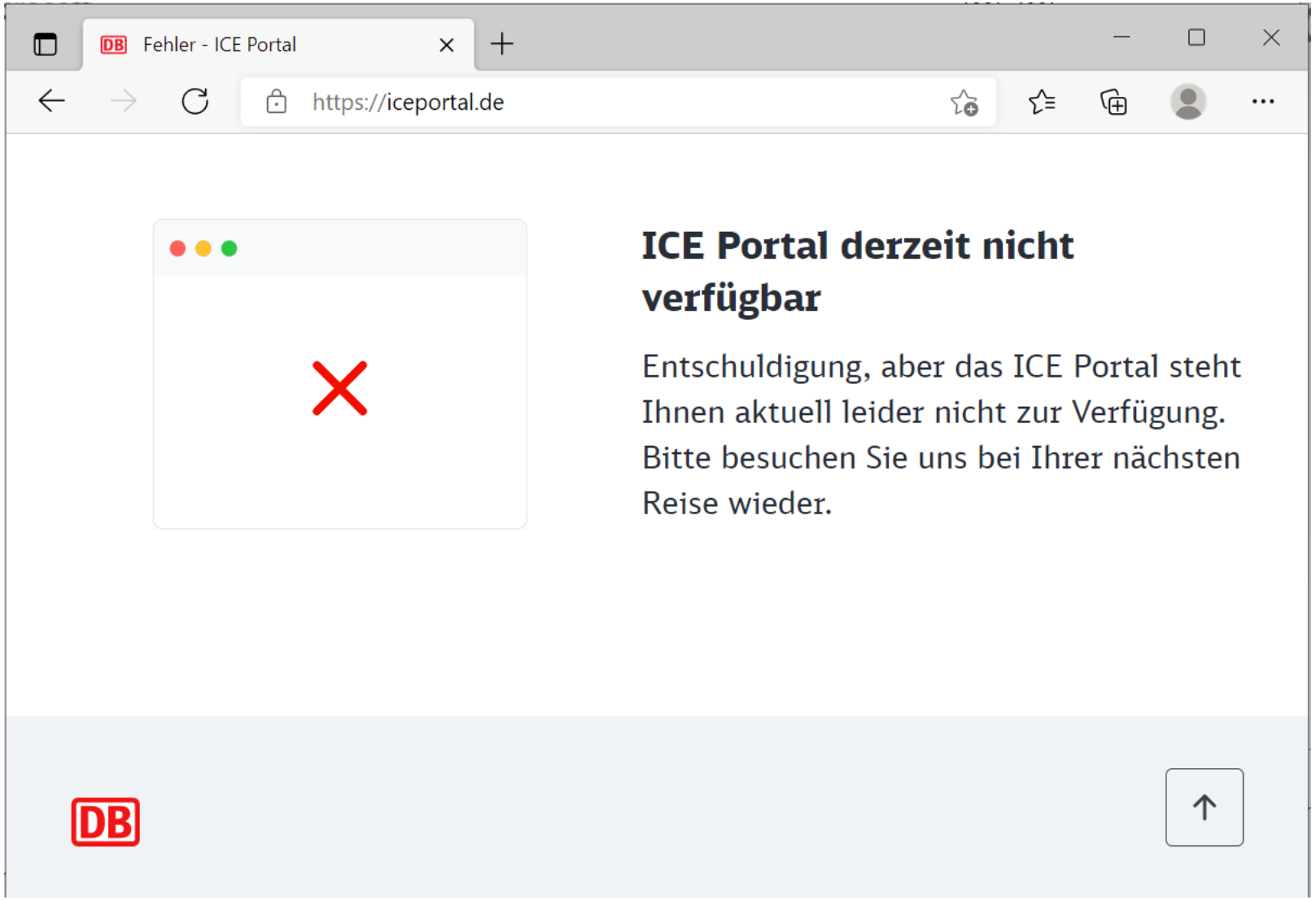
Mit dem „Digitalen Ersthelfer“ besser auf IT-Vorfälle reagieren – Nutzen und Chancen

T.I.S.P. Community Meeting 2022, Berlin/Köln (Remote) – 09.11.2022


Fehler - ICE Portal
https://iceportal.de
ICE Portal derzeit nicht verfügbar
Entschuldigung, aber das ICE Portal steht Ihnen aktuell leider nicht zur Verfügung. Bitte besuchen Sie uns bei Ihrer nächsten Reise wieder.

DigiTrace
Kompetenz in IT-Forensik

Automatisches Speichern | Incident Response und Forensi... | Martin Wundram MW

Datei Start Einfügen Zeichnen Entwurf Übergänge Animationen Bildschirmpräsentation Überprüfen Ansicht Hilfe | Teilen | Kommentare

1 protekt 12. – 13.11.2019 Leipzig
Incident Response und Forensic Readiness: Im IT-Ernstfall gut vorbereitet sein und richtig handeln

2

Leider haben wir vorübergehende Serverprobleme.

Wiederholen Abbrechen

LEIPZIGER MESSE

Leider haben wir vorübergehende Serverprobleme.

Wiederholen Abbrechen

Klicken Sie, um Notizen hinzuzufügen

Folie 1 von 77 | Notizen | 73 %

Digitaler Ersthelfer | Dipl. Wirt.-Ir

Wir schätzen Ihr Feedback an Microsoft. Gibt es etwas, das wir besser machen können?

Nehmen Sie bitte keine vertraulichen oder personenbezogenen Informationen in Ihren Kommentar auf.

☐ Screenshot einschließen

Die Screenshotfunktion wurde von Ihrem Administrator deaktiviert, oder sie ist nicht verfügbar, weil vertrauliche Informationen in einer Office-Anwendung geöffnet sind.

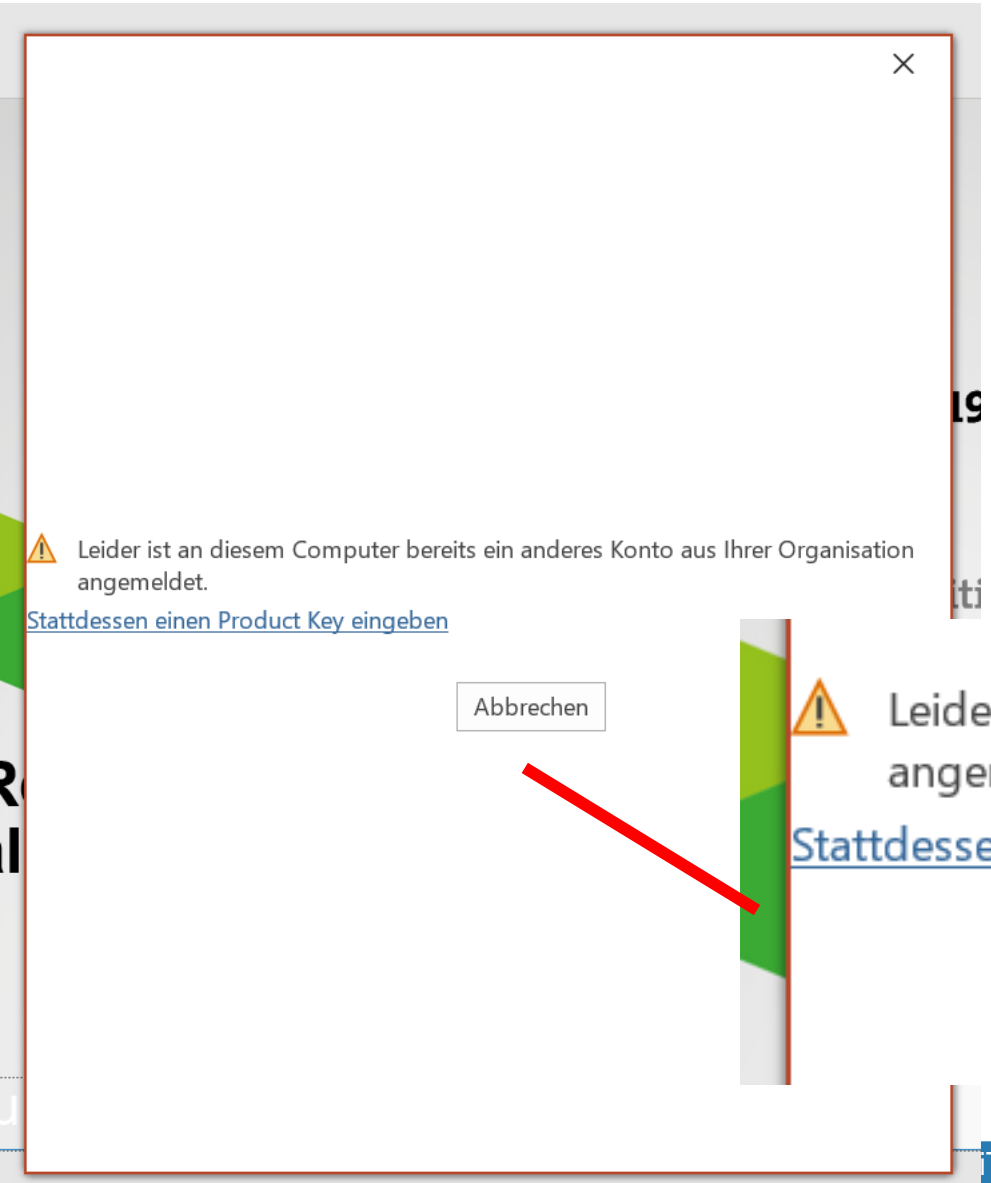
Ihre Organisation verwaltet Ihre Datenschutzeinstellungen und hat der Erfassung von optionalen Diagnosedaten zugestimmt, deshalb werden wir Diagnoseprotokolle für die Problembehandlung einschließen.

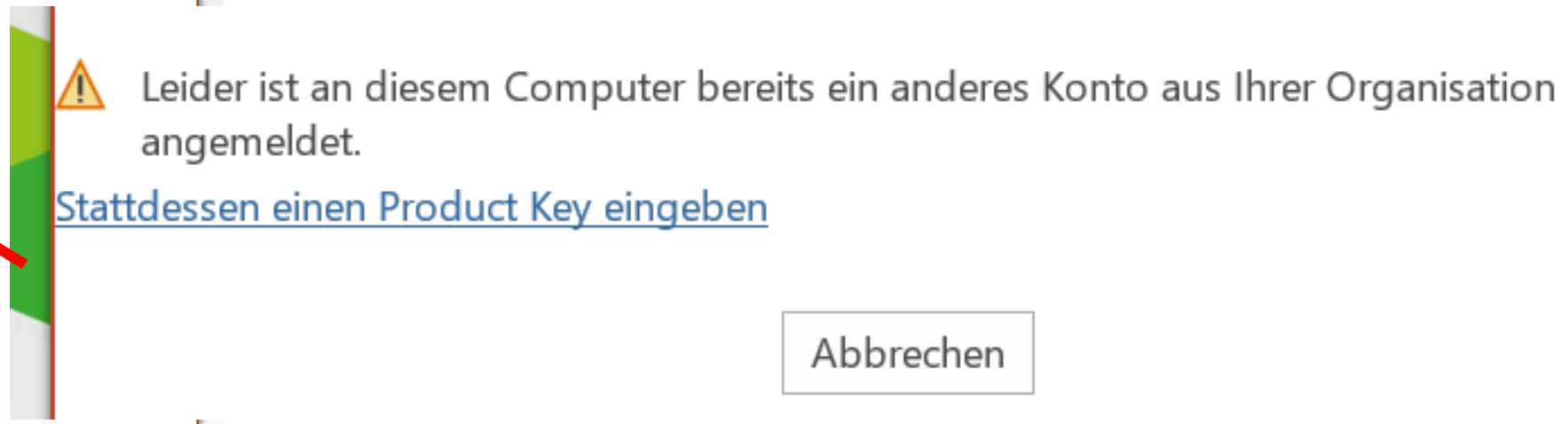
Weitere Informationen

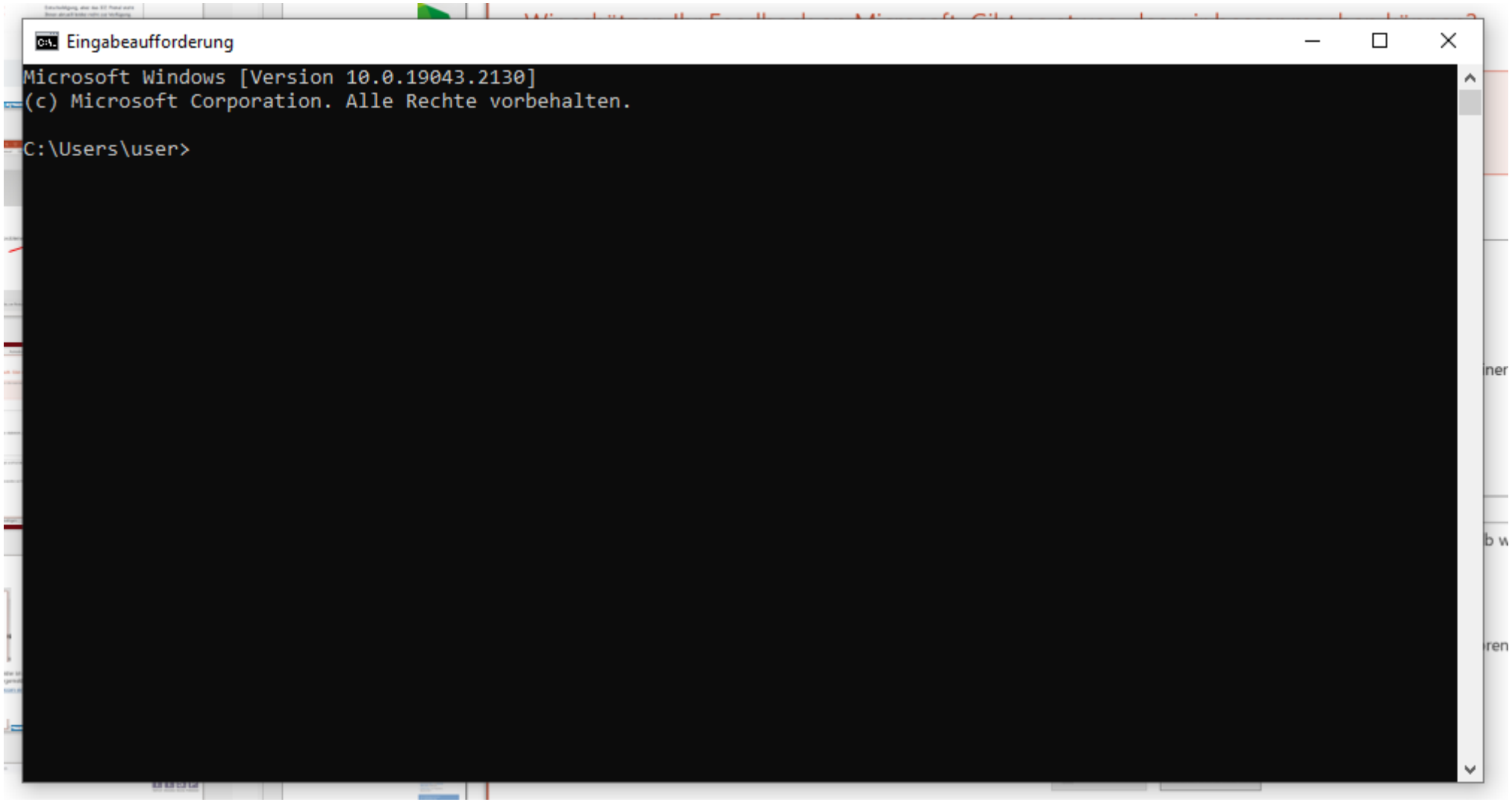
Wenn Sie auf "Absenden" klicken, wird Ihr Feedback verwendet, um Microsoft-Produkte und -Dienste zu verbessern. IT-Administratoren Ihrer Organisation können Ihre Feedbackdaten anzeigen und verwalten.

Datenschutzbestimmungen

Absenden Abbrechen


Leider ist an diesem Computer bereits ein anderes Konto aus Ihrer Organisation angemeldet.
Stattdessen einen Product Key eingeben
Abbrechen


Leider ist an diesem Computer bereits ein anderes Konto aus Ihrer Organisation angemeldet.
Stattdessen einen Product Key eingeben
Abbrechen


Eingabeaufforderung
Microsoft Windows [Version 10.0.19043.2130]
(c) Microsoft Corporation. Alle Rechte vorbehalten.
C:\Users\user>

heise online › News › 05/2022 › App "FairEmail" aus dem Google Play Store entfernt

App "FairEmail" aus dem Google Play Store entfernt

Die App "FairEmail" ist nicht mehr im Google Play Store verfügbar, der Entwickler erklärte das Projekt für beendet. Die App bleibt aber weiterhin nutzbar.

Lesezeit: 2 Min. In Pocket speichern 194

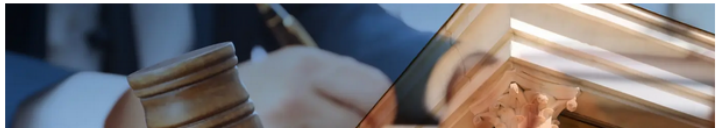
TOPTHEMEN: EXCHANGE BITCOIN AMAZON CORONA E-AUTO PODCASTS ANZEIGE: SECURITYHL

heise online › News › 04/2021 › DroidScript von Google-Algorithmen willkürlich aus dem Play Store…

DroidScript von Google-Algorithmen willkürlich aus dem Play Store ausgeschlossen

KI dürfte den offenbar irrtümlichen Ausschluss veranlasst haben. Google schweigt und gerät in Kritik wegen des intransparenten Durchsetzens von Store Policies.

Lesezeit: 2 Min. In Pocket speichern 104



https://www.heise.de/news/Terraria-Stadia-Version-nach-Bann-von-Google-Accou

IT Wissen Mobiles Security Developer Entertainment Netzpolitik Wirtschaft

TOPTHEMEN: EXCHANGE BITCOIN AMAZON CORONA E-AUTO PODCASTS

heise online › News › 02/2021 › "Terraria": Stadia-Version nach Bann von Google-Account vor dem Aus

"Terraria": Stadia-Version nach Bann von Google-Account vor dem Aus

Die Entwickler des Spiels "Terraria" erheben schwere Vorwürfe gegen Google: Ihr Google-Account sei ohne Begründung gesperrt worden. Nun gibt es Konsequenzen.

Lesezeit: 2 Min. In Pocket speichern 168

https://netzpolitik.org/2022/falscher-verdacht-gegen-vater-ein-fall-aus-den-usa-zeigt-die-gefahr-der-geplanten-chatkontrol

Suchen… NETZPOLITIK.ORG

Ob Chatkontrolle oder Staatstrojaner - mit deiner Hilfe bleiben wir dran. Jetzt spenden

Falscher Verdacht gegen Vater

Ein Fall aus den USA zeigt die Gefahr der geplanten Chatkontrolle

Ein Vater fotografiert den Genitalbereich seines kleinen Sohnes für den Kinderarzt – plötzlich wird sein Google-Account gesperrt. Die automatische Bilderkennung hatte falschen Alarm ausgelöst. Für die geplante Chatkontrolle lässt das wenig Gutes erwarten.

(Bild: R

24.08.2022 um 17:52 Uhr - Markus Reuter, Sebastian Meineck - in Überwachung - 17 Ergänzungen

09.02.2

Von Daniel Herbig

Vorstellung von und Arbeit mit Fallbeispielen

BSI: Alarmstufe Rot -> Exchange/Hafnium im März 2021

- BSI meldet wiederholt (verschiedene Medienkanäle)
- Kunden erkennen Ernst der Lage, manche melden sich präventiv
- BSI / Microsoft stellen Detektierungsmöglichkeiten bereit
- „Regelbetrieb nicht mehr aufrecht erhaltbar“ → das gilt auch bei den IT-Sicherheitsdienstleistern

Vorstellung von und Arbeit mit Fallbeispielen

In drei einfachen Schritten zur Katastrophe

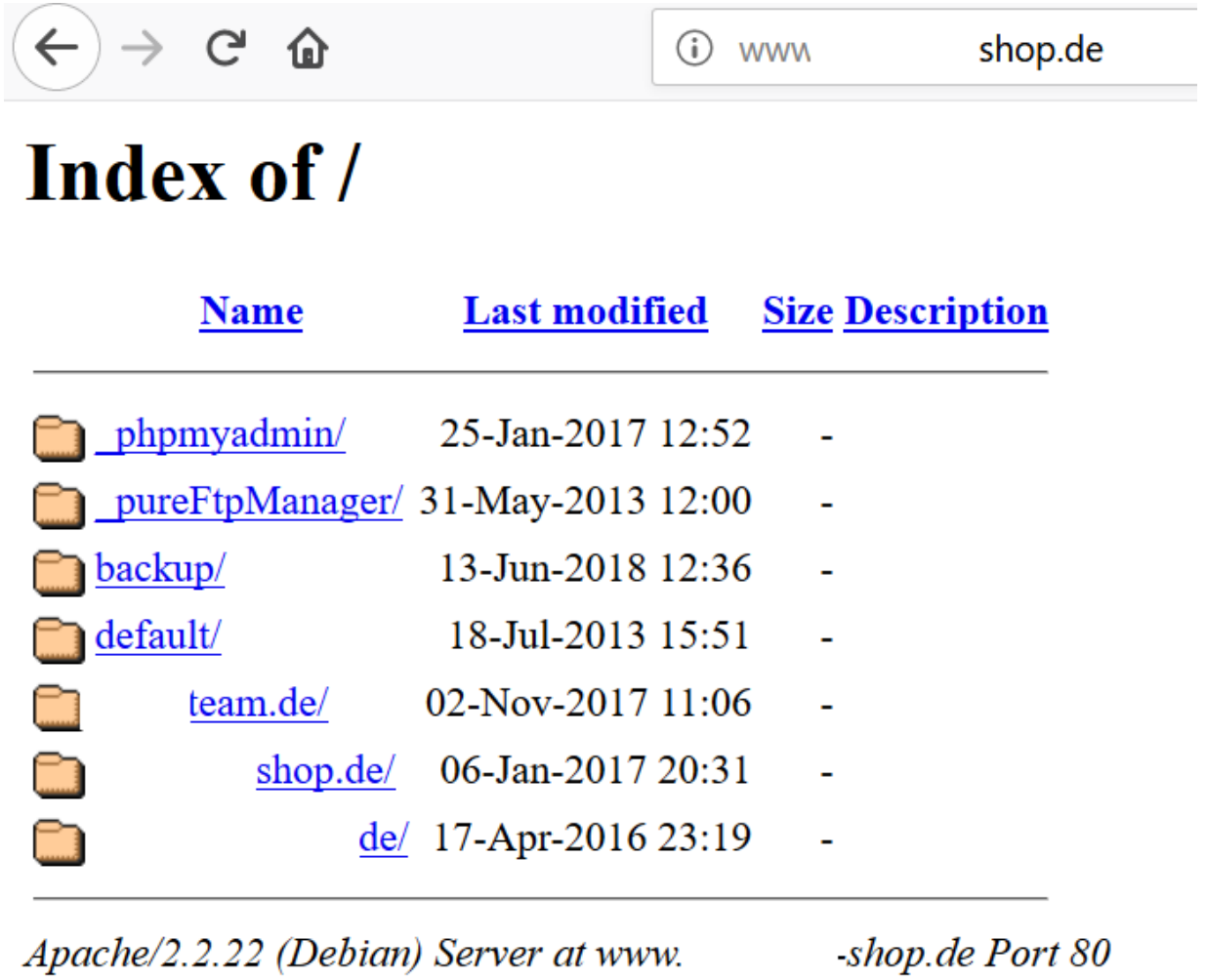
1. Alltäglicher Defekt an einem wichtigen Server inkl. Datenverlust
2. Das Backup wurde falsch konfiguriert – es wurde täglich nur ein leerer Ordner gesichert…
3. Aufgrund eines bestehenden Versicherungsschutzes wurde eine extrem teure Datenrettung beauftragt (x00.000 EUR)

Ergebnis:

- Versicherung möchte nicht zahlen (verständlich)
- Dienstleister wird in Regress genommen (x00.000 EUR, verständlich)
- Dienstleister ist insolvent

Vorstellung von und Arbeit mit Fallbeispielen

Jämmerlicher Umgang mit Meldungen von Dritten



Vorstellung von und Arbeit mit Fallbeispielen

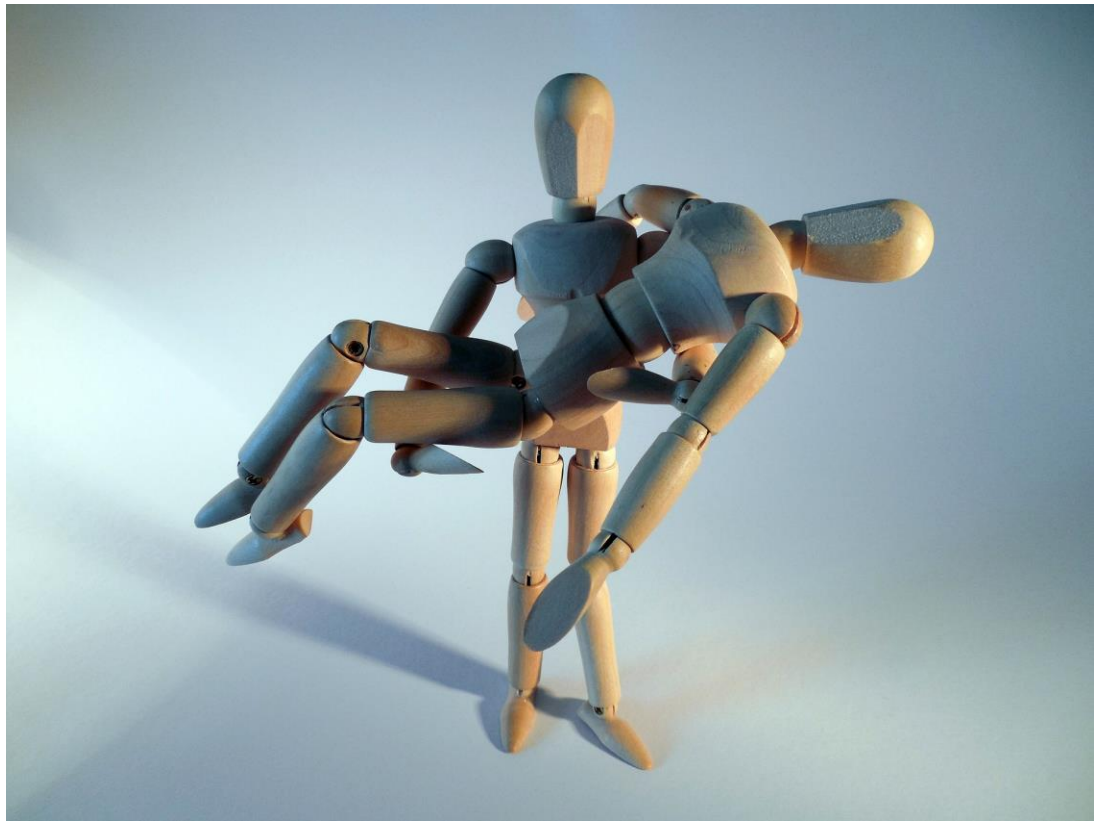
Schon erfahren und doch noch nicht routiniert

- Unternehmensgruppe, vierstellige Zahl an Mitarbeitern
- Vor wenigen Jahren von kapitalem IT-Sicherheitsvorfall betroffen (Ransomware)
- Aktuell: „CEO Fraud“ in/gegen M365-E-Mail-Konten
- Zwei betroffene Konten? Drei? Geld abgeflossen oder nicht? …
  - Mangel an strukturierter Doku

Vorstellung von/Arbeit mit Fallbeispielen

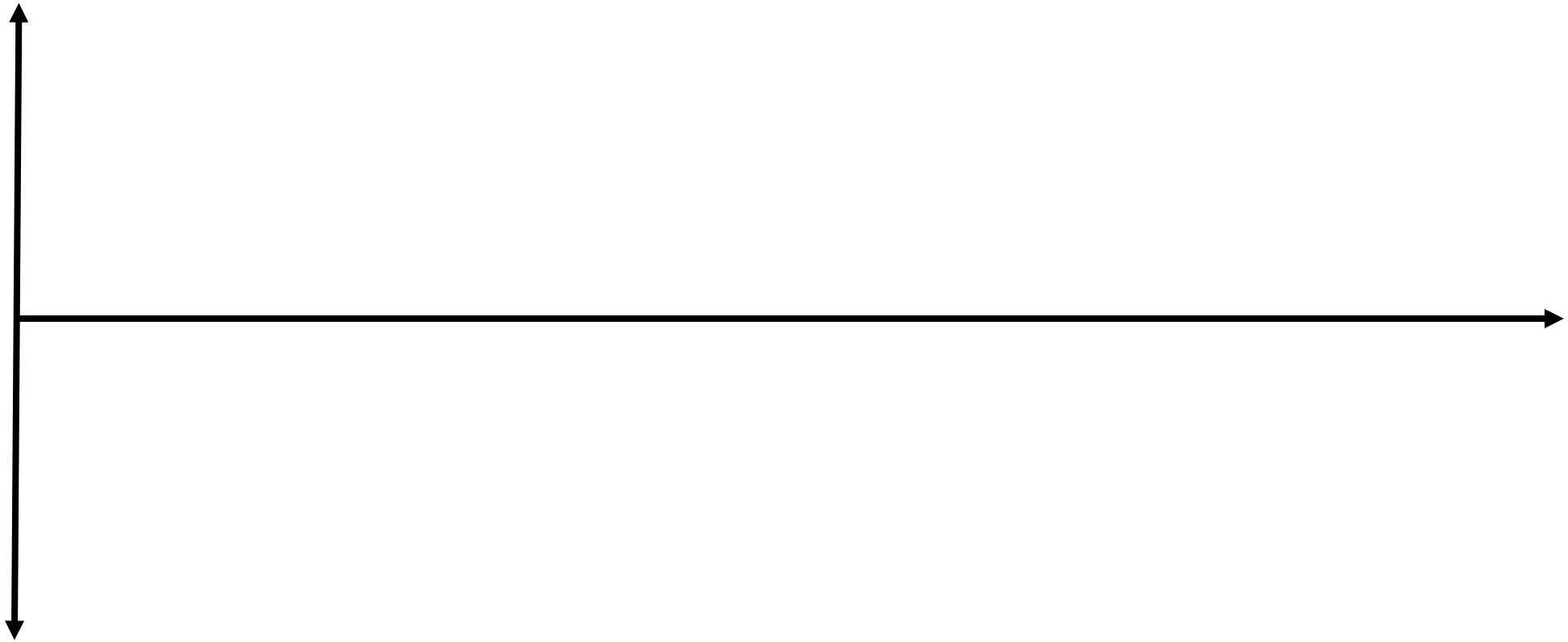
Der Digitale Ersthelfer im Einsatz

- Ein Kollege in der HR-Abteilung öffnet aus Versehen den Anhang einer „Bewerbung“. *Dateien.zip.exe* haben wohl keine Bewerbungsdateien ergeben, sondern eine schwarze Dosbox…
- Da eine Abteilungskollegin Digitale Ersthelferin ist, spricht er sie an
- Sie hört sich die Situation und den Ablauf an, lässt sich die E-Mail zeigen und wertet dies dann als möglichen Sicherheitsvorfall
- Sie zieht das Netzwerkkabel, beruhigt den Kollegen, bittet ihn, den PC ab sofort nicht mehr zu benutzen und zieht die internen IT-Experten hinzu
- Diese stellen fest, dass der Rechner tatsächlich kompromittiert ist und mit einer Schadfunktion ausgestattet ist, die versucht, im Ethernet übertragene Passwörter auszuspähen
- Der Vorfall wurde frühestmöglich gestoppt!



Vorstellung von und Arbeit mit Fallbeispielen

(Gefühlte) Kontrolle über einen Vorfall im Laufe der Zeit, kritische Punkte



Konzeptvorstellung „Digitaler Ersthelfer“

Die Rolle des „Digitalen Ersthelfers“

- Typisches Profil: IT-Laie, IT-erfahren oder sogar IT-Experte, aber kein Experte für IT-Forensik und Incident Response
- Wichtigste Tätigkeiten:
  - IT Incidents bemerken und erste Schritte einleiten
  - Erhalten und je nach Situation, Ausrüstung und Erfahrung auch Sichern digitaler Beweismittel
  - Hinzuziehung von IT-Forensikern koordinieren
- Je nach konkreter Rollenbeschreibung:
  - Fall abgeben an IT-Forensiker, oder
  - Fall koordinieren und als Bindeglied zwischen Unternehmen und beauftragtem IT-Forensiker fungieren
  - Einfache Fälle auch selbst abschließend bearbeiten

Konzeptvorstellung „Digitaler Ersthelfer“

Achtung 1

- Der Digitale Ersthelfer ist nicht explizit gesetzlich verankert/geregelt
- Es handelt sich um ein neues/“freiwilliges“ Konzept

Konzeptvorstellung „Digitaler Ersthelfer“

Die Rolle des Digitalen Ersthelfers

- Digitaler Ersthelfer (DE):
  - Eine Person, die im Bereich „digital“ (IT) im Ernstfall „erste Hilfe“ leistet.
- Wer kommt als DE in Frage:
  - Sowohl IT-Laien als auch IT-Experten (z.B. Fachinformatiker, Informatiker oder langjährig Berufserfahrene)
  - Sie füllen diese Rolle dann mit ihrer jeweiligen Erfahrung und Qualifikation aus.
- Sorgt dafür, dass das, was „menschenmöglich“ und zugleich notwendig ist, bis Experten für Incident Response und IT-Forensik (oder je nach Fall auch „normale“ IT-Experten) eintreffen und übernehmen, gemacht wird.

Konzeptvorstellung „Digitaler Ersthelfer“

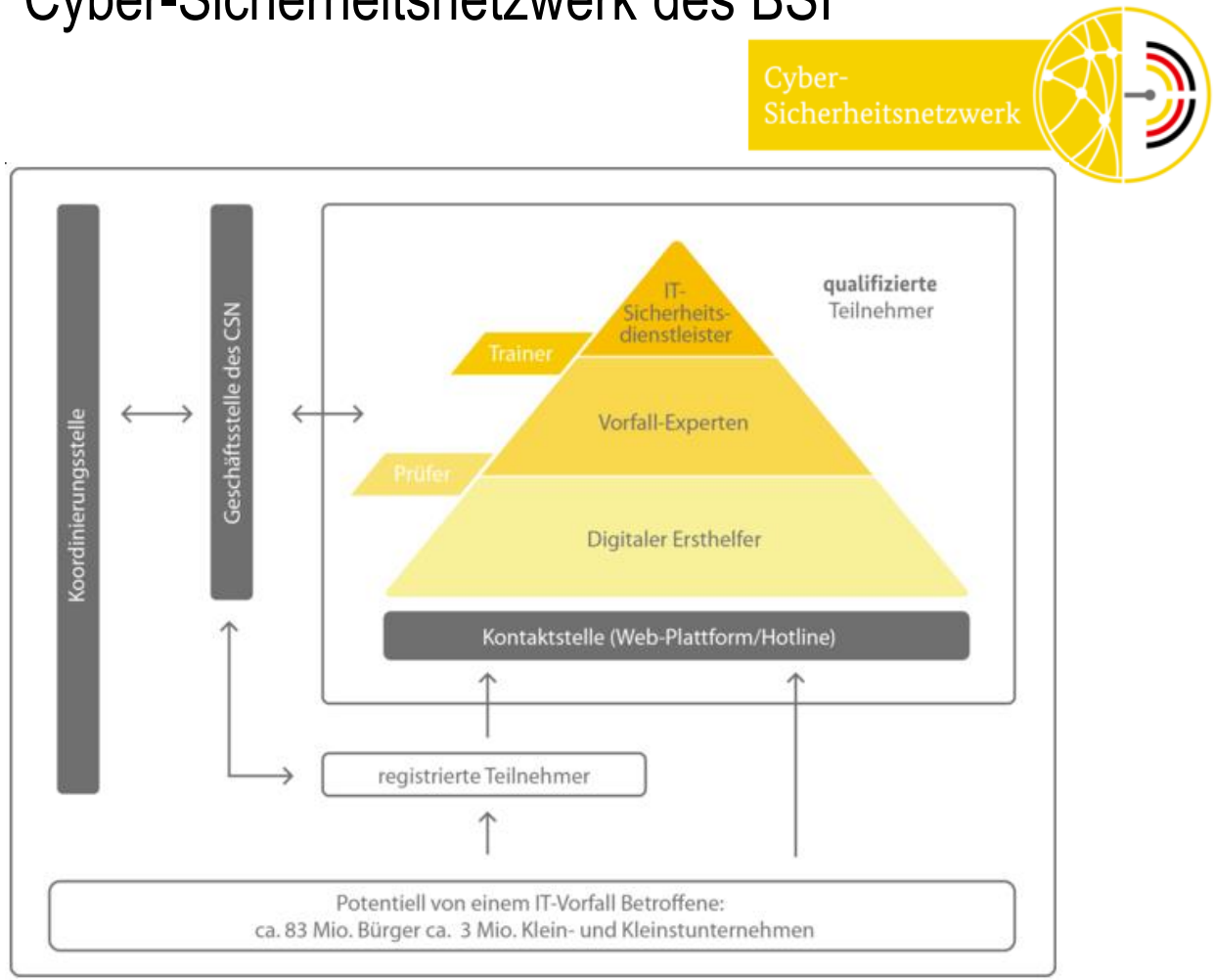
Die Rolle des Digitalen Ersthelfers

- DE ist jemand, der eine Ersteinschätzung der Lage vornimmt und dann
  - unmittelbar Hilfe leistet (selbst direkt handeln), oder
  - mittelbar Hilfe leistet (Hilfe von Dritten einholen)

- Ist Ansprechpartner für interne Kollegen: Fragen oder Hilfebedarf zu möglichen IT-Vorfällen
- Nimmt auch Erstmeldungen über mögliche IT-Vorfälle von Dritten entgegen
- Gibt jedoch keine Informationen nach außen!

Konzeptvorstellung „Digitaler Ersthelfer“

Cyber-Sicherheitsnetzwerk des BSI



Quelle: https://www.bsi.bund.de/DE/Themen/Unternehmen-und-Organisationen/Informationen-und-Empfehlungen/Cyber-Sicherheitsnetzwerk/cyber-sicherheitsnetzwerk_node.html

IT-Notfallkarte

Fazit

Rückblick: bewältigen Organisationen IT-Vorfälle zuverlässig, schnell und sicher?

- Viel wertvolle Zeit geht zwischen Vorfall und Entdeckung verloren
- Zu oft werden falsche Prioritäten gesetzt, Spuren vorschnell „verwischt“ oder befallene Systeme zu lang weiter verwendet
- Ein systematisches Problem liegt im häufigen „Blindflug“: Systeme erstellen zwar Ereignisprotokolle, diese werden aber nicht aggregiert, ausgewertet und überwacht
- Hinzu kommt vermeidbarer Stress, wenn ein Vorfall bemerkt wird
- Um so wichtiger ist es, Menschen (uns!) in die Lage zu versetzen, mit einfachen „Handgriffen“ IT-Auffälligkeiten besser erkennen und schnell Hilfe holen zu können

Diskussionsrunde und Ausblick

Zusammenfassende Einschätzung

- Erfahrungen aus der IT-Forensik und aus Penetrationstests
  - Standards/Prozesse/Rahmenwerke sind notwendig aber nicht hinreichend
  - Erst durch (zusätzliche) konkrete Tests und Übungen kann hinreichende IT-Sicherheit entstehen
- CERT, SIEM, SOC, etc. und doch falsch reagiert – Weltenbruch und Komplexität als Problem
  - KMU: wir haben keine Ressourcen, um diesen Windows 2003 Server abzulösen
  - Konzern: „Hm, diesen Windows 2003 Server haben wir unter unseren 5.000 anderen Serversystememem wohl übersehen“
- Werkzeugkoffer für Reaktionsmöglichkeiten
  - Zusätzliches „Werkzeug“: Digitaler Ersthelfer
- Cyber Security in die einzelnen Business-Abteilungen tragen
  - Digitaler Ersthelfer

Kurzvorstellung

PERSON

- **Martin Wundram**
- Jahrgang 1982
- Diplom Wirtschafts-informatik, Uni Köln

wundram@digitrace.de

ERFAHRUNG (AUSWAHL)

Von der IHK zu Köln öffentlich bestellter und vereidigter Sachverständiger für Systeme und Anwendungen der Informationsverarbeitung, **insbesondere IT-Sicherheit und IT-Forensik**

Lehrbeauftragter der Universität zu Köln, Vorstandsmitglied AKEUR e.V., Vorstandsmitglied des Bundesverbandes für den Schutz Kritischer Infrastrukturen (BSKI) e.V.

Geschäftsführer und Gründer der DigiTrace GmbH

Teamgröße am Standort Köln: 12, davon 11 IT‘ler

Kunden von KMU bis Konzerne + Behörden, **insb. auch im Bereich KRITIS**

- Präventive Projekte: Audits, Penetrationstests, IT-Sicherheitskonzepte, strategische Beratung zu IT-Sicherheit, …
- Reaktive Projekte: IT-Forensik, Incident Response, eDiscovery, …
- Sachverständigentätigkeit / Gutachten zu allen Themen der IT

Kurzvorstellung DigiTrace

DigiTrace
Kompetenz in IT-Forensik

Womit unterstützen wir?

ZAHLEN UND FAKTEN

Gegründet 2011 von Martin Wundram und Alexander Sigel, die beide Geschäftsführer und alleinige Gesellschafter sind (eigenkapitalfinanziert).

Seit 2013 Ausbildungsbetrieb. Teamgröße: 8 IT-Experten. Vom Standort Köln aus in die Welt: national und international tätig. Alle Mitarbeiter sind einschlägig qualifiziert und z.T. bereits seit Ausbildung/Studium bei DigiTrace.

Unser Team hat hunderte Projekte realisiert, hunderte Gutachten geschrieben, dutzende Vorträge sowie Schulungen durchgeführt.

beweisbar authentisch – unabhängig – sachverständig

IT-FORENSIK

Sachverständige Aufklärung mit Leidenschaft und Methodik: Sie haben Fragen zu auffälligen Sachverhalten, bei denen Datenspuren zur Erhellung beitragen können?
ind beurteilen
d von Datenquellen
er und beantworten

INCIDENT RESPONSE

Gekonnt reagieren im IT-Ernstfall: Bei IT-Sicherheitsvorfällen oder Notfällen unterstützen wir Sie kurzfristig. Wir beurteilen IT-Schäden und helfen Ihnen, diese zu minimieren, Notfallmaßnahmen umzusetzen, so wieder in den Normalbetrieb zu gelangen und Ihre Systeme gegen Angriffe zu härten. I
und erkennen und managen Ihre Risiken.

IT-SICHERHEIT | PENTESTS

Wir fordern Sie heraus – als Sparringspartner:
Egal ob 1 oder 4.000 Server – unsere Penetrationstester beherrschen verschiedenste Tätersimulationen, Black- wie White-Box-Vorgehen für Angriffe auf externe wie interne IT-Systeme und -Netze sowie auf Webanwendungen. Techniker wie Manager verstehen die in unseren Berichten aufgezeigten Schwachstellen und wie sie geschlossen werden können.

eDISCOVERY

Heiße Spuren treffsicher finden und beurteilen: Sie suchen in großen Datenmengen nach „der Nadel im digitalen Heuhaufen"? Mit Know-How, Methodik nach EDRM und geeigneten Werkzeugen und Systemen stellen wir beweisrelevante Daten sicher und bereiten diese verdichtend auf. Sie reviewen auf unserer Analyseplattform oder betrauen uns auch mit der inhaltlichen Durchsicht.

IT-BERATUNG

Mit Sachverstand passende Lösungen erarbeiten: Profitieren Sie vo
in IT-Forensik und IT-Sicherheit, um Ihr Problem zu lösen. Uns treibt de
– Organisation – Technik, denn Investition in nur mehr Technik wird Sie
Fragen Sie z.B. nach Schutzbedarfsanalysen und -konzepten, Angriffss

SCHULUNGEN

Know-How teilen – mit Ihnen: Sie lernen mit uns für Sie relevante Konzepte und ihre praktische Anwendung in der IT. Unsere Trainer schöpfen ihr Wissen authentisch aus eigener Projekterfahrung, insbesondere in IT-Forensik und IT-Sicherheit, und

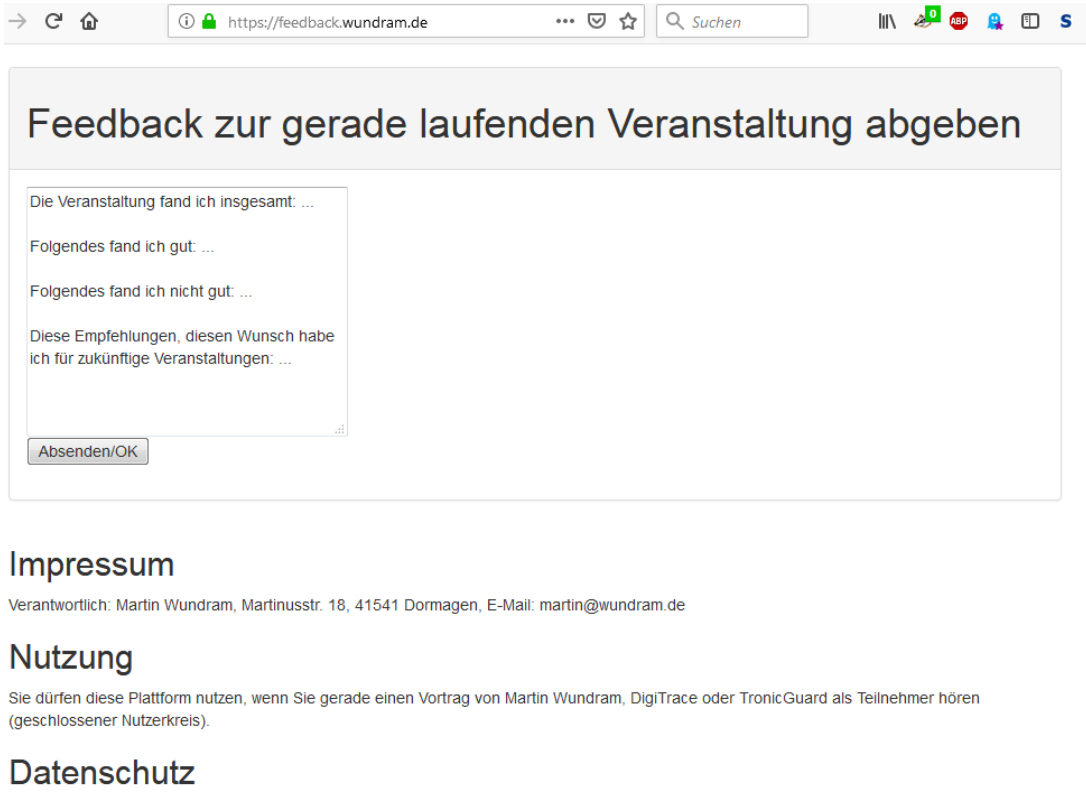
VORTRÄGE

Von Keynote bis Fachvortrag – wir berichten aus erster Hand: In unseren Vorträgen (Präsenz und online) zu IT-Forensik und IT-Sicherheit vermitteln wir seriös und verständlich den ernsthaften Kern des Themas. Sie erfahren aktuelle Entwicklungen und Einschätzungen aus dem Blickwinkel von Spezialisten, erhalten Denkanstöße und Handlungsempfehlungen oder erleben besondere Live-Hacks.

Diskussionsrunde und Ausblick

FOLIEN-DOWNLOAD ab sofort

- Anonymes Feedback-System und Folien-Download: https://feedback.wundram.de



Diskussionsrunde und Ausblick

Fragen

&

Antworten

Gerne auch im Nachgang an

Wundram@digitrace.de