IT & IoT in Healthcare: Wie können Krankenhäuser vor Hackerangriffen geschützt werden?

Bildquelle: katatonia82, iStockphoto LP

Moderation und Begrüßung

Dr. Bettina Horster

Director IoT eco - Verband
der Internetwirtschaft e.V

Vorstand VIVAI Software AG

Tatjana Hein

Projektmanagerin IoT

eco - Verband
der Internetwirtschaft e.V

Wie Sie an diesem Webinar teilnehmen können

- Wir zeichnen das Webinar auf
- Sie sind während des ganzen Webinars stumm geschaltet
- Stellen Sie Ihre Fragen **schriftlich über den Chat** in Ihrem Control Panel
- Die Fragen werden am Ende der heutigen Präsentationen besprochen
- Sie können **in der Fragerunde Ihre Frage auch gerne mündlich** stellen
  - Nutzen Sie bitte die **„Hände heben" Funktion** in Ihrem Control Panel
  - Wir werden Ihre Stummschaltung dann aufheben
  - Bitte nennen Sie dann kurz Ihren Namen und Ihre Firma und stellen Sie Ihre Frage
- Falls Sie lieber anonym bleiben möchten, können Sie natürlich weiterhin Ihre Frage schriftlich im Tool stellen

EUROPAS GRÖßTER VERBAND DER INTERNETWIRTSCHAFT


ÜBER 1.100 MITGLIEDER
IN ÜBER 70 LÄNDERN
eco
VERBAND DER
INTERNETWIRTSCHAFT

Wie können Krankenhäuser vor Hackerangriffen geschützt werden?

Agenda

13:40 Uhr: #angriffausderdunkelheit
Dr. Nicolas Krämer, Klinikgeschäftsführer hmg, Bergman Clinics B.V., Autor, Speaker

14:00 Uhr: "Cybercrime im medizinischen Umfeld - ein Problem?!"
Peter Vahrenhorst, Kriminalhauptkommissar – stellv. Sachgebietsleiter Landeskriminalamt Nordrhein-Westfalen, SG 41.1 – Grundsatz, Gremien, Auswertung, Prävention: Cybercrime-Kompetenzzentrum

14:20 Uhr: Patient Krankenhaus?
Thorsten Urbanski, Head of Communication DACH, ESET Deutschland GmbH

14:40 Uhr: Diskussionsrunde

15:00 Uhr: Ende

IT & IoT in Healthcare: Wie können Krankenhäuser vor Hackerangriffen geschützt werden?

Bildquelle: katatonia82, iStockphoto LP

DR. NICOLAS KRÄMER

#angriffausderdunkelheit

22. APRIL 2021

23. Februar 2016

#Krankenhausversagen #Patiententod

- **Cyberangriff auf ein Krankenhaus**
- **IT-Systeme heruntergefahren**
- **Erpressung des Krankenhauses durch kriminelle Hacker**
- **Das FBI ermittelt**
- **Intensivpatienten sterben durch ferngesteuerte Medikamentenpumpen und Beatmungsgeräte**

23. Februar 2016, 21.15 Uhr, RTL

#Krankenhausversagen #Patiententod

Quellen: www.freep.com, blog.starocotes.de

10. **Februar** 2016

Beginn der IT-Krise in einem Krankenhaus mitten in Deutschland

- **Cyberangriff auf ein Krankenhaus**
- **IT-Systeme heruntergefahren**
- **Erpressung des Krankenhauses durch kriminelle Hacker**
- **Das FBI ermittelt**
- **Intensi[illegible]esteuerte**

  Medik[illegible]gsgeräte

Im Darknet werden sensible Patientendaten verkauft

Wachstumsmarkt Cyberkriminalität

CYBERANGRIFF AUF EIN KRANKENHAUS

MITTEN IN DEUTSCHLAND

Quellen: www.amazon.de,, ww.buecher.de

Seit 1984 hat sich viel geändert

Eine Folge der Schwarzwaldklinik über einen Cyberangriff wurde niemals gedreht

Quelle vorherige Folie: Matze Trier

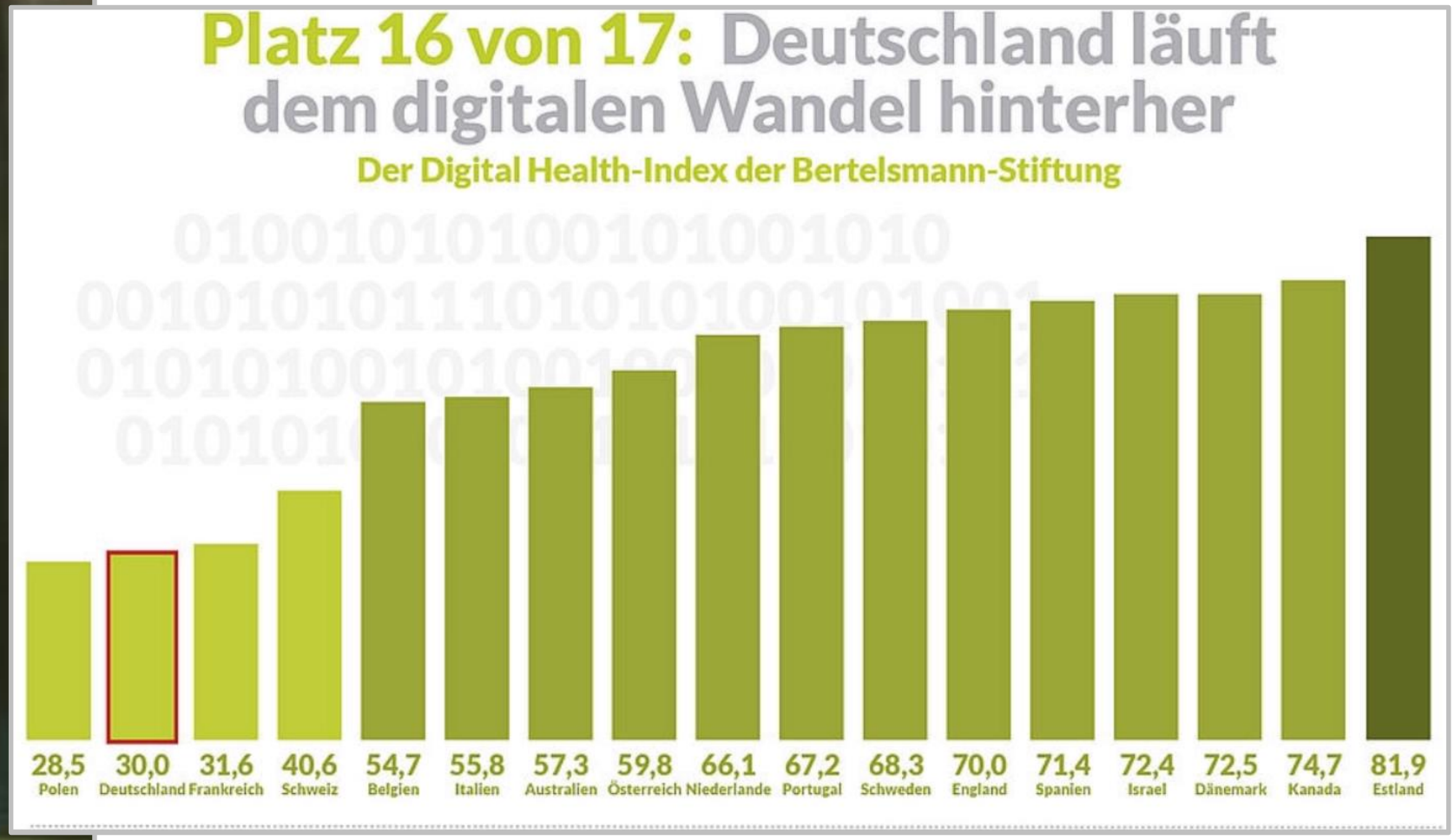
Heute sieht die Realität so aus

Digitale Visite

Quelle: pressebox.de

Das deutsche Gesundheitswesen hinkt in Sachen Digitalisierung hinterher

Rückstand durch Technik



Quellen: https://www.thebestsocial.media/de/nicht-deutsche-teilen-und-lachen-ueber-ihre-deutschesten-aktionen/online-formulare-wp/, Bertelsmann-Stiftung

10. Februar 2016: Am Aschermittwoch ist alles vorbei

Chronologie der Ereignisse

Quelle: ARD, [W] Wie Wissen, Sendung vom 9. April 2016

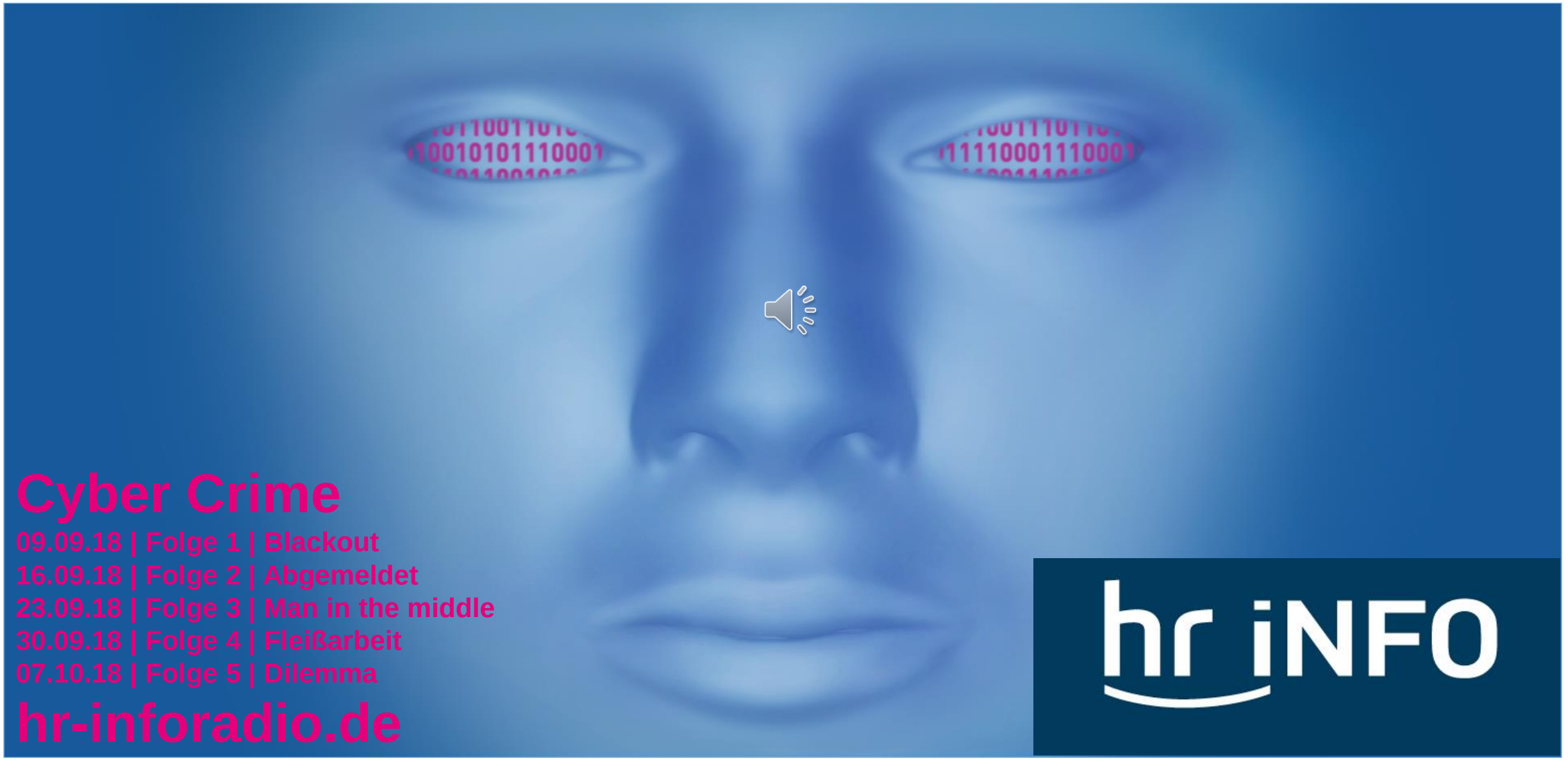
Einberufung eines Krisenstabes

Chronologie der Ereignisse

Quelle: Pixabay

Eine Nachricht des Erpressers

Folge 1 BLACKOUT des fünfteiligen Hörspiels des Hessischen Rundfunks



Einschaltung von LKA und BSI

Chronologie der Ereignisse

Quelle: ARD, [W] Wie Wissen, Sendung vom 9. April 2016

Staatsanwaltliche Ermittlungen wegen versuchter Erpressung

Einschaltung der Behörden

POLIZEI
Nordrhein-Westfalen
Landeskriminalamt

Bundesamt
für Sicherheit in der
Informationstechnik

Staatsanwaltschaft Köln
Zentralstelle und
Ansprechpartner Cybercrime
(ZAC)

Düsseldorf (ots) - Einladung zur gemeinsamen Pressekonferenz des Landeskriminalamtes Nordrhein-Westfalen (LKA NRW), der Zentralstelle und Ansprechpartner Cybercrime Köln (ZAC) der Staatsanwaltschaft Köln (StA Köln), des Bundesamtes für Sicherheit in der Informationstechnik (BSI) und des VOICE - Bundesverband der IT Anwender e.V. am Dienstag, den 8. März 2016 um 14:30 Uhr im LKA NRW.

Quellen: LKA NRW, BSI, Staatsanwaltschaft Köln

Cyberangriff auf Krankenhaus in Hollywood

Das FBI ermittelt

Hollywood Hospital Hacked Back to Paper Age

By John P. Mello Jr.
Feb 17, 2016 3:46 PM PT

Print
Email

Hollywood Presbyterian Medical Center last week revealed its computer systems were offline after a ransomware attack scrambled the data on its systems.

Quellen: E-Commerce Times, Pixabay

Die Mitarbeiter waren echte Engel!

Pressespiegel

Feiger Hackerangriff:
So wacker schlägt sich das Neusser Klinikpersonal

FOCUS vom 12. Februar 2016

Die meisten Patienten des Lukaskrankenhauses in Neuss merkten nicht einmal, dass ihre Klinik Opfer eines gefährlichen Angriffs geworden war. Ihnen fiel lediglich auf, dass sie über Tage hinweg nicht wie üblich zwischen mehreren Menüs wählen konnten.

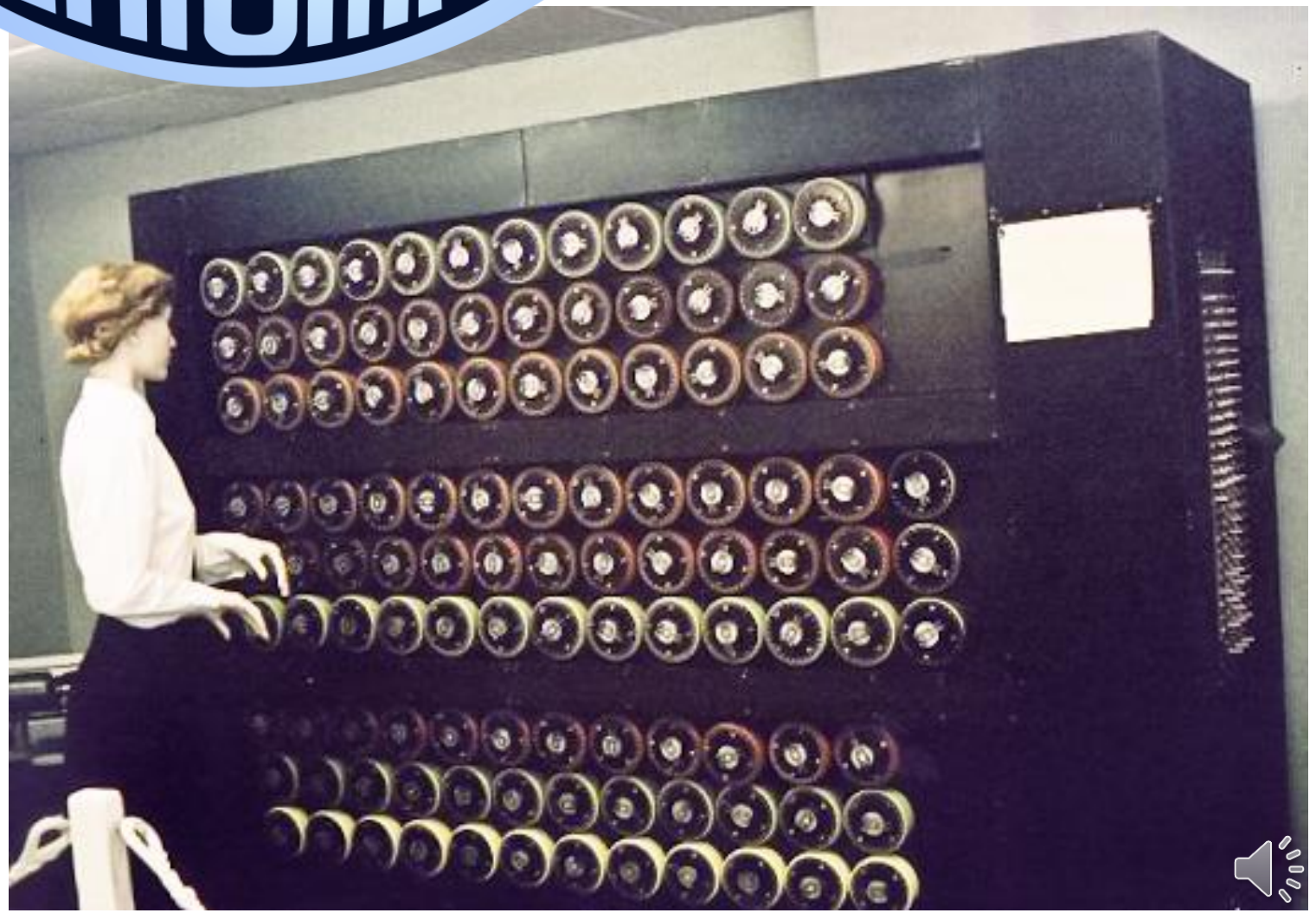
Welt am Sonntag vom 22. Februar 2016

Patient Oliver H. (28, Name geändert), der mit schwerer Mandelentzündung in der HNO-Abteilung lag, berichtet:
„Toll war, dass die Pfleger sich den Stress nicht haben anmerken lassen.“

EXPRESS vom 12. Februar 2016

Kennwortsicherheit und regelmäßige -änderungen sind von höchster Wichtigkeit

Historischer Vergleich



Quellen: Pixabay, Wikimedia, Wikipedia

Fragen wir Dr. med. James Bond

Cybersicherheit auf Rezept?

007

001 Beispiel für ein sicheres Kennwort: **P@Racet@m()l_2o2!**

002 Vorsicht bei E-Mails von unbekannten Absendern, Quarantänefilter und/oder Sandboxsystem

003 Firewalls, Netzwerksegmentierung, regelmäßige Datensicherungen/Backups und Patches

004 Penetrationstests, Notfallplan/Ausfallkonzept inkl. Versicherungsschutz

005 Keine Dienstgeheimnisse in den Sozialen Medien

006 BSI-Grundschutz oder Zertifizierung nach DIN EN ISO 27001

007 AWARENESS!

Quelle: am Puls, 4. Jg., Ausgabe 1/2017, S. 17

Im Zweifel ist es immer der Gärtner

Täter

Quelle: Fotolia

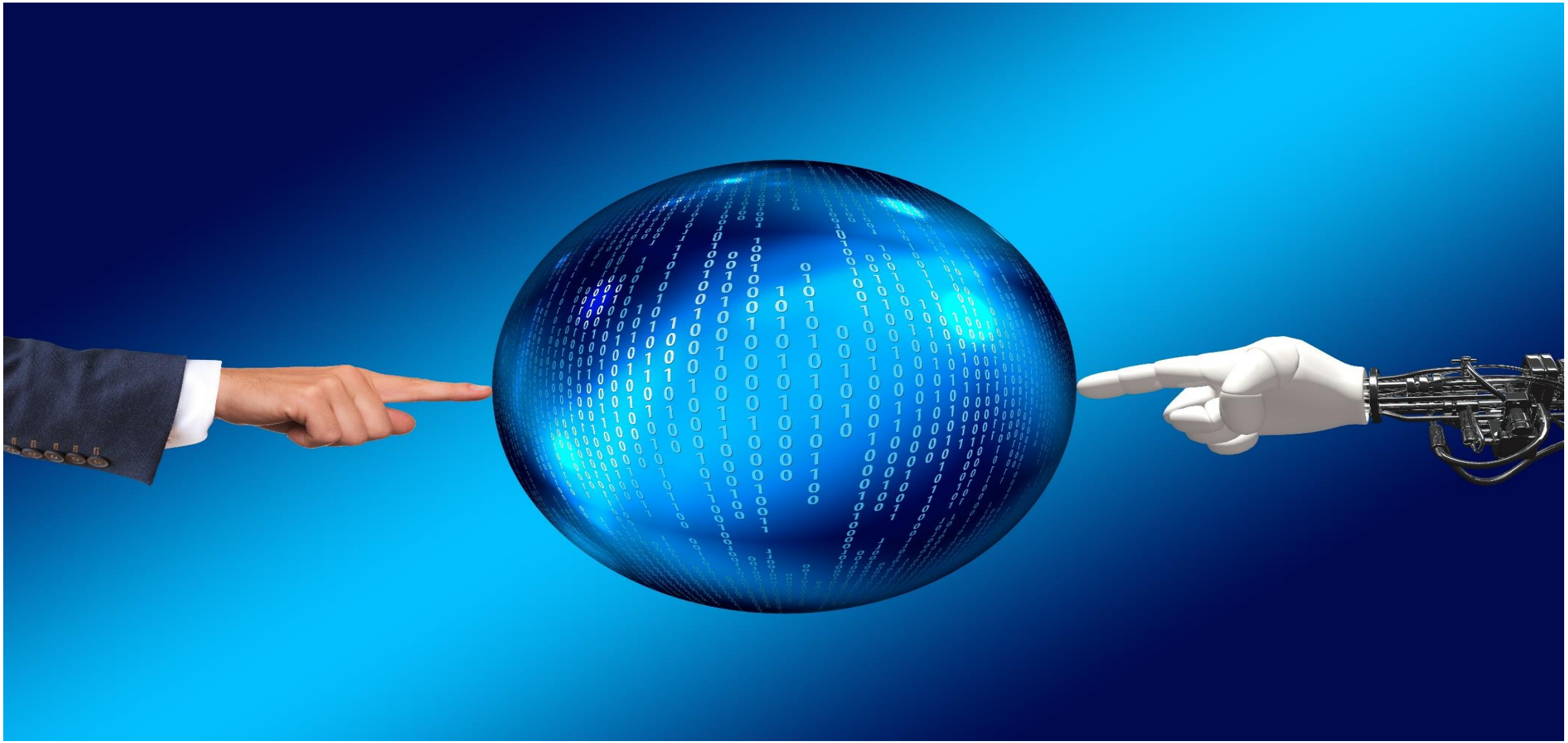
Verdächtige im Visier der Fahnder

Täter

Quelle: FBI

Corona bewirkt in Sachen Digitalisierung einen Paradigmenwechsel im Gesundheitswesen

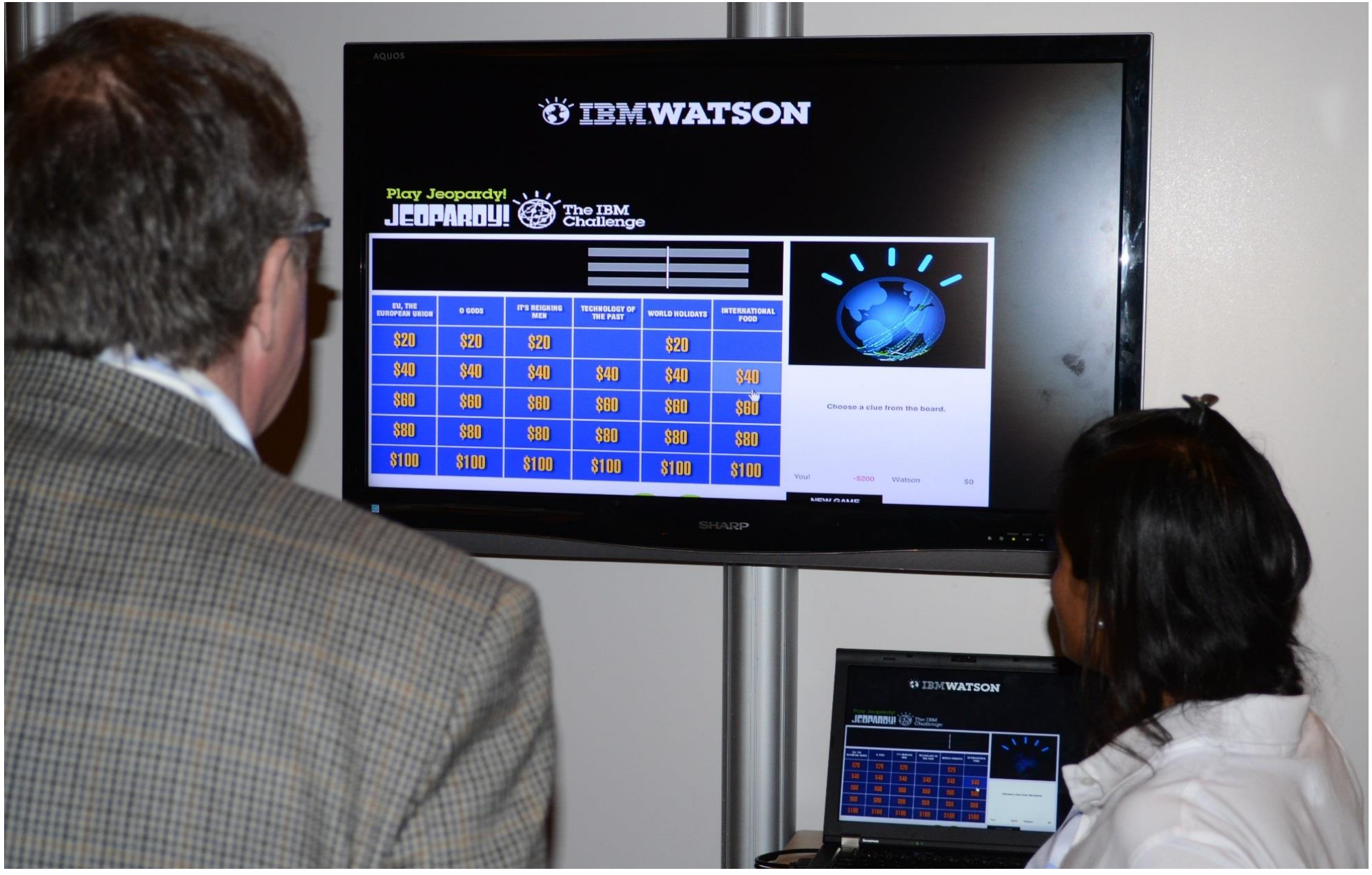
Operation Zukunft



Quelle: Pixabay

Künstliche Intelligenz unterstützt bei der ärztlichen Diagnose

IBM Watson



Quelle: Raysonho @ Open Grid Scheduler / Grid Engine

Komplette Sequenzierung der menschlichen DNA für unter 100 EUR

Big-Data-Analysen

Quellen: Zukunftsforscher Dr. Sven Gábor Jánszky, Pixabay

Es wäre fatal, wenn diese Zukunftstrends in eine falsche Richtung geleitet würden

IT-Sicherheit als wichtige Voraussetzung

Quelle: Pixabay

Trotz allem ist die Digitalisierung ein Erfolg!

Fazit

Das chinesische Schriftzeichen für Krise und Chance ist dasselbe. Wir haben es verstanden.

危机

KRISE

=

CHANCE

Quelle: Pixabay; Bilder in dieser Präsentation ohne direkte Quellenangabe stammen i.d.R. vom Referenten oder von Pixabay

STRATEGIEN ZUR DIGITALISIERUNG

Digitale Transformation im Krankenhaus unterstützt Leserinnen und Leser dabei, eine hausspezifische Digitalisierungsstrategie für ihr Krankenhaus zu entwickeln. Hierfür zeigt es beispielhaft Ansätze und Konzepte erfolgreicher Projekte auf und dokumentiert den derzeitigen Digitalisierungsgrad der Branche. Anhand konkreter Innovationsprojekte lässt sich eine strategische Zieldefinition ableiten und deren finanzielle Effekte für das Krankenhaus abschätzen.

Buchtipp Gesundheits-wirtschafts-kongress 2019

Dr. Christian Stoffers, Dr. Nicolas Krämer, Dr. Christian Heitmann (Hrsg.)
Digitale Transformation im Krankenhaus – Thesen, Potenziale, Anwendungen
Hardcover, Mai 2019, ca. 300 Seiten,
ISBN 978-3-947566-75-4, **59,95 Euro**

POLIZEI
Nordrhein-Westfalen
Landeskriminalamt

bürgerorientiert · professionell · rechtsstaatlich

Cybercrime im medizinischen Umfeld – ein Problem?!

eco AKADEMIE

webinar, 22.04.2021

POLIZEI
Nordrhein-Westfalen
Landeskriminalamt

Peter Vahrenhorst

Kriminalhauptkommissar

Landeskriminalamt NRW

SG 41.1 – Cybercrime-Kompetenzzentrum

Tel.: 0211 939 4114

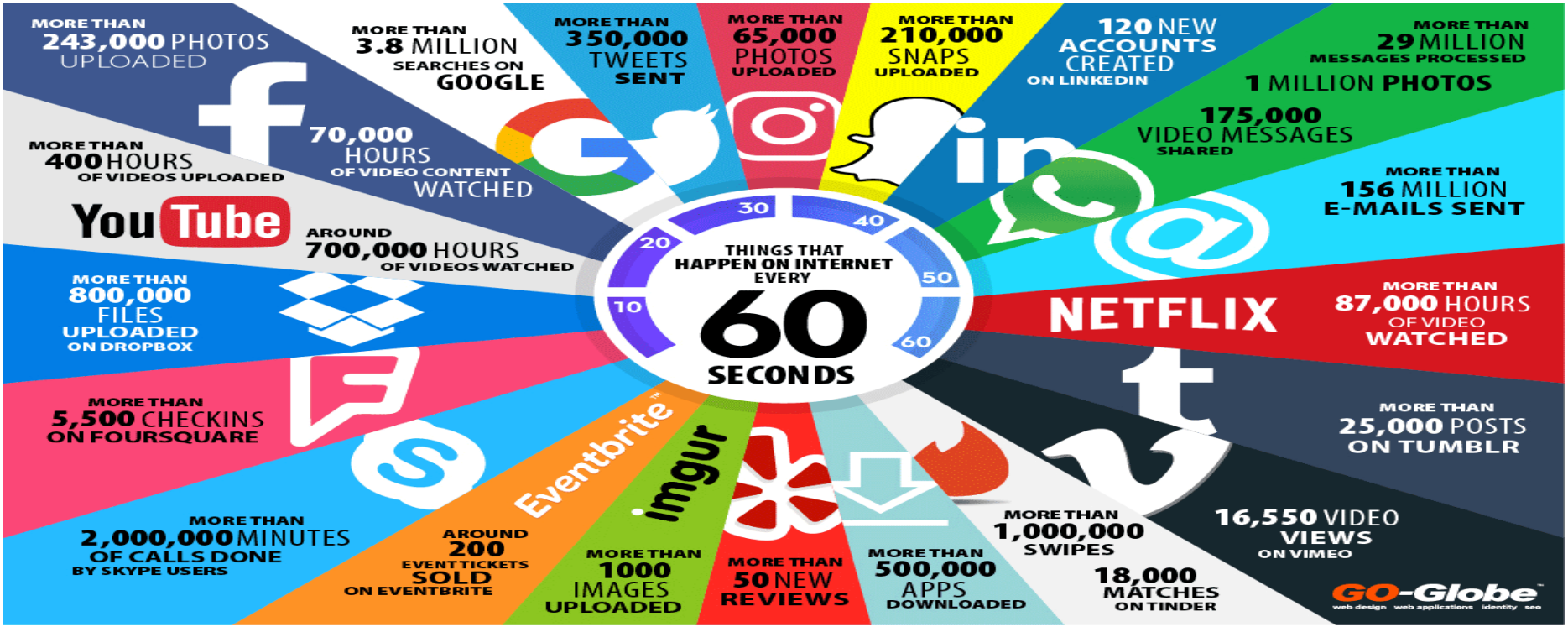
Fax: 0211 939 19 4114

Peter.Vahrenhorst@polizei.nrw.de

POLIZEI
Nordrhein-Westfalen
Landeskriminalamt

Herausforderung Digitalisierung

POLIZEI
Nordrhein-Westfalen
Landeskriminalamt



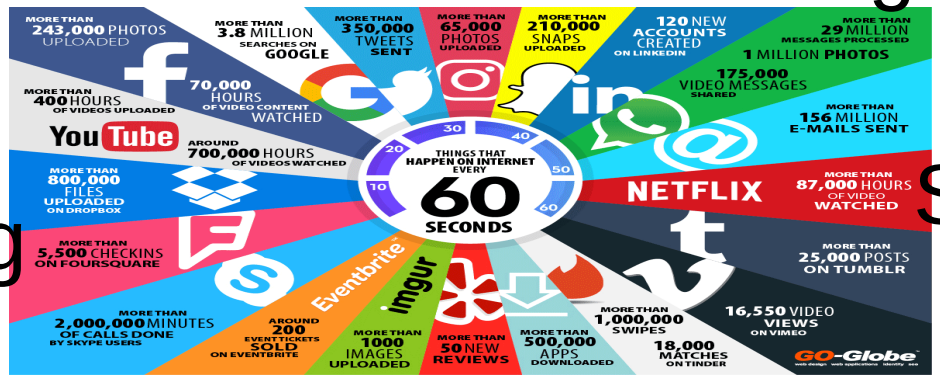
eco AKADEMIE

POLIZEI
Nordrhein-Westfalen
Landeskriminalamt

digitale Transformation

e-government

e-health



e-schooling

Smart Factory

KI/AI

cloud

automotive-IT

smart home

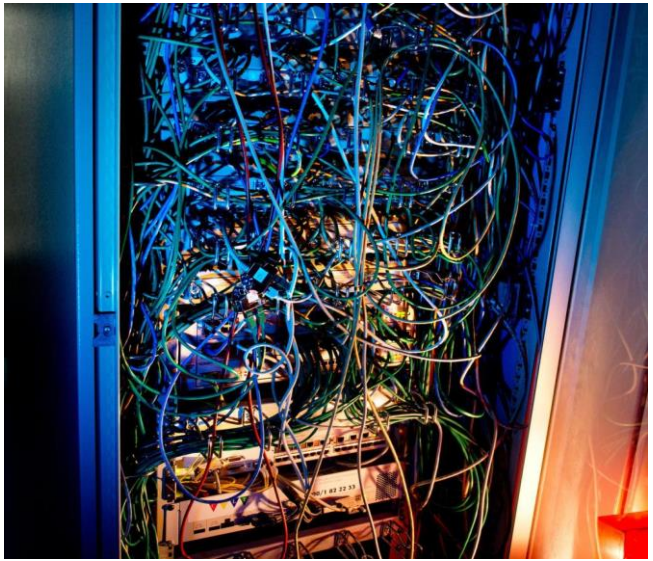
eco AKADEMIE

webinar, 22.04.2021

POLIZEI
Nordrhein-Westfalen
Landeskriminalamt

Medizin IT vs. Klassische IT

POLIZEI
Nordrhein-Westfalen
Landeskriminalamt



Virus vs. Virus

POLIZEI
Nordrhein-Westfalen
Landeskriminalamt

POLIZEI
Nordrhein-Westfalen
Landeskriminalamt

Fallbeispiel

Fall Beispiel „UKD“

POLIZEI
Nordrhein-Westfalen
Landeskriminalamt

Fall Beispiel „UKD“

Kooperationen
Gemeinsam gegen Cybercrime

POLIZEI
Nordrhein-Westfalen
Landeskriminalamt

VOICE Bundesverband der IT-Anwender e.V.

bitkom

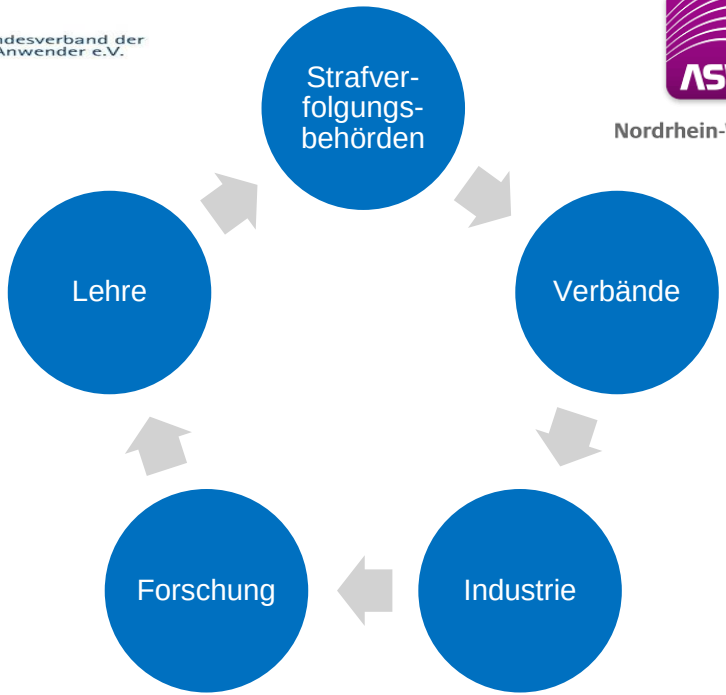
ASW Nordrhein-Westfalen

eco Verband der Internetwirtschaft e.V.

networker NRW
Der IT Verband

FH AACHEN
UNIVERSITY OF APPLIED SCIENCES

SMARTHOME DEUTSCHLAND



Fazit

POLIZEI
Nordrhein-Westfalen
Landeskriminalamt

- **Cybercrime betrifft Behörden, Unternehmen und Privatleute gleichermaßen**
- **Die Fortschreitende Digitalisierung in allen Bereichen bietet neue Möglichkeiten für Straftäter**
- **Die Bekämpfung ist eine gesamtgesellschaftliche Aufgabe und es bedarf gemeinsamer Anstrengungen aller Akteure bei der Bekämpfung**

Fragen?

Vielen Dank für Ihre Aufmerksamkeit.

PATIENT KRANKENHAUS?

ZERO-TRUST-SECURITY-IMPFSTOFF

Thorsten Urbanski

Head of Communication & PR DACH

ESET Deutschland GmbH

Leiter der TeleTrust Initiative „IT-Security made in EU“

ENJOY SAFER TECHNOLOGY™

14 Niederlassungen

234 Distributoren

24/7 Cyber Intelligence

über **100** VB100 Awards (Rekord)

über **110** Millionen Anwender

30 Jahre ESET Technologie

Secur|Ty made in EU
Trust Seal
www.teletrust.de/itsmie

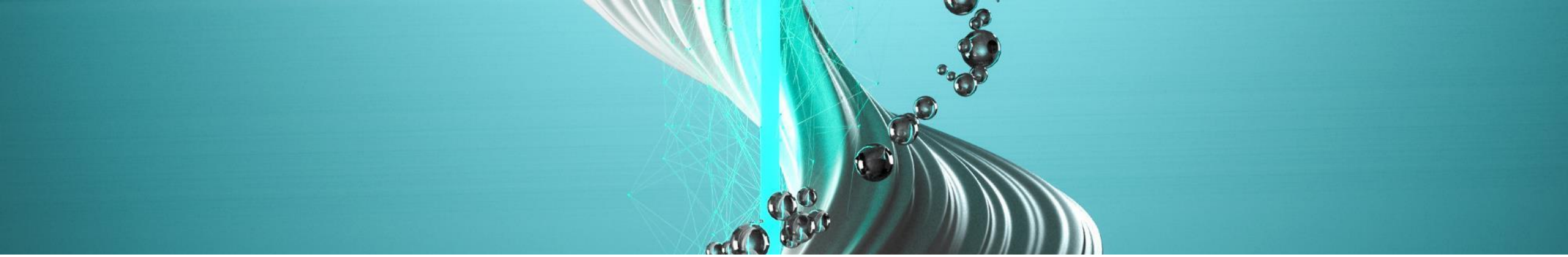
CERTIFIED ISO 27001:2013 COMPANY

CERTIFIED ISO 9001:2015 COMPANY

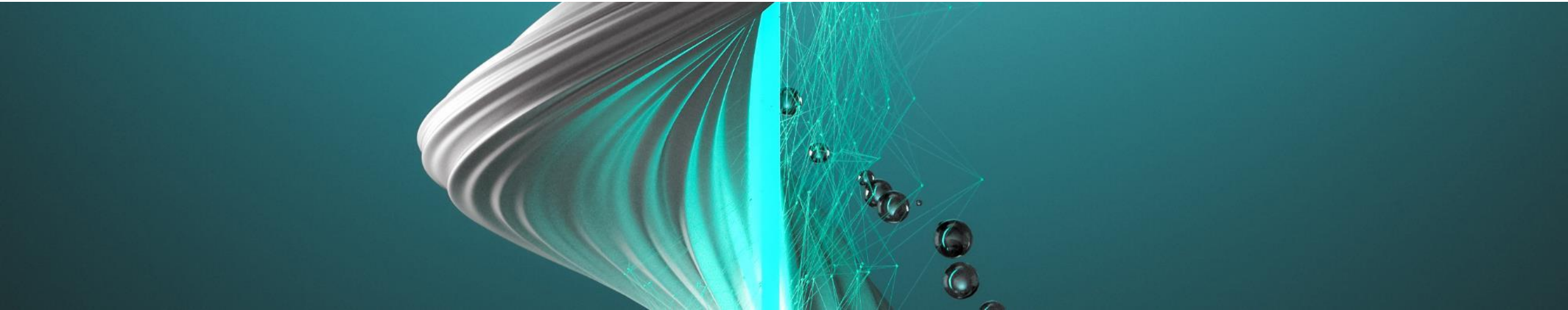

chrome


Google Play
Protect


>2,000,000,000

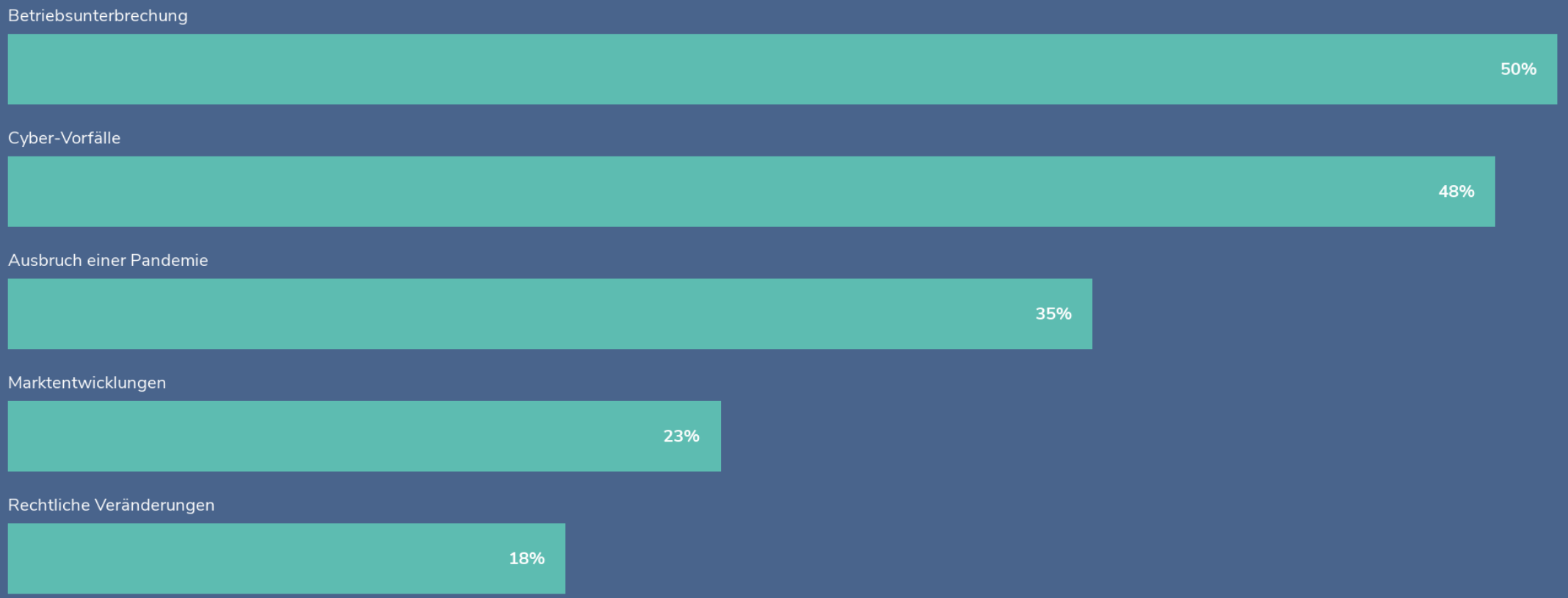


Risikoeinschätzung



TOP 5 GESCHÄFTSRISIKEN IN DEUTSCHLAND

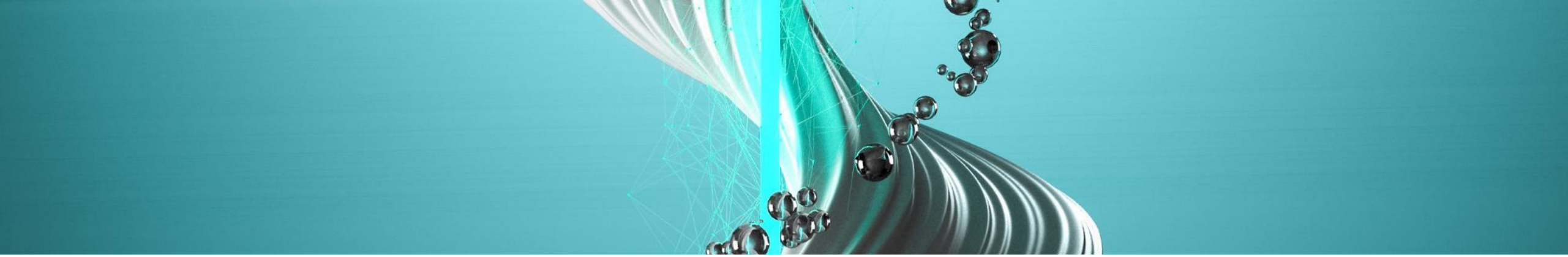
ALLIANZ RISK BAROMETER 2021



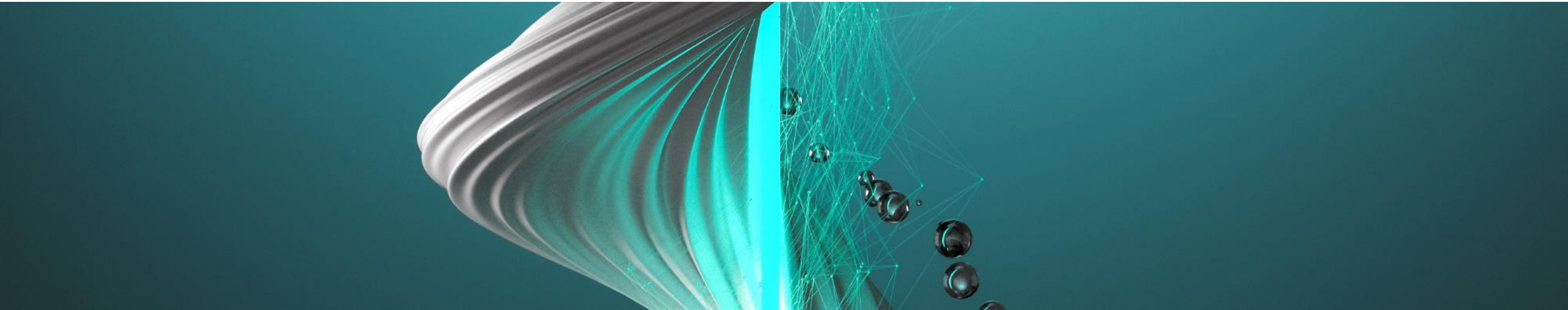
Die Zahlen geben als Prozentsatz für das jeweilige Land an, wie oft ein Risiko ausgewählt wurde. Die Zahlen addieren sich nicht zu 100%, da bis zu bis zu drei Risiken ausgewählt werden konnten. Anzahl der Befragten in Deutschland: 282.

made with 23° | reuse

Quelle: Allianz Global Corporate & Specialty



Gefahrenbarometer



Kritische Schwachstellen in Windows' Remote Desktop Protokoll

Sachverhalt
Das Remote Desktop Protocol (RDP) ist ein Dienst in Microsofts Betriebssystem Windows und ermöglicht unter anderem die Fernwartung des Systems. Im Mai 2019 wurde die kritische Schwachstelle BlueKeep in diesem Dienst bekannt, die es entfernten Angreifern ermöglicht, beliebige Programme – auch Schadprogramme – auf dem angreifbaren System auszuführen (vgl. *Quellenverzeichnis*[11]: www.microsoft.com). Von BlueKeep sind die älteren Systeme Windows XP, Windows Server 2003, Windows 7, Windows Server 2008 und Windows Server 2008 R2 betroffen. Seit Juni 2019 sind öffentliche *Exploits* für BlueKeep verfügbar. Diese Schadprogramme suchen nach offen erreichbaren RDP-Diensten im Internet, um sich über die Schwachstelle automatisiert weiterzuverbreiten. BlueKeep wird deshalb auch als „wurmfähig" bezeichnet. Szenarien wie 2017, als die *Ransomware* WannaCry innerhalb kurzer Zeit mehrere 100.000 Windows-Systeme infizierte und Daten in großem Umfang verschlüsselte, sind denkbar.

Darüber hinaus wurden im August 2019 unter dem Namen DejaBlue zwei weitere Schwachstellen mit ähnlichem Bedrohungspotenzial bekannt. Diese betrafen auch neuere Windows-Systeme bis einschließlich Windows 10 und Windows Server 2019. Auch über DejaBlue können Angreifer ohne *Authentifizierung* oder Interaktion eines Nutzers einen beliebigen Code aus der Ferne ausführen.

Die Schwachstellen sind als kritisch anzusehen. Zwar ist der RDP-Dienst in der Standardeinstellung nicht aktiv, für eine hohe Anzahl von Servern wird der Dienst aber für die Fernwartung verwendet, und dies teilweise relativ ungeschützt über das Internet.

Reaktion
Microsoft hat in der Konsequenz Sicherheitsupdates für die betroffenen Systeme bereitgestellt, und zwar auch für die sonst nicht mehr unterstützten WindowsXP und Windows-Server-2003-Systeme. Zudem wiesen Microsoft sowie verschiedene deutsche und internationale Sicherheitsbehörden und –dienstleister auf die Schwachstellen und die zur Verfügung stehenden Sicherheitsupdates hin.

Das BSI hat zu BlueKeep und DejaBlue Cyber-Sicherheitswarnungen und Pressemitteilungen veröffentlicht (vgl. *Quellenverzeichnis*[12]: www.bsi.bund.de).

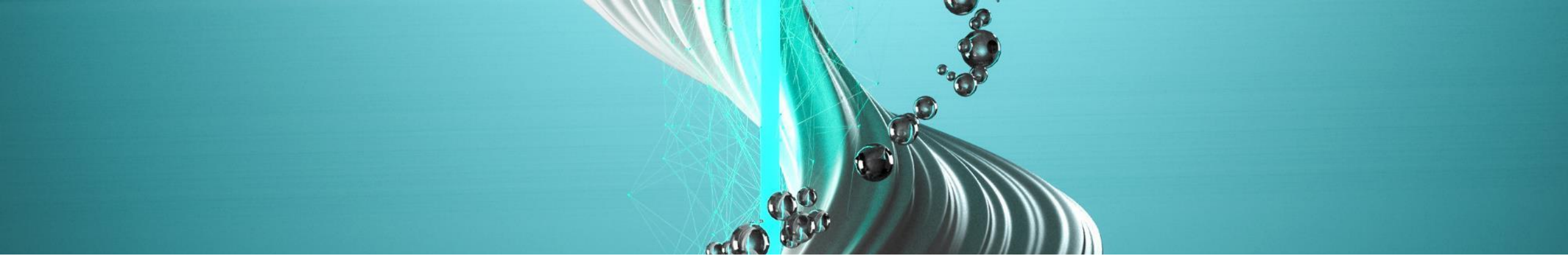
Empfehlung
Bereits bei der Einrichtung von Systemen sollten nur die Programme installiert und betrieben werden, die auch notwendig sind. Eine verkleinerte Angriffsfläche senkt das Risiko, Opfer eines Angriffs zu werden.

Wenn ein Sicherheitsupdate zur Verfügung steht, um eine Schwachstelle zu schließen, sollte dies umgehend installiert werden. In Fällen, in denen dies nicht möglich ist, sollten vorübergehende Lösungen geprüft werden, die die Ausnutzung der Schwachstelle verhindern. Mögliche vorübergehende Lösungen sind stark abhängig von der Art der Schwachstelle und dem betroffenen Dienst. Sie können beispielsweise in einer zeitweisen Abschaltung des jeweiligen Dienstes oder einer zeitweisen Nutzung einer alternativen Softwarekomponente liegen.

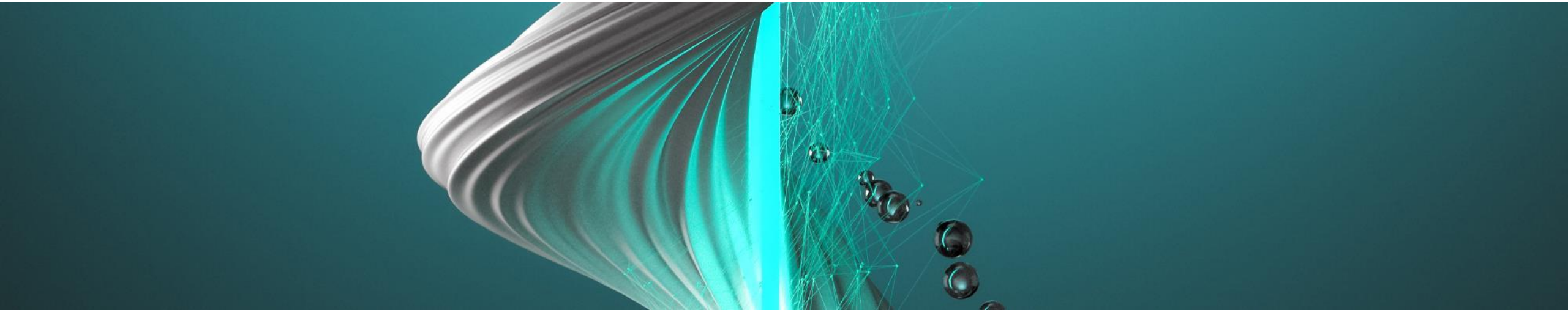
„Die Corona-Pandemie hat gezeigt, wie bedeutend funktionierende, sichere Informationstechnik ist, im privaten Alltag ebenso wie im globalen, wirtschaftlichen Miteinander."
Arne Schönbohm, Präsident des Bundesamtes für Sicherheit in der Informationstechnik

RDP
unter Beschuss

- Anstieg: + 4.256 Prozent
- täglich 14,3 Millionen Angriffe
- 166 Angriffe pro Sekunde



Faktor Mensch



Welche zentralen Herausforderungen sehen Unternehmen bei der Einrichtung von Home-Offices?

Erhöhtes Risiko für die IT-Sicherheit, das von menschlichem Verhalten verursacht wird

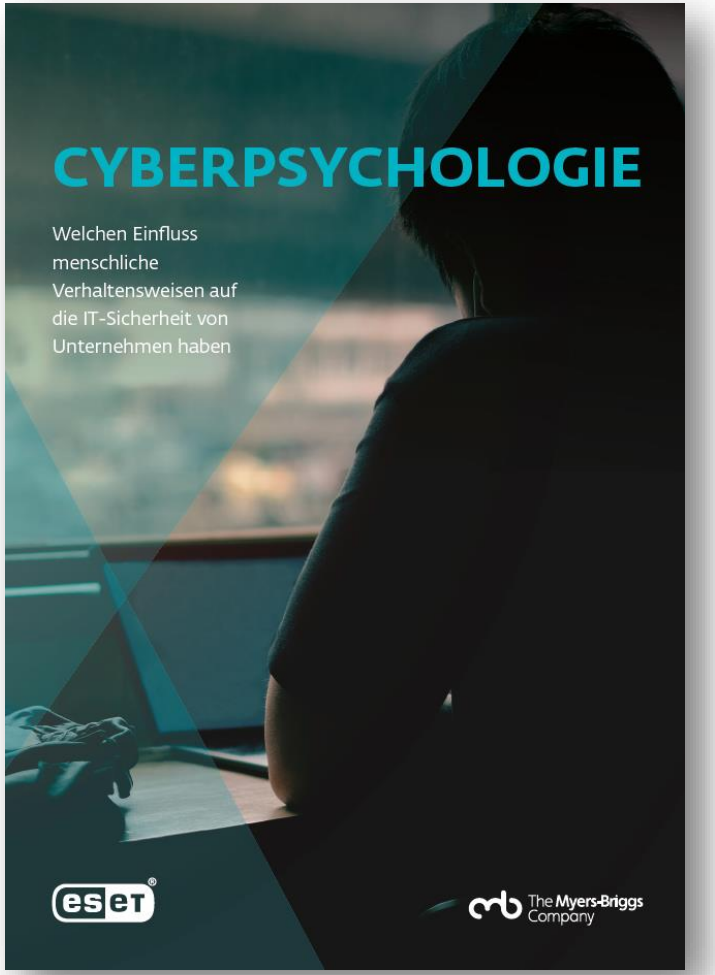
Zunahme von Cyberverbrechen

Integration neuer Lösungen und Systeme

Authentifizierung der Identität

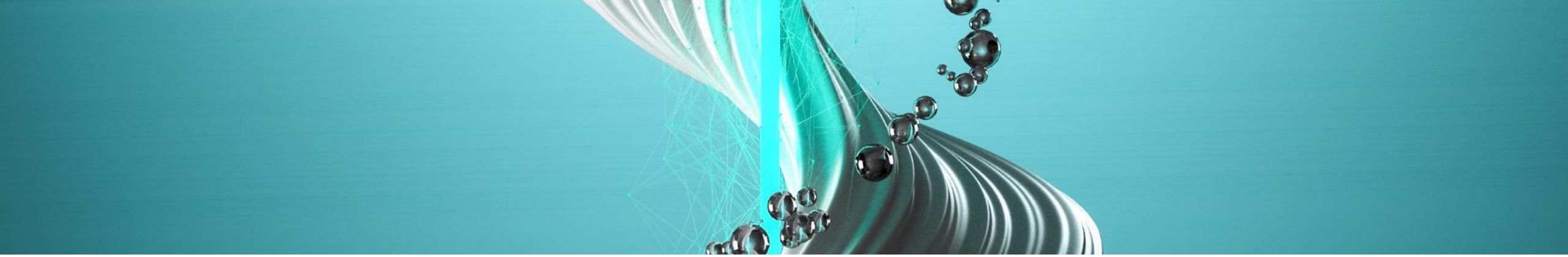
Notwendigkeit kurzfristiger Investitionen

Digitalisierung von Arbeitsplätzen und die Umstellung auf Mobile Working

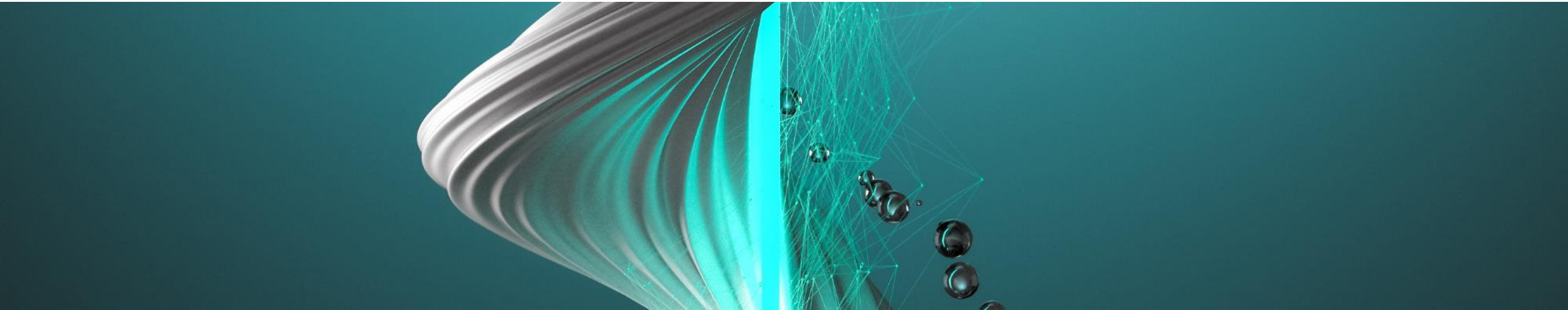


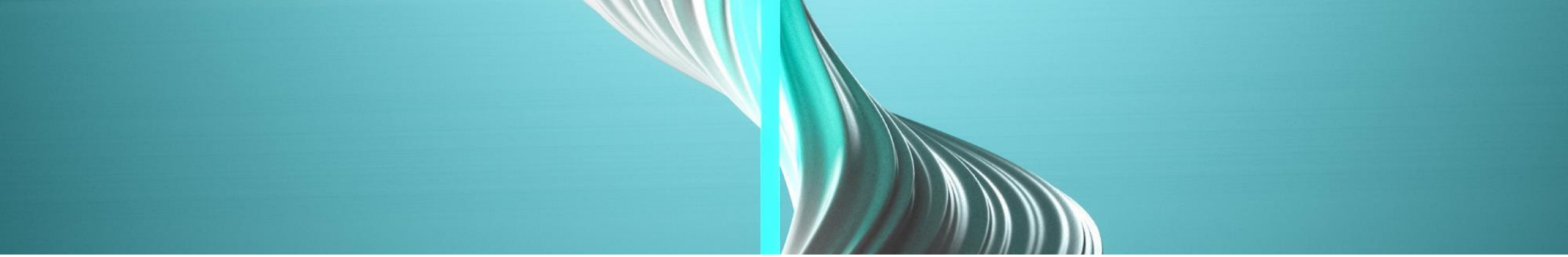
Cyberpsychologie: Welchen Einfluss menschliche Verhaltensweisen auf die IT-Sicherheit von Unternehmen haben

datasecurityguide.eset.com

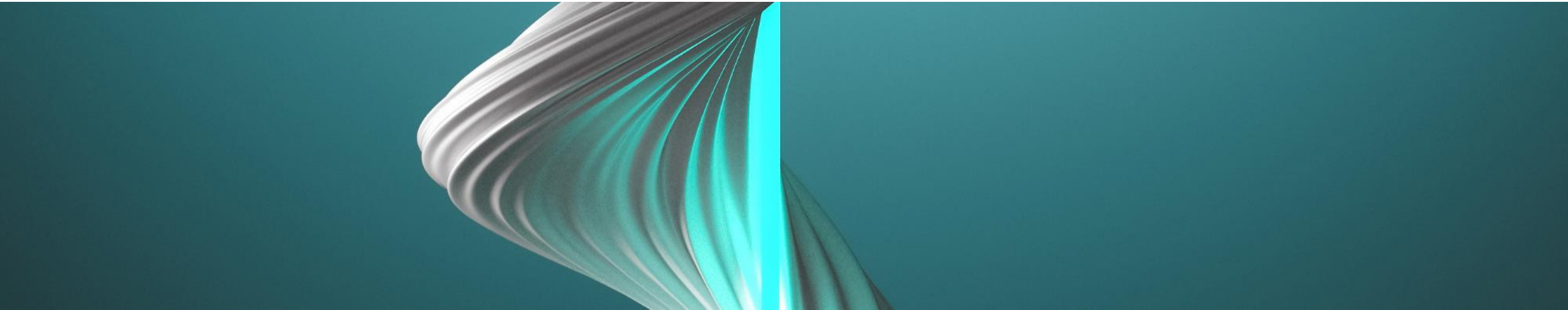


Welches Konzept hilft?

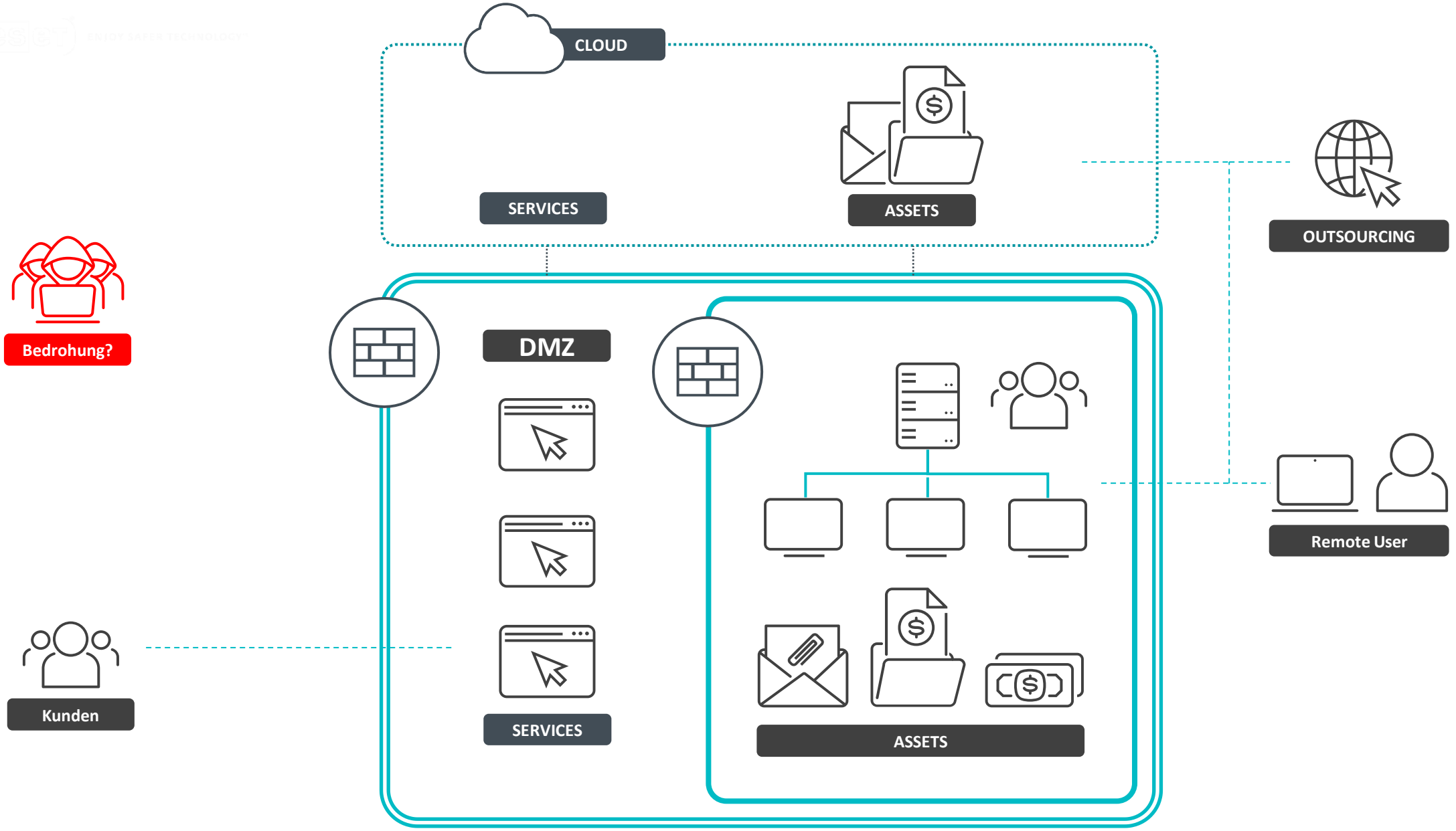


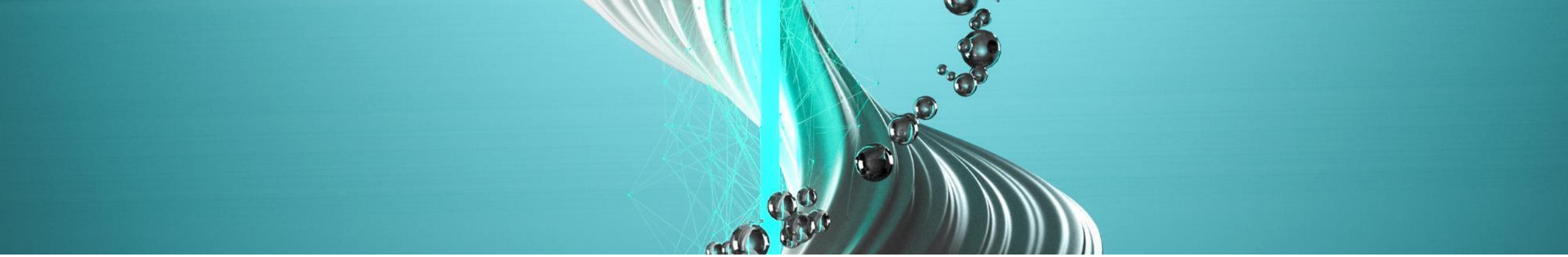


Zero-Trust-Security
Ganzheitlicher Handlungsansatz

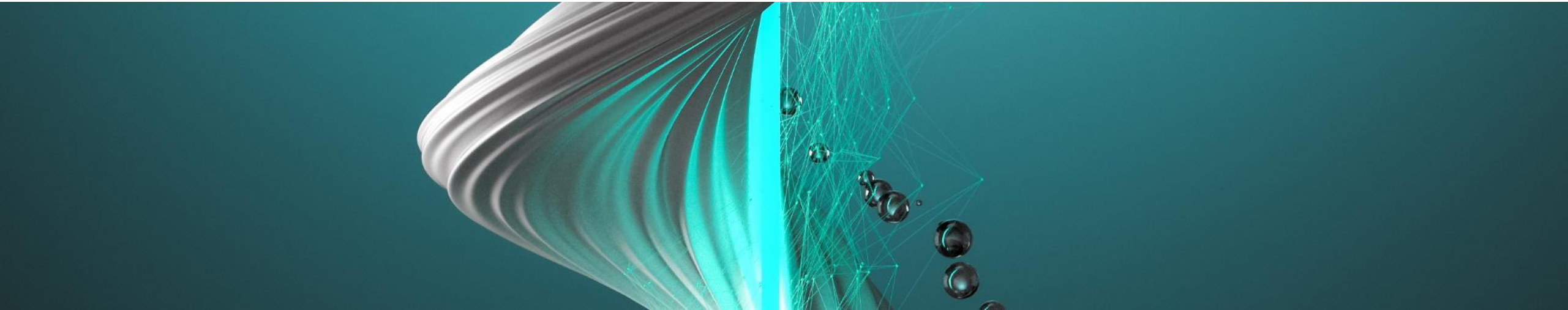


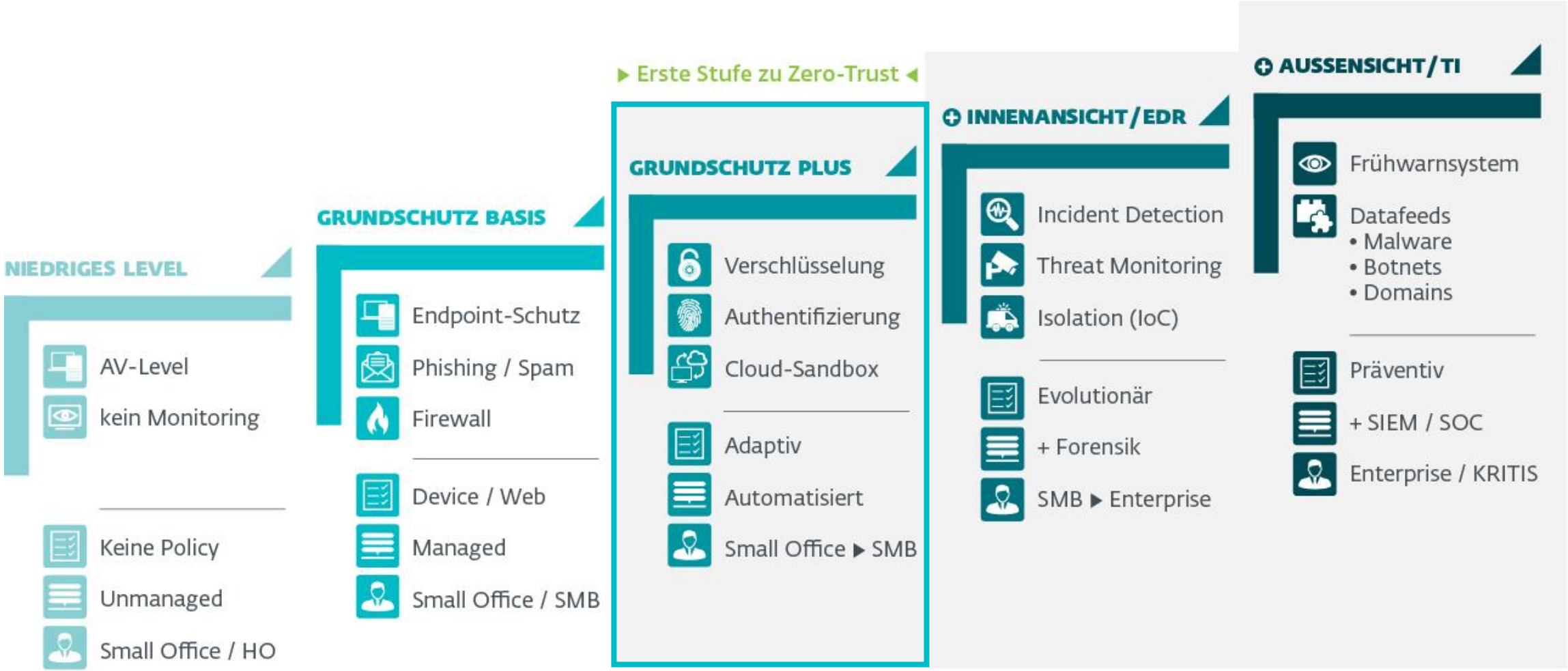

welivesecurity BY ESET
Menu
Exchange Server werden von mindestens 10 APT-Gruppen angegriffen
ESET Forscher haben ermittelt, dass unter anderem die Gruppen LuckyMouse, Tick, Winnti Group und Calypso weltweit Microsoft Exchange E-Mail-Server attackieren.
Matthieu Faou
Mathieu Tartare
Thomas Dupuy
10 Mar 2021 - 03:30PM
ESET
ENJOY SAFER TECHNOLOGY™


CLOUD
SERVICES
ASSETS
OUTSOURCING
Bedrohung?
DMZ
Remote User
Kunden
SERVICES
ASSETS

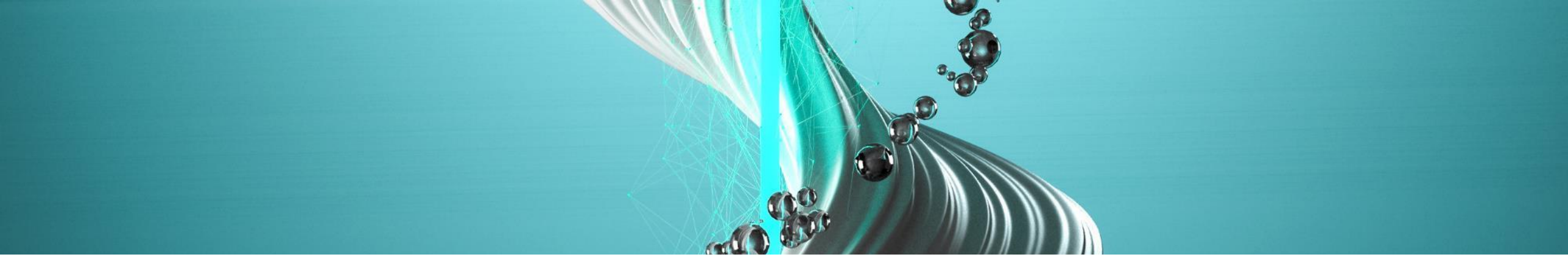


Der Weg:
Zero-Trust-Ansatz

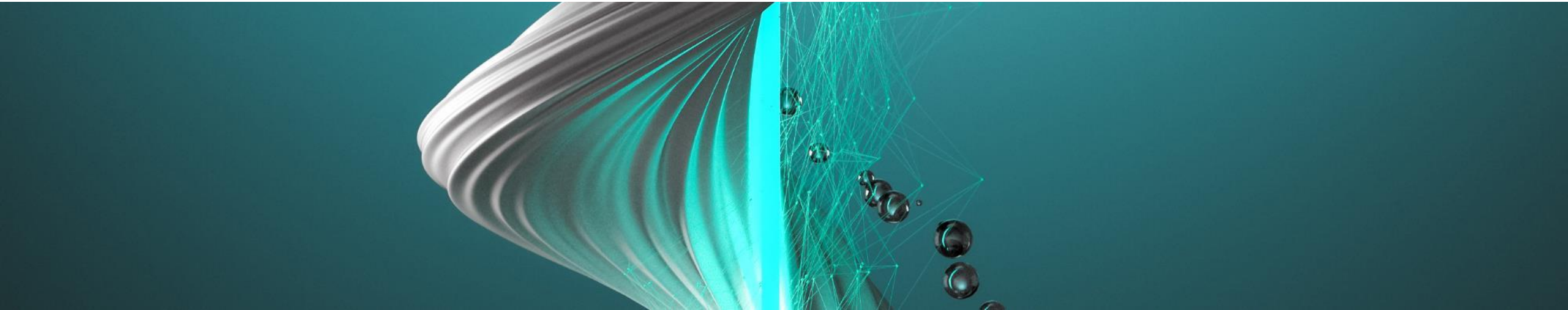


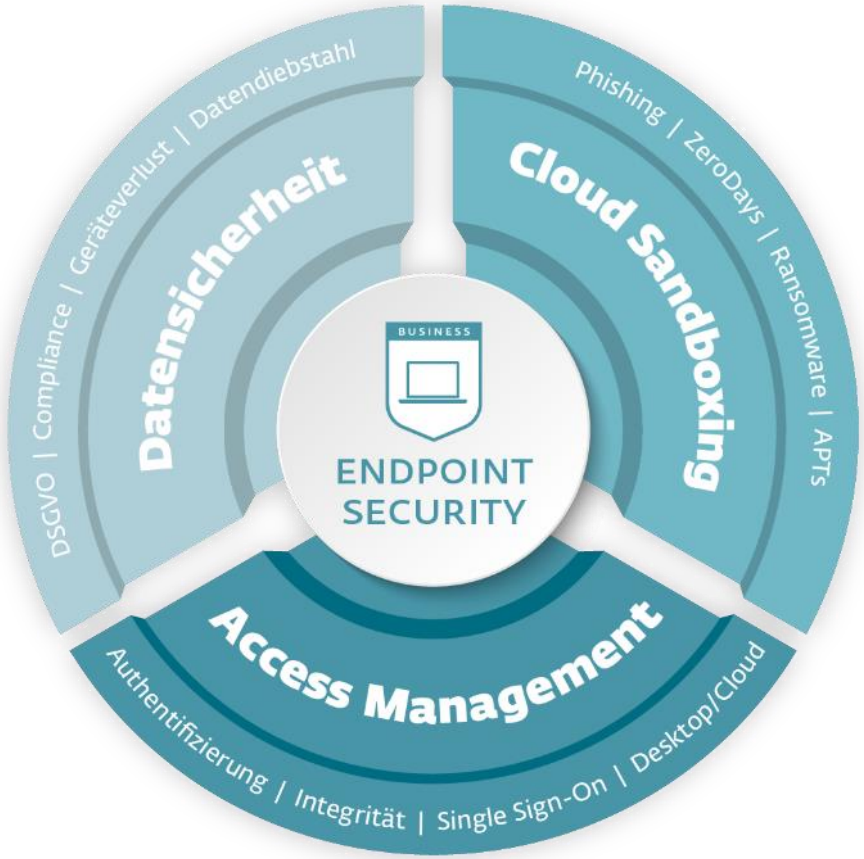


ESET Zero-Trust-Reifegradmodell

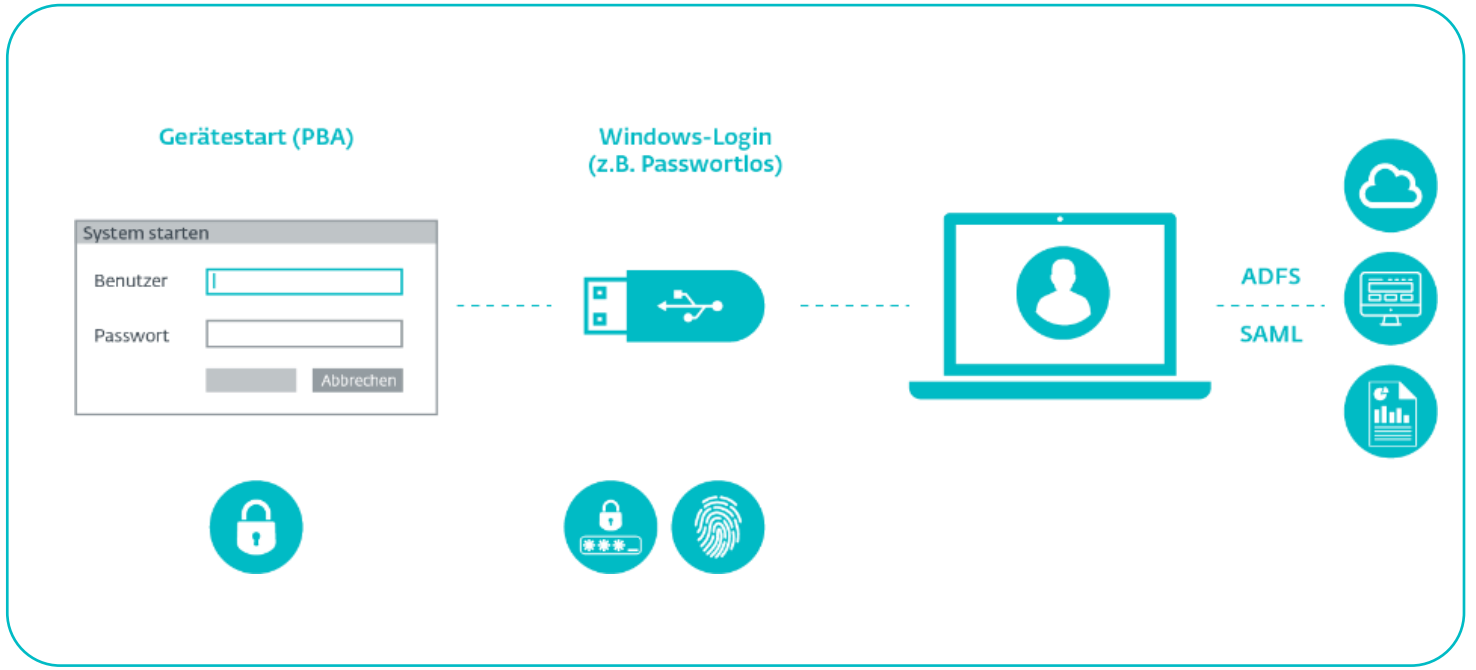


Zugänge zu Patientendaten schützen





Multi-Secured-Endpoint

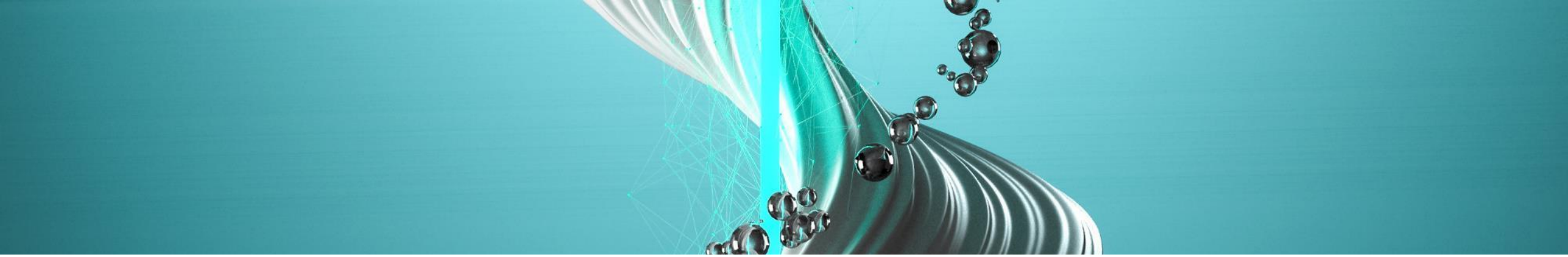


Multi-Faktor-Authentifizierung statt unsichere Passwörter mit ESET Secure Authentication

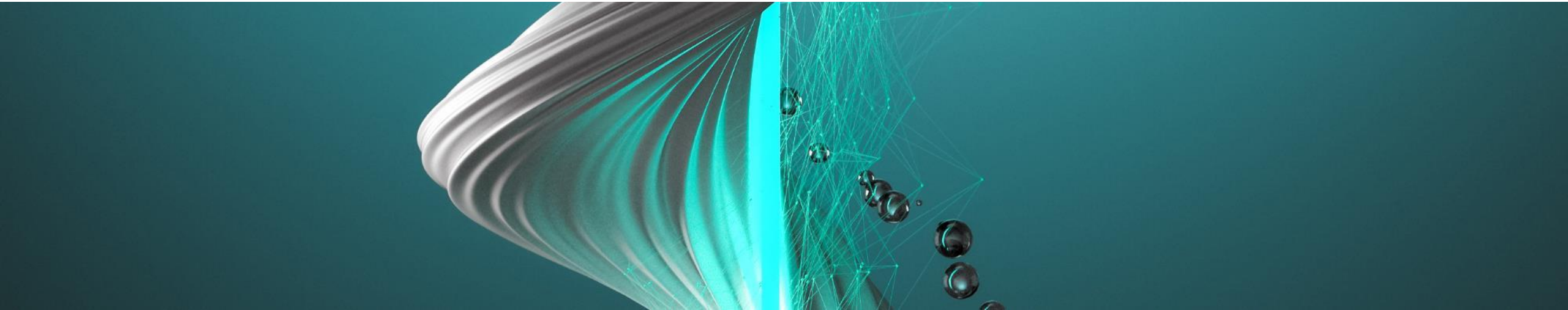
Secur|Ty made in EU
Trust Seal
www.teletrust.de/itsmie

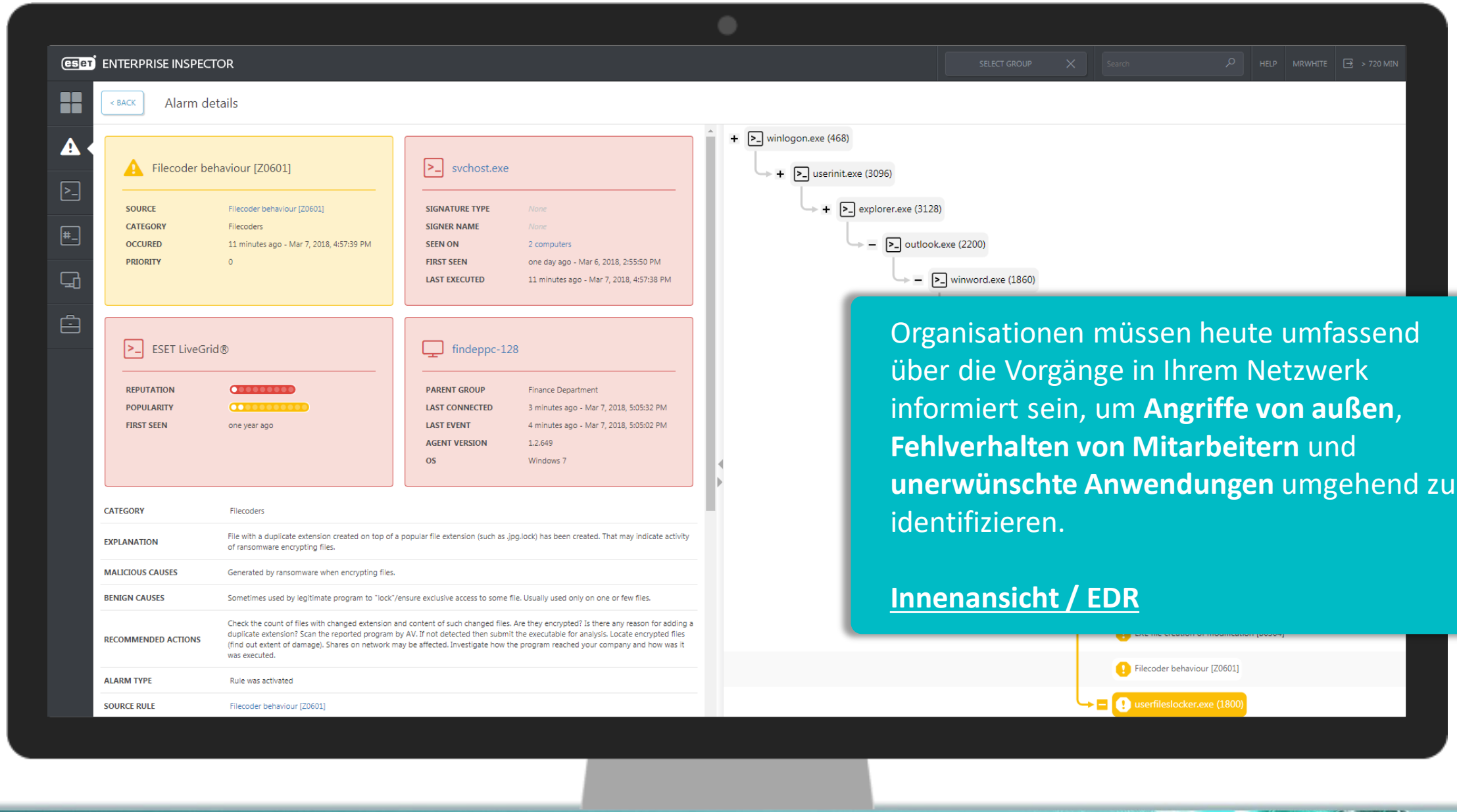
CERTIFIED ISO 27001:2013 COMPANY

CERTIFIED ISO 9001:2015 COMPANY



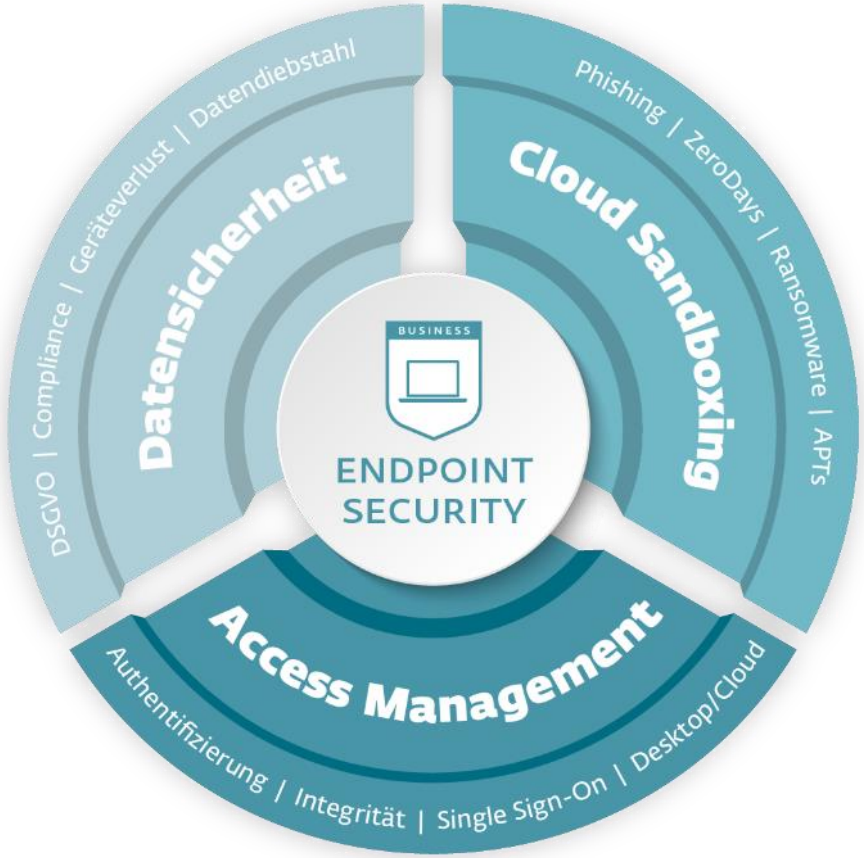
Datenabfluss erkennen und verhindern





Organisationen müssen heute umfassend über die Vorgänge in Ihrem Netzwerk informiert sein, um **Angriffe von außen**, **Fehlverhalten von Mitarbeitern** und **unerwünschte Anwendungen** umgehend zu identifizieren.

Innenansicht / EDR



Multi-Secured-Endpoint

ESET Deutschland GmbH
Spitzweidenweg 32
07743 Jena

Mehr Informationen auf
www.eset.de

Stay Safe !

CYBERSECURITY EXPERTS ON YOUR SIDE