CERT@VDE

VDE Workshop

Andreas Harner, VDE Kompetenzzentrum Informationssicherheit

Hannover-Messe, 27.04.2017

Agenda

Vorstellung CERT@VDE
Ansgar Hinz, VDE Vorstandsvorsitzender

Andreas Harner, VDE Kompetenzzentrum Informationssicherheit

Schwachstellen im Umfeld von Prozess-IT
Dr. Kai Lorentz, Leiter der Business Unit Electronics, Weidmüller Interface GmbH & Co. KG

Umgang mit Schwachstellenmeldungen – Vorteile durch CERT@VDE
Jens Schmidt, Team Leader–Fieldbus Technology, Pepperl+Fuchs GmbH

Michael Kessler, Exec. Vice President Components+Technology, P+F GmbH

Vertrauensvolle Behandlung – Auf kurzem Weg zwischen Anbietern und Anwendern
Dr. Lutz Jänicke, Product & Solution Security Officer, Phoenix Contact GmbH & Co. KG

Noch ein CERT! Warum?
Prof. Dr. Klaus-Peter Kossakowski, DFN-CERT Services GmbH

Agenda – II.

Anschließend:

Offene Diskussion mit den Podiumsteilnehmern
Moderation: Prof. Dr. Kossakowski, Andreas Harner

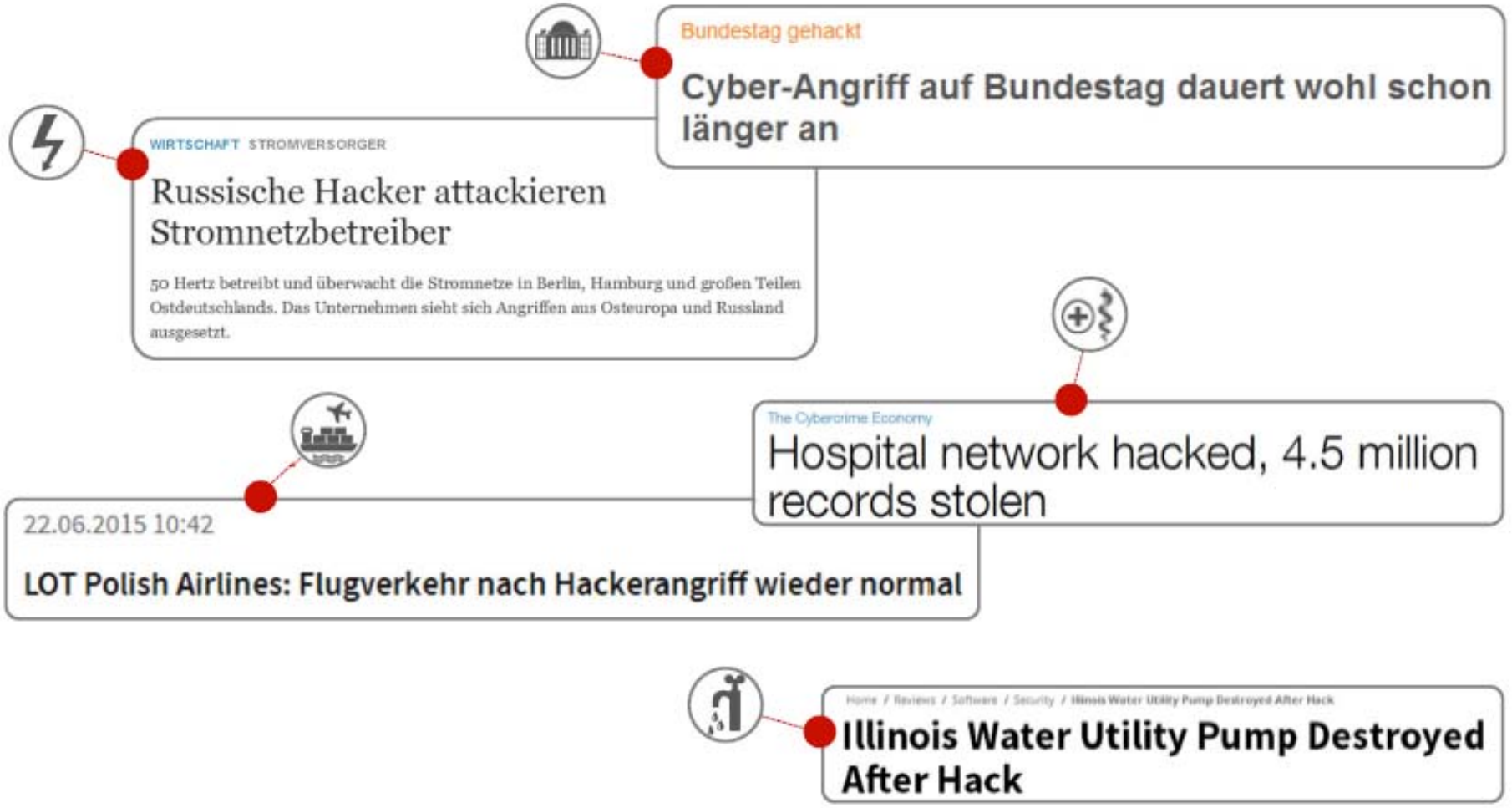
Abschluss und Gelegenheit zum bilateralen Austausch

Vorstellung CERT@VDE

Andreas Harner, VDE Kompetenzzentrum Informationssicherheit

Hannover, 27.04.2017

Cybersicherheit: … haben wir ein Problem?
… es gibt doch Standardlösungen?



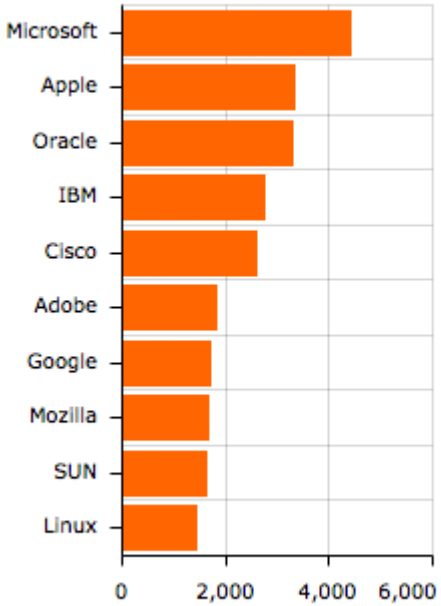
… Standardlösungen:

(Quelle:
Steffen Heyde, Secunet)

Problem: Vereinzelte 08/15-Internet-Sicherheitslösungen sind in kritischen Bereichen nicht wirklich geeignet.

Problemumfeld

Allzeit Top-10 Anbieter mit Sicherheitslücken:



Quelle: www.cvedetails.com

2799 Sicherheitslücken wurden dieses Jahr alleine in den Top 50 der meist verwendeten Softwareprodukte verifiziert – nahezu alle namhaften Anbieter haben ihren festen Platz in dieser wenig ruhmreichen Liste.

2 bis **4** Wochen dauert es, bis **Hacker 50%** der Sicherheitslücken in Software-Updates geknackt haben.

40 bis **120** Tage brauchen Hacker, um **90%** der Sicherheitslücken auszunutzen.

120 Tage benötigen Unternehmen im Schnitt, um die Sicherheitslücken mit den Hersteller-Patches zu schließen!

Professionelles Patch-Management ist essentiell für den Datenschutz und die IT-Sicherheit von Unternehmen.

… Lücken werden spät/gar nicht erkannt und zu spät geschlossen!

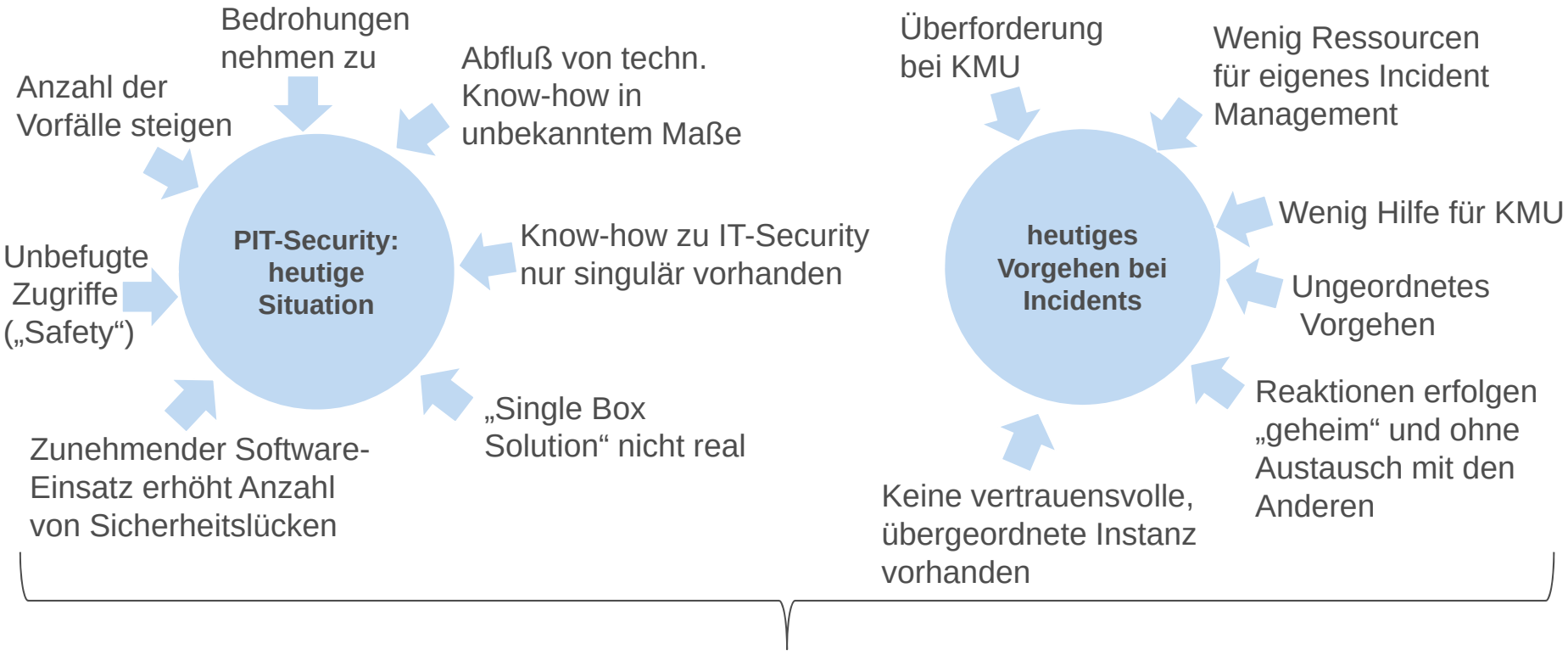
Problemumfeld – II.

… Schwachstellen bringen Geld!

Es gab im November 2014 Hinweise darauf, dass der BND Zero-Day-Exploits ankaufen möchte, um SSL-Verschlüsselungen abzuhören. Voll funktionsfähige Zero-Day-Exploits von noch unbekannten Schwachstellen würden, laut Schätzungen von **bis zu 100.000 Dollar** kosten, wenn sie sich in weit verbreiteter Software, wie Internet Explorer, Flash, Android oder iOS befänden. Es wird vermutet, dass für den Ankauf (unter dem Codenamen „Swop“) im Jahr 2015 bis zu 4,5 Mio. Euro bereitgestellt werden. Dies würde den Schwarzmarkt zusätzlich anheizen und wird deshalb kritisiert.

Nach Erkenntnissen des Nachrichtenmagazins Der Spiegel und der Süddeutschen Zeitung hat der Bundesnachrichtendienst (BND) eine "Strategische Initiative Technik" (SIT) begonnen, um "auf Augenhöhe mit führenden westlichen Nachrichtendiensten" kooperieren zu können. Für die Vorbereitung von SIT sollen noch in diesem Jahr 6,22 Millionen Euro ausgegeben werden, nächstes Jahr dann 28 Millionen. Insgesamt sollen bis 2020 rund **300 Millionen Euro** in die technische Aufrüstung investiert werden. Für diese Summe sollen **unter anderem Softwareschwachstellen** eingekauft und beispielsweise verdeckte Netzzugänge finanziert werden.

Ausgangslage im Bereich der Prozess-IT (PIT)



FOLGEN

- Level der Security sinkt mit zunehmender Vernetzung („Industrie 4.0“)
- Ressourcenverschwendung und Innovationsverlust
- IT-Sicherheitslage nicht einschätzbar: „Was bringt eine Maßnahme?“

➡ Es gibt ein klares Informationsdefizit bezüglich PIT-Security!

➡ Notwendigkeit eines **CERT@VDE**

Initiatoren für ein CERT@VDE: Computer Emergency Response Team for Automation Industry

Die Idee für ein CERT@VDE wurde in Gremien der DKE|VDE initiiert und in einem ersten Workshop am Anfang 2016 konkretisiert.

BECKHOFF

PEPPERL+FUCHS

Weidmüller

PHOENIX CONTACT
INSPIRING INNOVATIONS

Endress+Hauser

SIEMENS

Warum VDE?

Idee einer *vertrauenswürdigen* Ingenieurs-Kontaktstelle bei einer neutralen Instanz mit hoher Reputation:

VDE Verband der Elektrotechnik Elektronik Informationstechnik e.V.

… steht für Innovation und Sicherheit in der Elektro- und Informationstechnik

… ist ein gemeinnütziger technisch-wissenschaftlicher Verband

Vorgehensweise

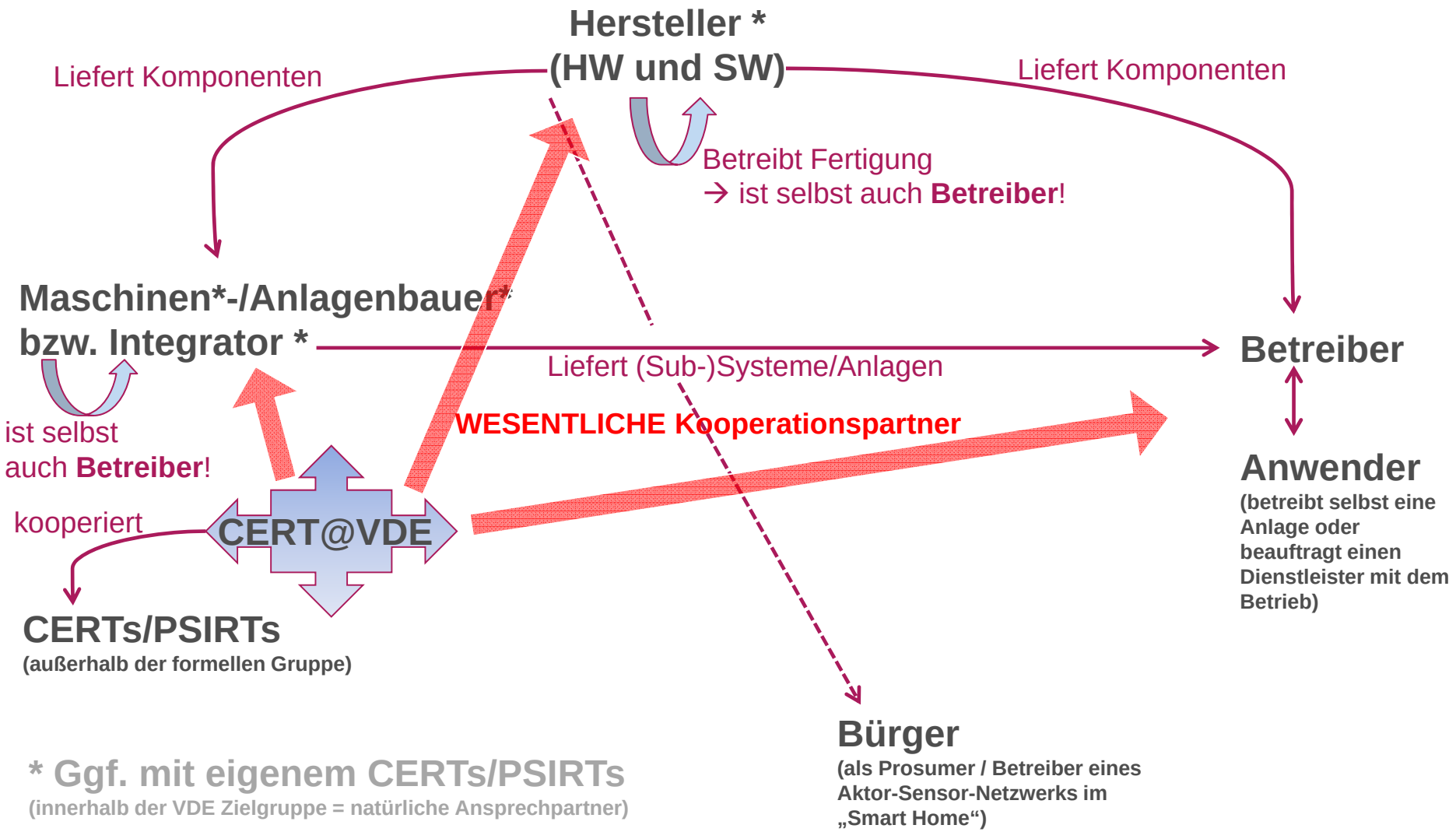
Anforderung:
Umsetzung eines CERT@VDE

Beschreibung der Aufgaben und Dienstleistungen eines CERT@VDE (Abgrenzungen gegenüber anderen Ausprägungen)

→ **Beschreibung der spezifischen Handlungsoptionen, die sich für den CERT-Aufbau für den VDE ergeben**

→ **Beschreibung der Maßnahmen zur Risikominimierung**

Zielgruppenrelevante Rollen für ein CERT@VDE



*** Ggf. mit eigenem CERTs/PSIRTs**
(innerhalb der VDE Zielgruppe = natürliche Ansprechpartner)

WERTE- UND NUTZEN-VERSPRECHEN - 1

Kategorie	Mit Aufnahme des Betriebs	Späterer Einstieg
Präventiv	▪ Verteilung von Produktsicherheits-informationen (aus der formellen Zielgruppe an Dritte) ▪ Verteilung von Produktsicherheits-informationen (von Dritten an die Unternehmen der formellen Zielgruppe) ▪ Verfügbarkeit eines Frühwarnsystems (Informations-managementsystem auf Textbasis)	▪ Allgemeine Anfragen mit PSIRT-Relevanz

WERTE- UND NUTZEN-VERSPRECHEN - 2

Kategorie	Mit Aufnahme des Betriebs	Späterer Einstieg
Reaktiv	▪ Betrieb einer Kontaktstelle ▪ Koordinierende Unterstützung bei der Bewältigung von Sicherheitslücken	▪ Quantitative und qualitative Auswertungen für Zielgruppe (Fallstudien/ Lagebilder)
Weitere Aufgaben	▪ Expertengruppe ▪ Außenvertretung ▪ Innenvertretung	▪ Unterstützung der Bewusstseinsbildung ▪ Allgemeine Fallstudien bzw. Lagebild-einschätzungen ▪ Beiträge zur Standardisierung

Mehrwerte durch CERT@VDE:

- ***Firmenübergreifender Austausch zu Sicherheitsproblemen in geschützten Interaktionsräumen***
  des CERT@VDE: d.h. Konkurrenten diskutieren ähnliche/gleiche Probleme und deren Lösung gemeinsam und (bei Bedarf) anonymisiert

- ***Firmenübergreifendes voneinander Lernen:***
  Wie geht die Konkurrenz mit Cybersecurity Problemen um? … man spricht beim CERT@VDE darüber!

- ***„Marktdifferenzierung durch Wissensvorsprung“***
  Wissen kommt vom CERT@VDE, aus der (inter-)nationalen CERT-Community, von Dienstleistern und aus öffentlichen Quellen die im CERT@VDE gebündelt werden

- Mitglieder gelangen zu ***schnelleren Einschätzungen bei Vorfällen*** und betreiben somit eine effektive Schadensbegrenzung

- Eine frühe Mitgliedschaft ermöglicht ***Mitgestaltungsmöglichkeiten beim Aufbau des CERT@VDE*** und seinen Prozessen → KMU sind dadurch früher und besser vorbereitet → Wettbewerbsvorteil

- Mitgliedschaft im CERT@VDE bietet ***Wettbewerbsvorteil*** und verhindert
  - Produktionsausfälle
  - Know-how Abfluss
  - IT-Security-Vorfälle

- **KMU im Wettbewerb mit den Großen der Branche … und die haben eigene Produkt-CERTs (PSIRTs)**
  … machen Sie mit bei CERT@VDE!

CERT@VDE- Kontakte

Telefon	+49 69 6308 400
Email	info@cert.vde.com
PGP-Key	4096R/C3E3E8AD
PGP-Fingerprint	F5F7 FFB6 32D9 EAC7 1E74 F344 0CF5 E79A C3E3 E8AD

https://cert.vde.com

CERT@VDE
Andreas Harner
Telefon: +49 69 6308-392
andreas.harner@vde.com
Stresemannallee 15
60596 Frankfurt am Main
www.vde.com

Vielen Dank für Ihre Aufmerksamkeit

VDE CERT

Ihr Ansprechpartner:

Dipl.-Ing. Andreas Harner
DKE Deutsche Kommission Elektrotechnik
Elektronik Informationstechnik im DIN und VDE

Phone: +49 69 6308 392
andreas.harner@vde.com