adobe accounts were breached with each containing an internal ID, username, email, *encrypted* password and a password hint in plain text. The password cryptography was poorly done and many were quickly resolved back to plain text. The unencrypted hints also disclosed much about the passwords adding further to the risk that hundreds of millions of Adobe customers already faced.

Breach date: 4 October 2013
Date added to HIBP: 4 December 2013
Compromised accounts: 152,445,165
Compromised data: Email addresses, Password hints, Passwords, Usernames

LinkedIn — 164 Millionen Datensätze

In May 2016, LinkedIn had 164 million email addresses and passwords exposed. Originally hacked in 2012, the data remained out of sight until being offered for sale on a dark market site 4 years later. The passwords in the breach were stored as SHA1 hashes without salt, the vast majority of which were quickly cracked in the days following the release of the data.

Breach date: 5 May 2012
Date added to HIBP: 21 May 2016
Compromised accounts: 164,611,595
Compromised data: Email addresses, Passwords

Wiener Büchereien — 224119 Datensätze

In June 2019, the library of Vienna (Wiener Büchereien) suffered a data breach. The compromised data included 224k unique email addresses, names, physical addresses, phone numbers and dates of birth. The breached data was subsequently posted to Twitter by the alleged perpetrator of the breach.

Breach date: 10 June 2019
Date added to HIBP: 28 June 2019
Compromised accounts: 224,119
Compromised data: Dates of birth, Email addresses, Names, Phone numbers, Physical addresses

Stratfor — 859777 Datensätze

In December 2011, "Anonymous" attacked the global intelligence company known as "Stratfor" and consequently disclosed a veritable treasure trove of data including hundreds of gigabytes of email and tens of thousands of credit card details which were promptly used by the attackers to make charitable donations (among other uses). The breach also included 860,000 user accounts complete with email address, time zone, some internal system data and MD5 hashed passwords with no salt.

Breach date: 24 December 2011
Date added to HIBP: 4 December 2013
Compromised accounts: 859,777
Compromised data: Credit cards, Email addresses, Names, Passwords, Phone numbers, Physical addresses, Usernames

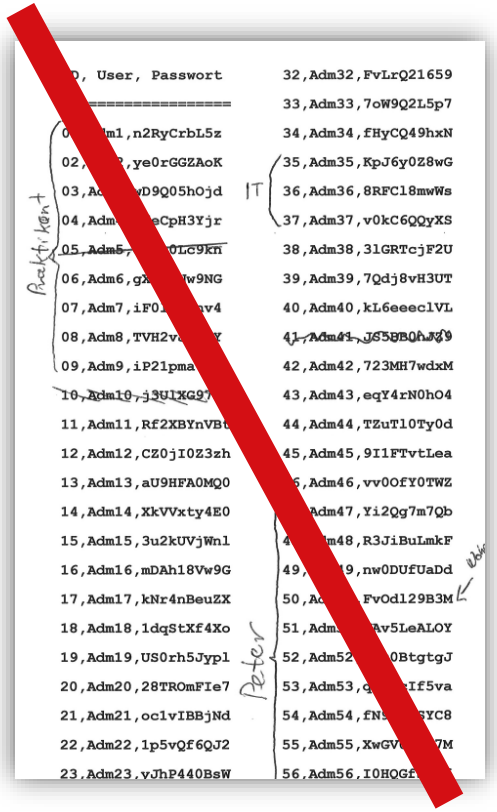
Quelle https://haveibeenpwned.com/PwnedWebsites

Login an Desktop und Industriesteuerung

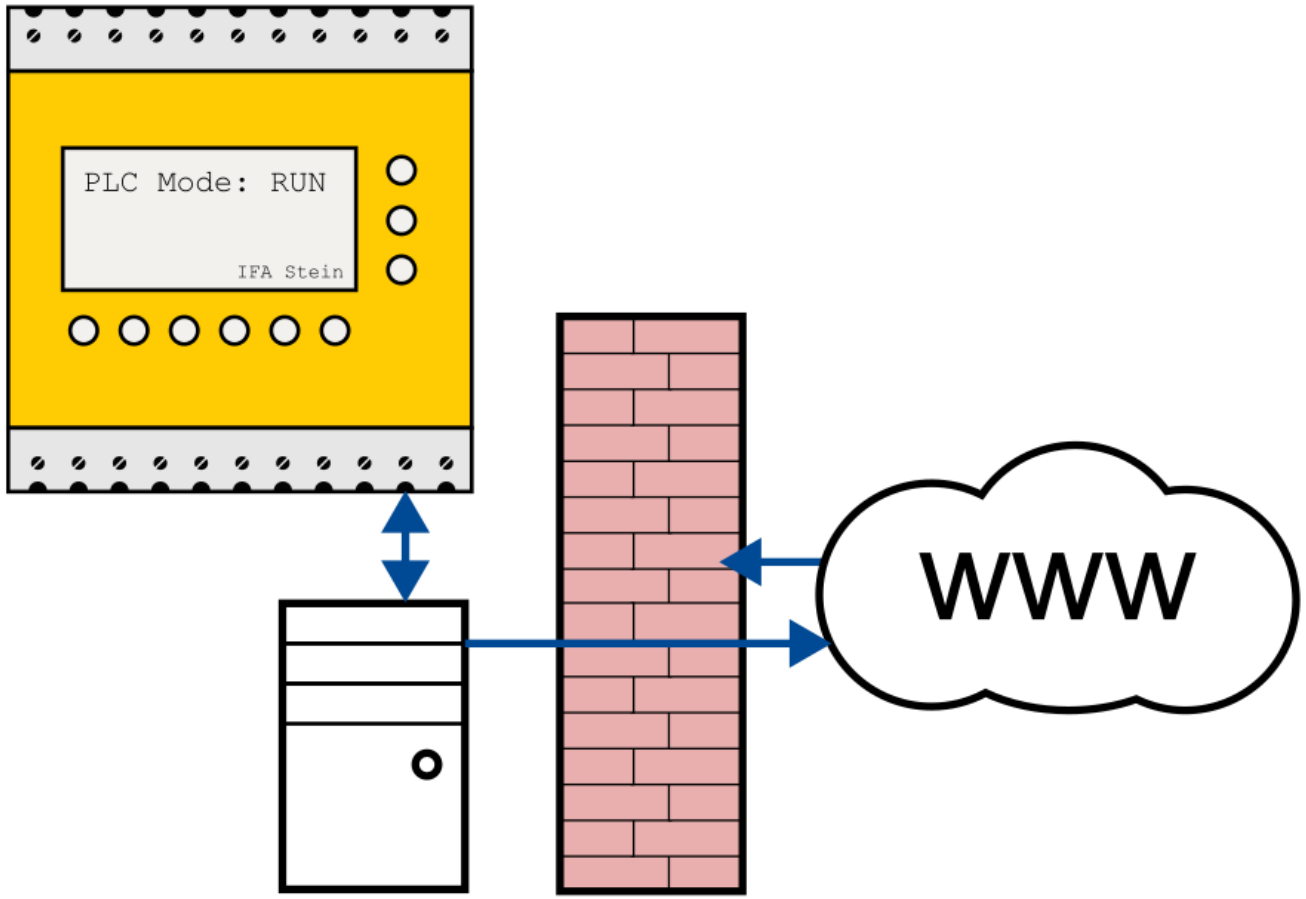
	Desktoprechner	Industriesteuerung	Auswirkung
Loginfrequenz	Oft, ~ 1 Login / Tag	Unregelmäßig z.B. 10 Logins, 5 Jahre kein Login, 3 Logins	Fehlende Routine
Komplexes Passwort	Einfach, 104 Tasten, Passwortmanager	eingeschränkt	Schwache Passwörter
Menschen pro Account	1	viele	Weitergabe von Pw.
Systeme pro Mensch	1	viele	Synchronisation notw.
Passwort vergessen	geringer Schaden, Passwort zurücksetzen	Hoher Schaden, Stillstand, Insolvenz	Geringe Bereitschaft für sichere Pw.

Alternativen zum Passwort

- kryptographische Hardware zertifiziert, versiegelt
- geheimer Schlüssel verlässt Chip nie
- anwenderfreundlich:
  1 Geheimzahl schützt Chip
  1 Chip für viele Accounts
- bis SL 3 und SL 4 nach DIN EN 62443 möglich



Szenario 3: Steuerung „nur“ mit Office Netzwerk verbunden



Zeit für eine kleine Demonstration...

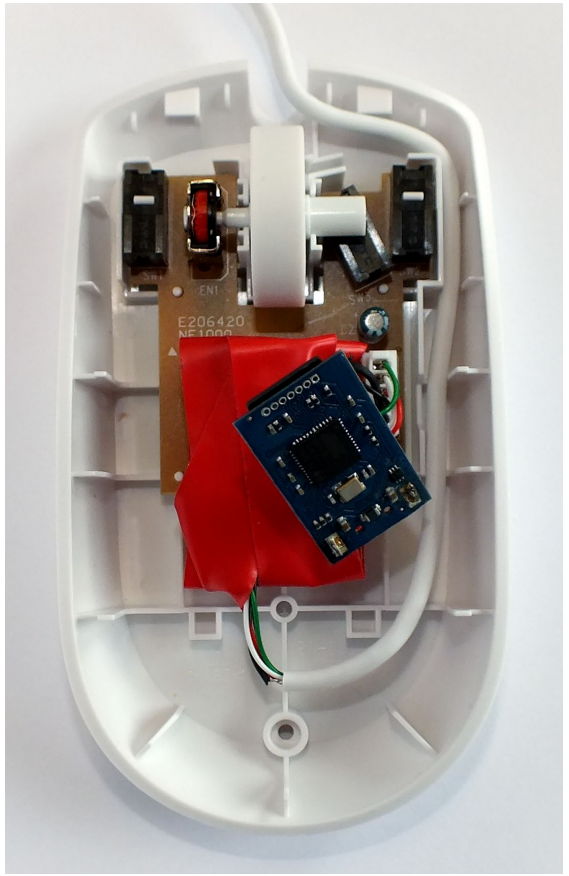
Tunnel durch Firewalls in das Firmennetz

Angriff mit manipulierter Firmware

- kann Firewalls von innen durchtunneln
- ist unsichtbar für Virenscanner
  (können nur alte, bekannte Malware erkennen)
- ist nicht auf USB beschränkt

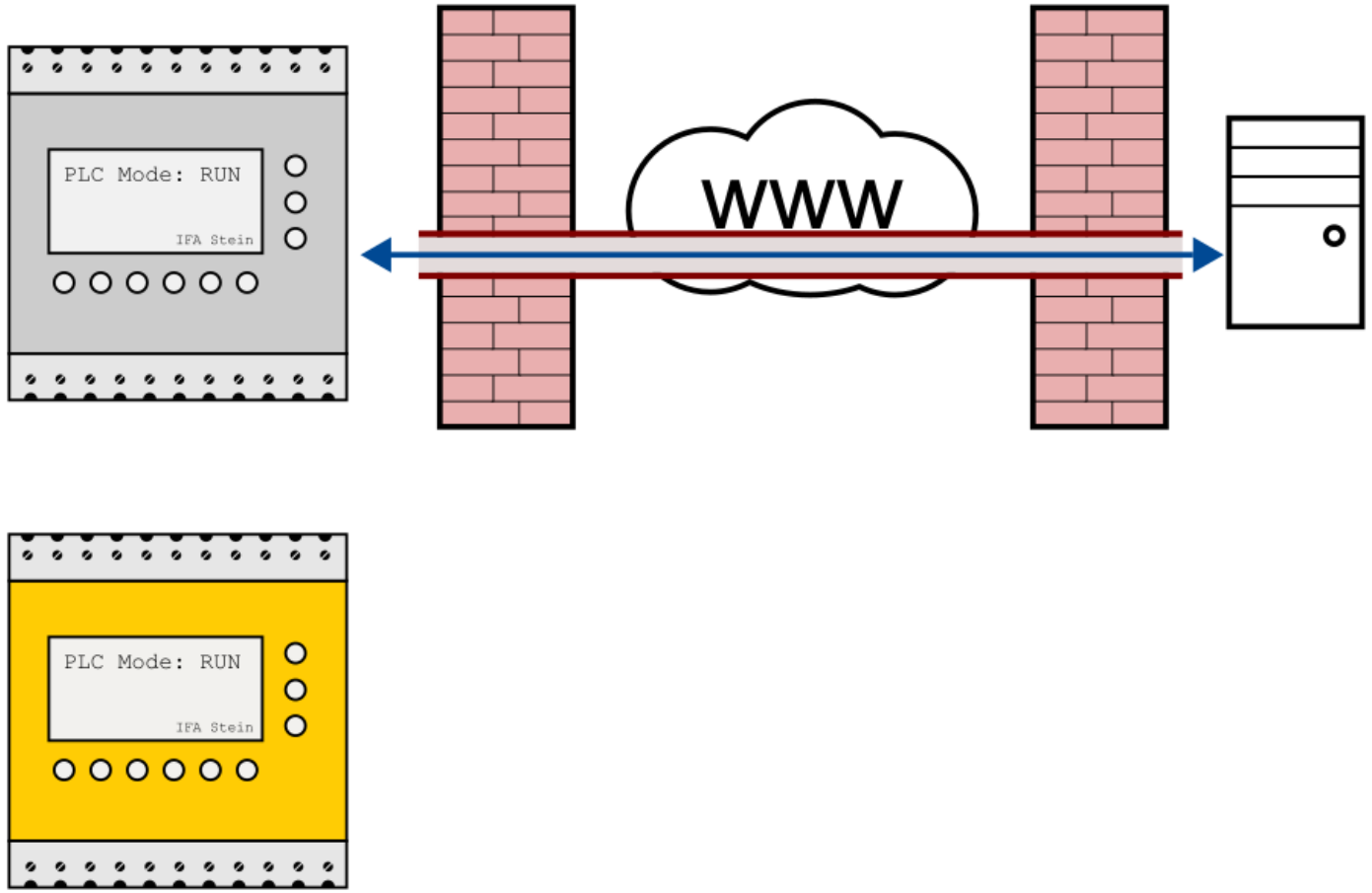
Gegenmaßnahmen:

- Firmware: Herstellfirma verhindert Überschreiben
- USB-Sticks: IFA Prototyp mit Datenschleuse



Weitere Informationen zu BadUSB: Karsten Nohl, Sascha Krißler und Jakob Lell, Blackhat (2014)

Lösungsansatz: Rückwirkungsfreie Trennung



Umfrage: Ansprechperson für Sicherheitslücken erreichbar?

Gedankenexperiment:

Ihre **Fernwartungslösung** hat eine **kritische Sicherheitslücke**.

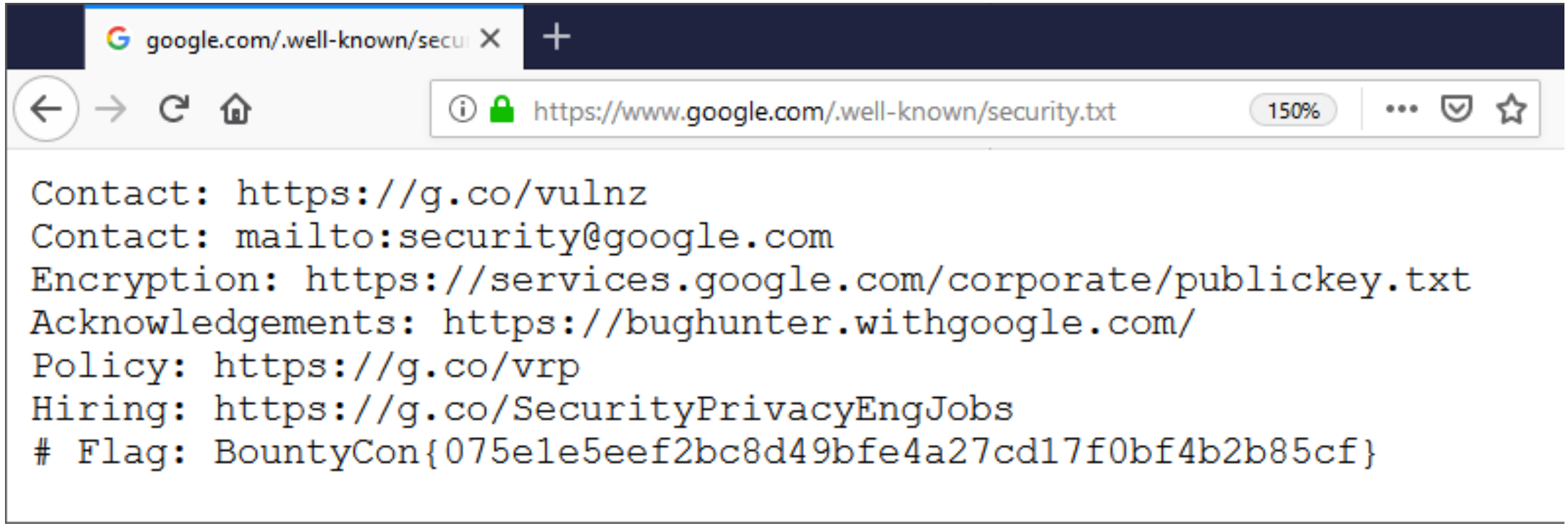
Jemand **entdeckt** diese und möchte sie Ihnen **melden**.

Findet man in Ihrem Betrieb die richtige Ansprechperson für Sicherheitslücken innerhalb von 15 Minuten?

Ja / Nein

Dauert die Suche nach dem richtigen Kontakt zu lange, wird die Nachricht nicht mehr verschickt.

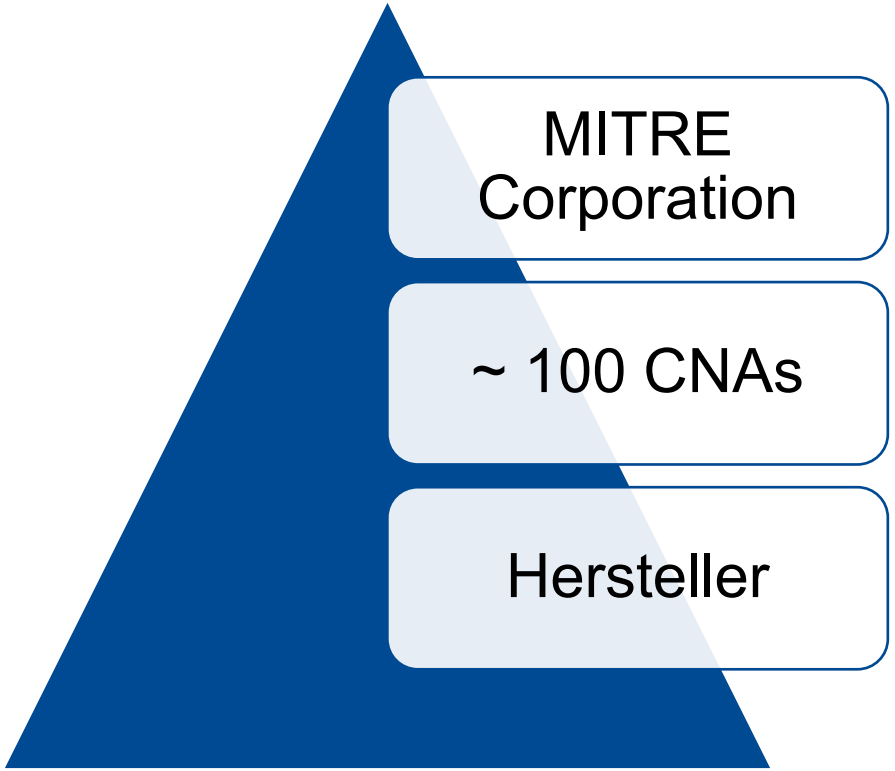
Lösungsansatz: security.txt



- kostenlos
- Standard, Internet Engineering Task Force (IETF), siehe https://securitytxt.org/

Internationale Sicherheitswarnungen

- Herstellfirmen vernetzen sich per CNA
- CNA (z.B. https://cert.vde.com/) koordiniert
- Zentrale CVE Datenbank mit koordinierten Warnmeldungen https://cve.mitre.org/
- Betreiber und Integratoren können sich zu Komponenten der Fernwartungskette informieren.
  Software, Router, Firewall, Steuerung, Bibliotheken



CVE: Common Vulnerabilities and Exposures

CNA: CVE Numbering Authority

Zusammenfassung

- Weg vom Passwort
  hin zu kryptographischer Hardware
- Rückwirkungsfreie Trennung
- Erreichbarkeit schaffen:
  CNA, security.txt