PEPPERL+FUCHS

Umgang mit Schwachstellenmeldungen

Vorteile durch CERT@VDE

PEPPERL+FUCHS

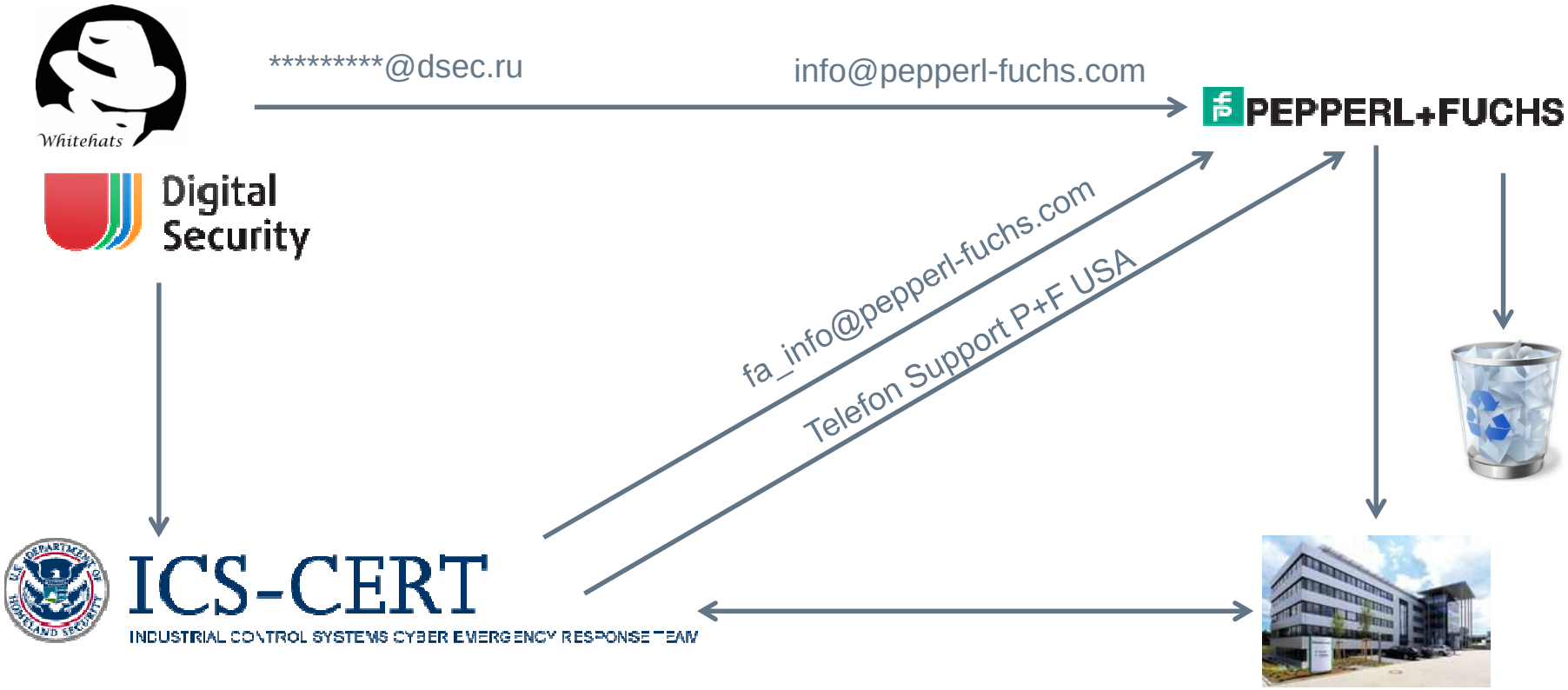
HART DTM Schwachstelle

Wie alles begann

- Alexander Bolshev begann 2013 mit “security research” im Bereich FDT/DTM
- „Some hat“ Entwickler der russischen Digital Security Research Group
- Es wurden XML injection errors in verschiedenen DTMs entdeckt
- Durchführung von Fuzz Tests für HART Telegramme an DTMs in 2014
- Dabei wurde eine fehlerhafte Eingabeüberprüfung in einer weit verbreiteten HART Device Type Manager (DTM) Bibliothek entdeckt

HART DTM Schwachstelle

Kontakt Rekonstruktion



PEPPERL+FUCHS

HART DTM Schwachstelle

Behebung der Schwachstelle

- Koordination mit ICS-CERT (DHS)
  - Absprache über die Verfügbarkeit eines Software Patches und Veröffentlichung der Informationen
- Fehlerbehebung und Freigabe der Software
- Freigabe der Informationen für die Öffentlichkeit

PEPPERL+FUCHS

HART DTM Schwachstelle

Gewonnene Erkenntnisse

2.2. Reaktion auf Schwachstellen

Jeder Hersteller sollte auf die Entdeckung einer Schwachstelle in einer seiner Komponenten nach der Freigabe und dem Verkauf vorbereitet sein. Schwachstellen werden regelmäßig entdeckt, da fehlerhafte Implementierungen von Soft- und Hardware nicht ungewöhnlich sind. Je nach Art der Schwachstelle unterscheiden sich die Auswirkungen. Grundsätzlich sollte jedoch jede Art von Fehler beseitigt werden, soweit dies aus Kosten-/Nutzen-Aspekten vertretbar ist. Im Einzelfall kann auch die Empfehlung des Umstiegs auf eine neue Produktversion oder ein Nachfolgeprodukt geeignet sein. Hierbei sollte trotzdem ein Workaround vorgeschlagen werden, so dass Bestandskunden nicht völlig schutzlos sind.

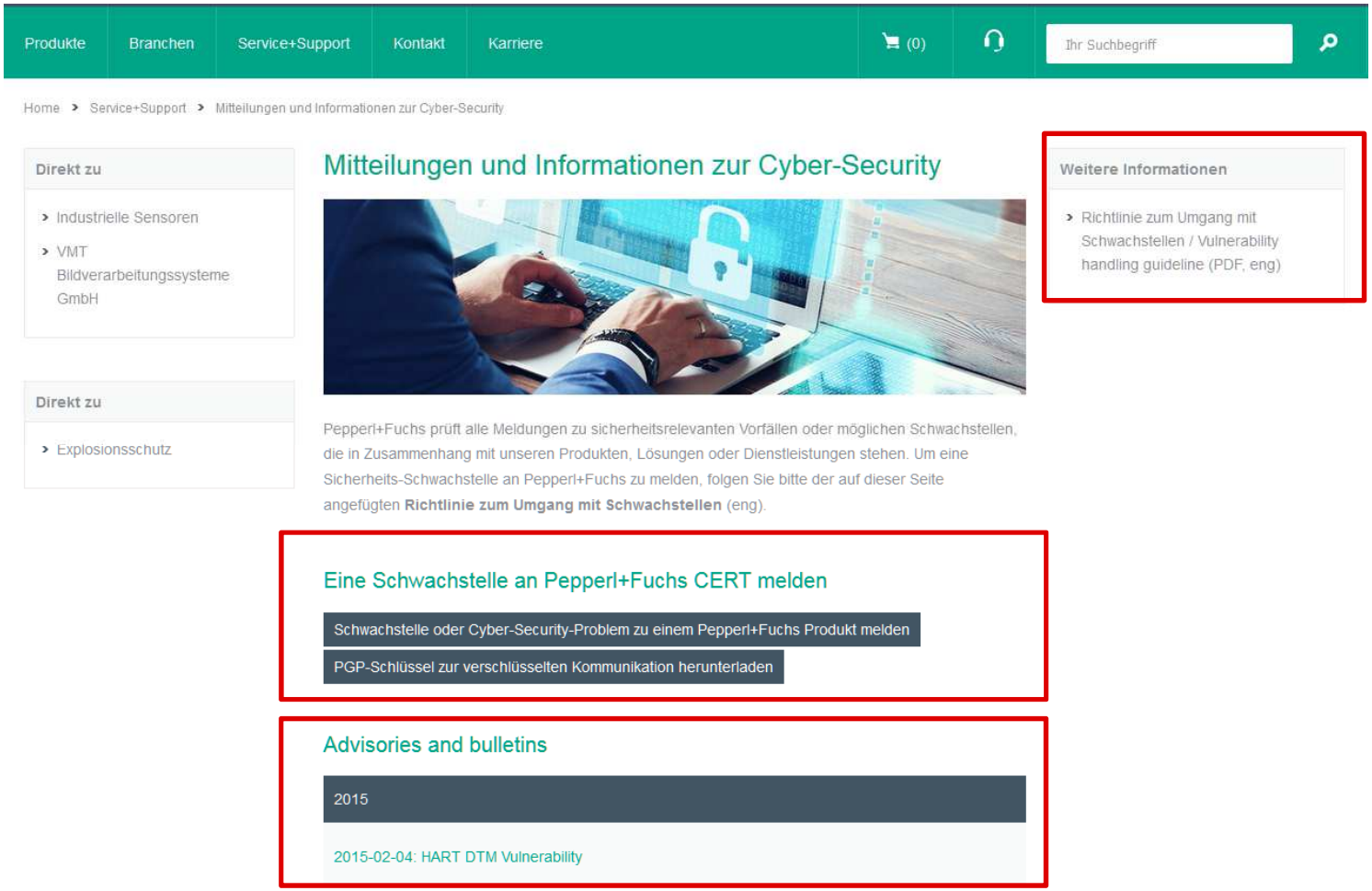
M 9 Zentrale Kontaktmöglichkeit für Schwachstellenmeldungen

Es sollte eine zentrale und vertrauliche Möglichkeit zur Kontaktaufnahme beim Hersteller vorhanden sein, über die Schwachstellen gemeldet werden können. Die Kommunikation der Informationen zu der Schwachstelle an den Hersteller sollte zudem verschlüsselt erfolgen, da es sich um vertrauliche Daten handelt. Dazu kann ein öffentlicher Schlüssel in einem Verzeichnisdienst oder auf der Webseite hinterlegt werden.

Neben der Möglichkeit Kontakt mit dem Hersteller aufzunehmen, sollte ebenfalls eine zeitnahe Rückmeldung des Herstellers erfolgen. Diese sollte eine Bewertung der Schwachstelle und ggf. das weitere Vorgehen enthalten.

HART DTM Schwachstelle

Gewonnene Erkenntnisse



PEPPERL+FUCHS

Umgang mit Schwachstellenmeldungen

Vorteile durch CERT@VDE

- Zentrale Anlaufstelle für Betreiber, Integratoren und Hersteller
- Bereitstellen und betreiben der Kontaktinfrastruktur
- Zentrale Know-How Stelle zum Umgang mit Schwachstellen
- Etablierung der notwendigen Prozesse
- Koordination von Schwachstellenmeldungen zwischen verschiedenen Parteien
- Informationsvorsprung durch firmenübergreifenden Austausch über Sicherheitsprobleme

PEPPERL+FUCHS

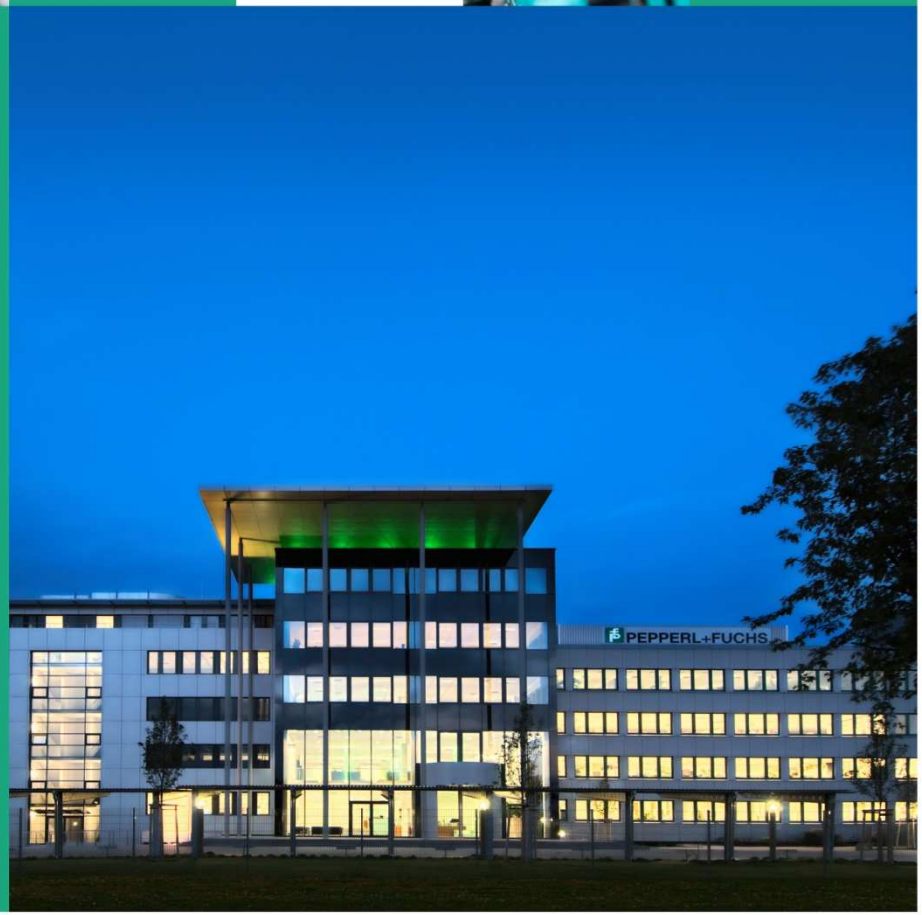
Umgang mit Schwachstellenmeldungen

Vorteile durch „Marke“ CERT@VDE

Ein Versprechen zum Umgang mit Schwachstellen als Grundlage von Vertrauen:

- Firmenübergreifende Prozesse und Vorgehensmethoden
- Zeitgerechte Bearbeitung von Schwachstellen
- Responsible disclosure policy
- Vertrauensvolle Datenbasis über Schwachstellen

Thank you



PEPPERL+FUCHS