

Das Cyber- Sicherheitsnetzwerk

Sandra Karger und Dustin Kernke, Gelsenkirchen den 19.09.2023

Gliederung

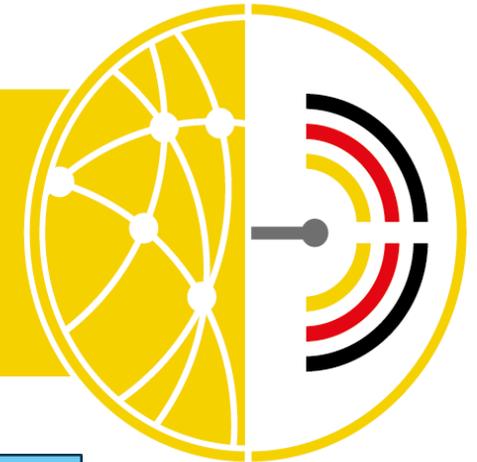
1. Das Cyber-Sicherheitsnetzwerk (CSN)

- Aufbau, Qualifikationen und Funktionsweise

2. Der Trainingskoffer des CSN

- Mini-Games, Trainingsspiele, Rollenspiele und Escape-Game

Cyber-Sicherheitsnetzwerk

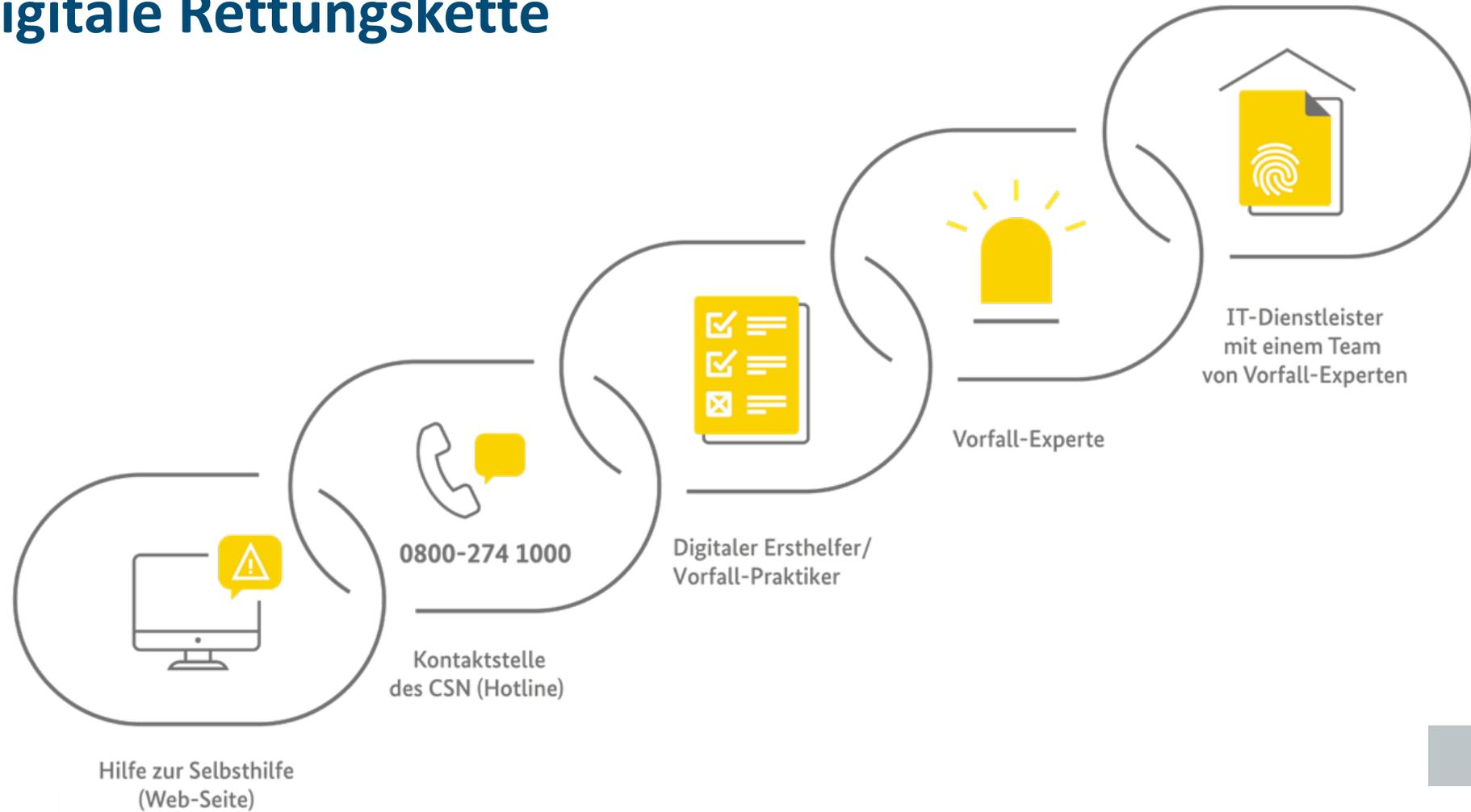


Das Cyber-Sicherheitsnetzwerk (CSN)

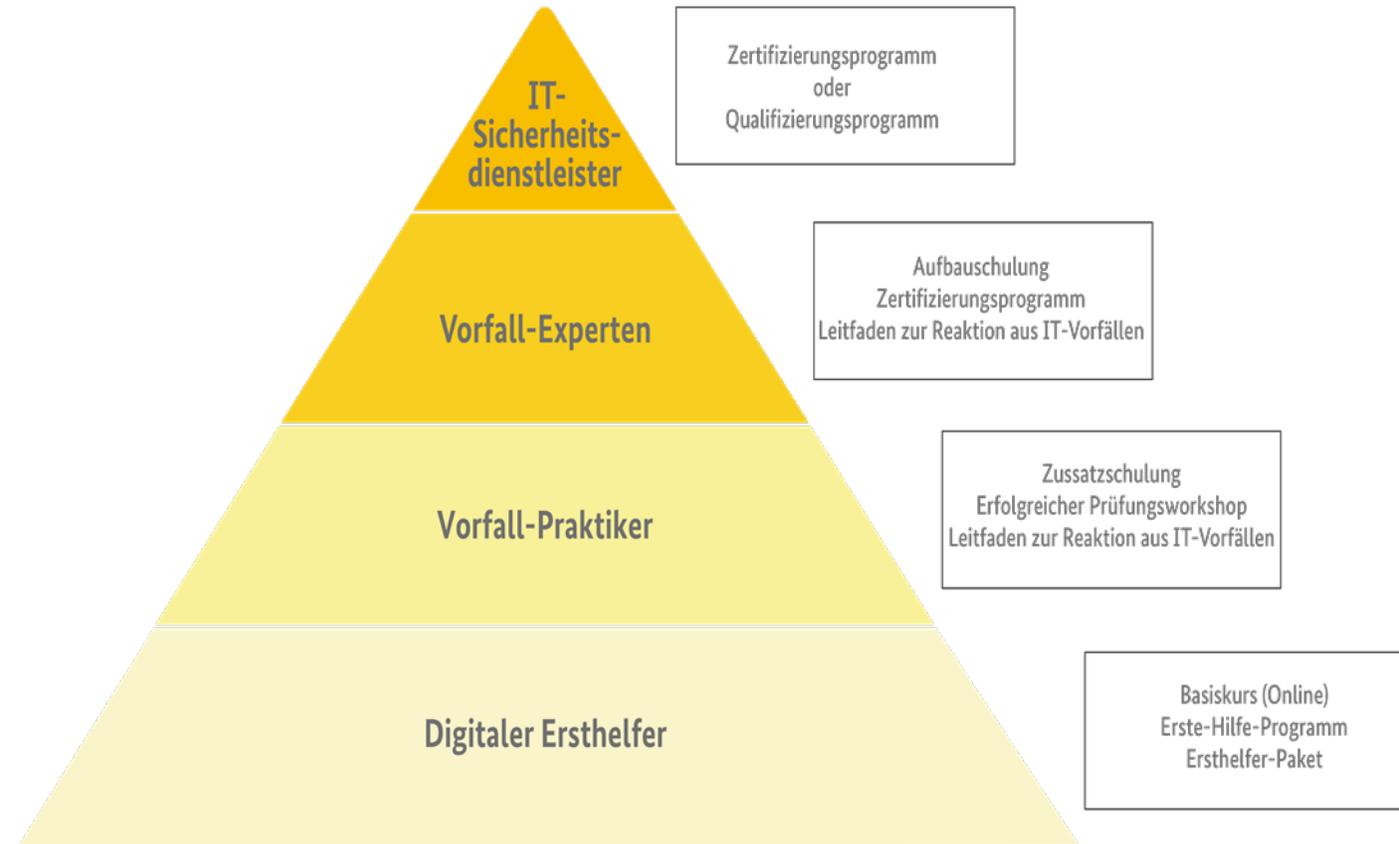
**Mit dem Cyber-Sicherheitsnetzwerk soll
eine flächendeckende dezentrale Struktur aufgebaut werden,
die effizient und kostengünstig
KMU und Bürger bei
IT-Sicherheitsvorfällen Unterstützung vermittelt.**



Die Digitale Rettungskette



Qualifizierungsprogramm



Kostenlose Kontaktstelle bei IT-Sicherheitsvorfällen

Deutschland
Digital•Sicher•BSI•

Hilfe zur Selbsthilfe

- „TOP 12 Maßnahmen“ bei Cyber-Angriffen
- Maßnahmenkatalog zum Notfallmanagement - Fokus IT-Notfälle
- Erste Hilfe bei einem schweren IT-Sicherheitsvorfall Version 1.1

Kontakt zum Service Center (Hotline)

- Kostenlose Hotline-Nummer
- Zentrale Anlaufstelle, deutschlandweite Hotline
- Ersteinschätzung des IT-Sicherheitsvorfalls, um im richtigen Glied der Rettungskette einzusteigen



Schnelle Hilfe bei IT-Sicherheitsvorfällen

Deutschland
Digital•Sicher•BSI•

Schnelle und einfache Ersthilfe durch Digitale Ersthelfer (DEH) für Verbraucherinnen und Verbraucher

- DEH löst kleine IT-Störungen und IT-Sicherheitsvorfälle (telefonische Ersthilfe)
- Leitplanken gibt ein Leitfaden mit konkreten Handlungsempfehlungen

Schnelle Ersthilfe für KMU durch Vorfall-Praktiker (VP)

- VP löst kleine IT-Sicherheitsvorfälle (telefonische Ersthilfe)

Umfangreiche IT-Vorfallanalyse durch personenzertifizierte Vorfall-Experten (VE)

- Tiefgehende Analysegespräche
- Vor-Ort-Unterstützung möglich, falls erforderlich

Lösung komplexer IT-Sicherheitsvorfälle durch einen IT-Sicherheitsdienstleister mit einem Team von Vorfall-Experten





Kartenansicht **Suchen nach**

Aktivierung notwendig

Wenn Sie die interaktive Karte nutzen möchten, wird Ihre IP-Adresse an den Kartenanbieter OpenStreetMap übertragen. Dieser ist selbst für die Verarbeitung verantwortlich. Alle Informationen dazu finden Sie in der [OpenStreetMap Privacy Policy](#)

EINVERSTANDEN

- Digitaler Ersthelfer
- Vorfall-Praktiker
- Vorfall-Experte
- IT-Sicherheitsdienstleister



Kartenansicht **Suchen nach**

- Digitale Ersthelfer
- Vorfall-Praktiker
- Vorfall-Experten
- IT-Sicherheitsdienstleister

Suche Digitale Ersthelfer

Mit der Suchfunktion können Sie nach Namen, Ort oder PLZ filtern. Durch Eingabe von mehr oder weniger Buchstaben des Ortes bzw. des Namens oder Ziffern der PLZ können Sie Ihre Suche entsprechend einschränken oder ausweiten.

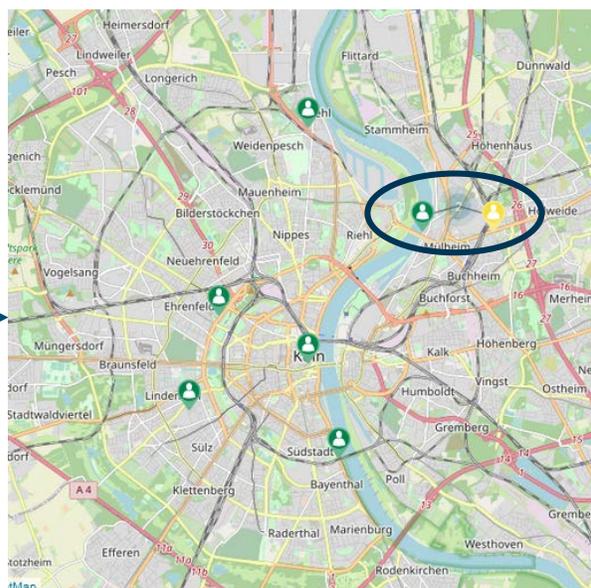
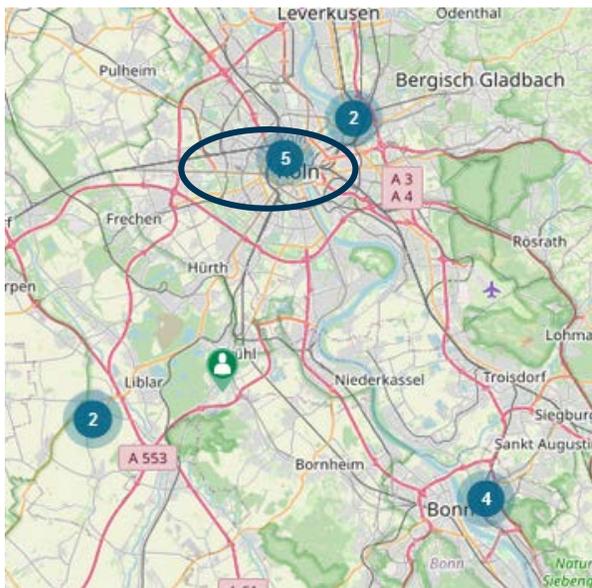
Ohne Sucheintrag, werden Ihnen alle eingetragenen "Digitale Ersthelfer" ausgegeben.

Name
Ort
PLZ

Senden

1 bis 1 von 1 Ergebnissen für Ihre Suche nach ""

Name	Ort	PLZ
Subotta, Michel	Köln	51063



Max Mustermann
54321 Musterstadt
+49 123456789
Beispiel@csn.de

Mehr

Max Mustermann

Max Mustermann

Servicezeiten:
Montag-Donnerstag: 10:00 – 17:00 Uhr
Freitag: 10:00 – 15:00 Uhr
54321 Musterstadt
Telefon: +49 123456789
E-Mail: Beispiel@csn.de

Zahlen, Daten, Fakten des Cyber-Sicherheitsnetzwerks



19 Trainingseinheiten im neuen Trainingskoffer

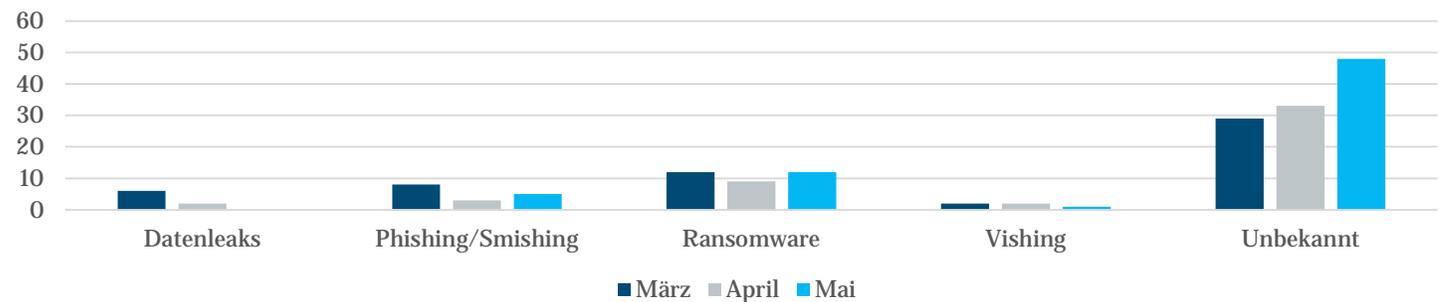
35 Anzahl der Schulungsanbieter

372 durch die Hotline weitergeleitete IT-Sicherheitsvorfälle

335 Teilnehmerinnen und Teilnehmer an Schulungen zum Vorfall-Praktiker bzw. Vorfall-Experten

302 (332)	20 (22)	11 (13)	18
Digitale Ersthelfer	Vorfall-Praktiker	Vorfall-Experten	IT-Sicherheitsdienstleister

Arten der über die Hotline weitergeleiteten IT-Sicherheitsvorfälle



Der Trainingskoffer des CSN

Inhalt des Trainingskoffers



Spiellesammlung und Rollenspiele aus dem Trainingskoffer:

- > Mini-Games
- > Trainingsspiele
- > Rollenspiele
- > Escape Game

Weitere Informationen



Mini-Games



Trainingsspiele



Rollenspiele



Escape Game



Mini-Games

- **Störung oder Vorfall** (Zuordnungsspiel)
- **Vor-Ort-Unterstützung** (Memorie)
- **Digitale Rettungskette** (Domino)
- **Vorfallbearbeitungs-Quiz** (Quizspiel)
- **Trainingszirkel** (Trainingsstationen)



Deutschland
Digital•Sicher•BSI



Trainingsspiele

Deutschland
Digital•Sicher•BSI•

- **Tutorium** (Karten-/Quizspiel)
- **Protect & Hack** (Brettspiel)



Rollenspiele

- IT-Störung
- Social Engineering
- Phishing
- Ransomware
- Fernzugriff
- Webshop
- Bots

Deutschland Digital•Sicher•BSI

CSN TRAININGS-KOFFER: Social Engineering & CEO-Fraud
Rollenspiel: Rollenkarte 4

Herr Rath S. 1/4

Rolle: Herr Rath, Geschäftsführer der Lions IT GmbH

Du bist Herr Rath, Geschäftsführer der Lions IT GmbH.

Du bist seit 20 Jahren auf deiner jetzigen Position, nachdem du bei der frisch gegründeten Lions IT GmbH bereits deine kaufmännische Ausbildung absolviert hast und über die Jahre in die Geschäftsleitung aufgestiegen warst.

Du bist lokal sehr engagiert, unter anderem in Gemeindefarbeit deiner katholischen Kirche und als Trainer bzw. in der Jugendarbeit des lokalen Hockeyvereins und daher lokal bekannt und sehr beliebt.

Deine weiteren Hobbys sind Rennradfahren, Restaurantbesuche, Kochen und Social Media.

Gestern warst du bei einem Vorstandessen des Hockeyvereins, der gerade Spenden für ein neues Trainingszentrum akquiriert.

Abends hast du von der Security Managerin, Frau Schmitt, erfahren, dass es einen Versuch eines gerade noch vereitelten CEO-Fraud gegeben haben soll und auch deine Assistenz, Frau Miller, sensible Informationen am Telefon vermutlich gegenüber einem Fremden preisgegeben hat, der sich als dein „alter Schulfreund“, Herr Merkel, ausgeben hatte.

Du kennst Merkel tatsächlich aus der Schule, hast ihn aber seitdem nicht mehr getroffen oder gesprochen.

Diese Informationen haben dich erinnern lassen, dass es zuletzt auf den Social Media-Kanalen eine ungewöhnliche Häufung von Kontaktanfragen dir fremder Personen gegeben hat – normalerweise erhältst du beinahe ausschließlich Anfragen aus dem geschäftlichen Umfeld oder dem deines sozialen Engagements bzw. deiner Hobbys. Du kannst dich nicht genau erinnern, von wem bzw. ob du Anfragen von Fremden angenommen hast, weil es gegebenenfalls Überschneidungen mit deinen geschäftlichen oder freizeithlichen Aktivitäten gegeben haben könnte.

CSN TRAININGS-KOFFER: Social Engineering & CEO-Fraud
Rollenspiel: Rollenkarte 4

Herr Rath S. 3/4

In der Spielsituation geht es unter anderem darum, dass einer Mitarbeitenden, die als Assistentin der Geschäftsführung tätig ist, nach einem Telefonat mit einer ihr unbekannt Person gewährt worden ist, dass sie möglicherweise von einem Social Engineer ausgehört wurde und potenziell Informationen über ihren Chef preisgegeben hat.

Außerdem hat sich ein Mitarbeitender aus der Finanzbuchhaltung gemeldet und einen Verdacht in Richtung eines versuchten CEO-Fraud geäußert.

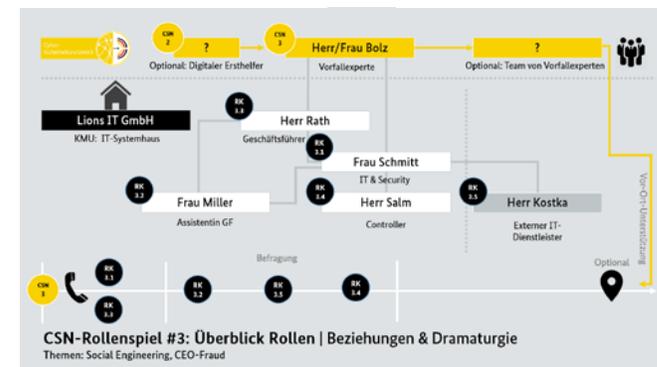
Durch die Meldung bei Frau Schmitt wurde der Geschäftsführer zu weiteren Auffälligkeiten befragt.

Emotionaler Hintergrund

Du denkst: „Mensch, dass ausgerechnet uns als IT-Berater so etwas passieren muss – das ist schon peinlich. Aber gut, dass es erstmal keine schlimmen Konsequenzen hatte. Und gerade ich als Geschäftsführer muss besser aufpassen, dass mir so etwas nicht mehr passiert.“

Du wirst jedoch auch zunehmend bewusst, dass du als Chef möglicherweise kein gutes Vorbild warst und alle Mitarbeitenden zu einer sehr offenen Informationskultur eingeladen hast – vielleicht keine gute Idee bei fortschreitender Digitalisierung mit all den Risiken des Informationsverlustes bei hoher Verfügbarkeit von Informationen.

Eigene Notizen zum Rollenspiel:



Escape-Game – Szenario 1

- Fiktive Spielsituation zu existenzbedrohendem Cyber-Angriff auf ein Unternehmen.
- Ziel ist es gemeinsam mit einer Vorfall-Praktikerin des CSN einen IT-Sicherheitsvorfall zu lösen.
- Die Trainingseinheit ist für eine Gruppengröße von vier bis zwölf Personen geeignet.
- Zeitumfang ca. 90 Minuten, inklusive Einführung und Nachbesprechung



Deutschland
Digital•Sicher•BSI•



Escape Game: Benton-Plast GbR

4

Einheit 2: Unter Zeitdruck

Leider kam die Schulung dann doch etwas zu spät, wie sich in den Folgetagen herausstellt. Ein unbedachter Klick und schon hat sich die Beton-Palast GbR Schadssoftware eingefangen - und den ganzen Betrieb lahmgelegt. Jetzt heißt es, unter Zeitdruck Ruhe zu bewahren.

Materialien

- ↳ Audiodatei zu Szene 2
- ↳ Anleitung V1.2
- ↳ Hilfe V1.2
- ↳ Lösung V1.2
- ↳ Trainingsmaterialien V1.2

Tutorium: Vorfallsbehandlung durch Digitalen Ersthelfer

5

Einheit 3: Angriff mit Ransomware

Herr Schmitz muss feststellen, dass die Beton-Palast GbR Opfer eines Angriffs mit Ransomware geworden ist - und er diesen Vorfall nicht alleine bewältigen kann. Doch zum Glück gibt es ja das CSN, das in solchen Fällen Unterstützung anbietet und dabei hilft, die vielen Fragen zu klären, die von einem betroffenen Unternehmen gestellt werden.

Materialien

- ↳ Audiodatei zu Szene 3
- ↳ Anleitung V1.3
- ↳ Hilfe V1.3
- ↳ Lösung V1.3
- ↳ Trainingsmaterialien V1.3

6

Einheit 4: Datensicherung

Back-Ups könnten dabei helfen, den Schaden für die Beton-Palast GbR zu minimieren - wenn die Datensicherung regelmäßig erfolgt ist und die Datenträger nicht ebenfalls vom Vorfall betroffen sind. Herauszufinden ist, ob die Vorkehrungen von Herrn Schmitz ausreichend waren.

Materialien

- ↳ Audiodatei zu Szene 4
- ↳ Anleitung V1.4
- ↳ Hilfe V1.4
- ↳ Lösung V1.4
- ↳ Trainingsmaterialien V1.4

7

Abschluss

Nur noch ein Schritt fehlt, damit die Beton-Palast GbR wieder den Betrieb aufnehmen kann: die Eingabe des Entsperrcodes, der sich aus den Lösungen der vier Trainingseinheiten ergibt. Wenn alles richtig war, steht der Fortführung der Baustellen nichts mehr im Wege.

Materialien

- ↳ Audiodatei zu Szene 5
- ↳ Bonusmaterial



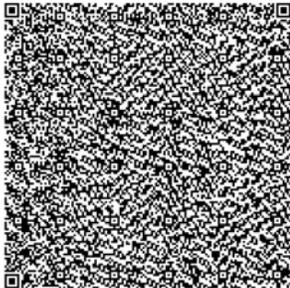
Vielen Dank für Ihre Aufmerksamkeit!

Deutschland
Digital•Sicher•BSI

Sandra Karger

Referatsleiterin WG 21

*Kooperation mit Herstellern
und Dienstleistern*

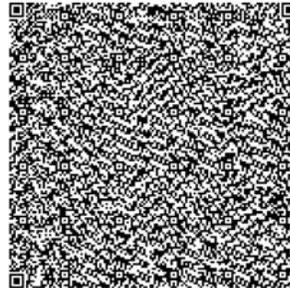


 Bundesamt
für Sicherheit in der
Informationstechnik
Digital•Sicher•BSI

Dustin Kerne

WG 21

*Kooperation mit Herstellern
und Dienstleistern*



 Bundesamt
für Sicherheit in der
Informationstechnik
Digital•Sicher•BSI

Mit dem Cyber-Sicherheitsnetzwerk soll
eine flächendeckende dezentrale Struktur aufgebaut werden,
die effizient und kostengünstig,
KMU und Bürger bei
IT-Sicherheitsvorfällen Unterstützung vermittelt.

Cyber-
Sicherheitsnetzwerk

