IT SECURITY MADE IN EU

DIGITALE SOUVERÄNITÄT SETZT EINE STARKE IT-SECURITY VORAUS

Thorsten Urbanski

Head of Communication DACH

ESET Deutschland GmbH

Leiter der TeleTrust AG „IT Security made in EU“

ENJOY SAFER TECHNOLOGY™

Impulse

Thorsten Urbanski, ESET Deutschland, Leiter TeleTrusT-AG "IT Security made in EU" (ITSMIE)

- Warum Europa in puncto vertrauenswürdiger IT-Sicherheitslösung Vorreiter sein muss!
- Welche Kriterien sind in diesem Kontext von essenzieller Bedeutung und wofür steht ITSMIE?

RA Karsten U. Bartels, LLM., HK2, Stellv. TeleTrusT-Vorstandsvorsitzender, Leiter TeleTrusT-AG "Recht"

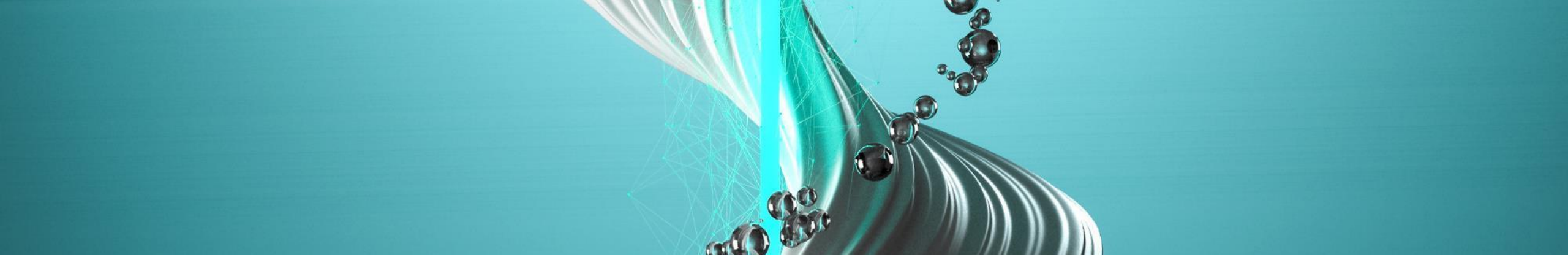
- IT-Sicherheit in der Pandemie-Praxis. Wie staatliche Desorientierung bei Vergabe, Nutzung und Aufsicht von IT die digitale Souveränität gefährdet.

Dr. André Kudra, esatus, TeleTrusT-Vorstandsmitglied, Leiter TeleTrusT-AG "Blockchain", Leiter TeleTrusT-AK "Secure Platform"

- Self-Sovereign Identity (SSI): Kernelement des europäischen Identitäts-Ökosystems und Digitalisierungs-Beschleuniger in einem.
- Digitale Souveränität geht nur mit sicheren Computing-Plattformen!

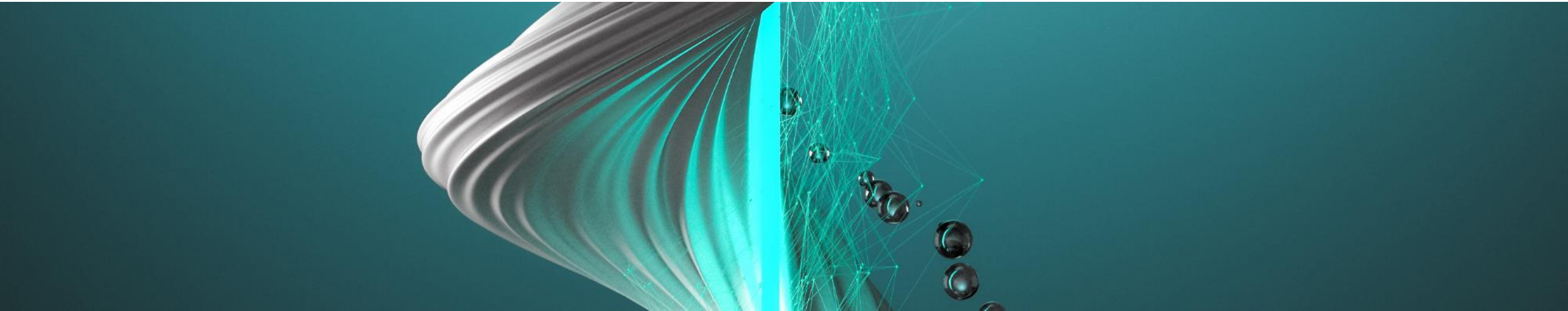
Markus Bartsch, TÜViT, Leiter TeleTrusT-AG "RSA"

- Quo Vadis Cyber Security: Warum Standards und Testverfahren für IT-Sicherheitstechnologien auf europäischer Ebene harmonisiert werden müssen.



Digitale Souveränität

Warum Europa in puncto vertrauenswürdiger IT-Sicherheitslösung Vorreiter sein muss!



DIME

Staatliche Dimension

ndividuelle Dimension

Wettbe

der EU

DIGITALE SO

TONOMIE

Handelsblatt

DIGITALISIERUNG

Appell von vier Regierungschefinnen an die EU: „Europa muss seine digitale Souveränität stärken“

In einem Brief wendet sich Kanzlerin Merkel mit ihren Amtskolleginnen aus Dänemark, Finnland und Estland an die EU-Kommissionschefin.

Angela Merkel, Mette Frederiksen, Kaja Kallas, Sanna Marin

02.03.2021 • Update: 02.03.2021 - 06:51 Uhr • 21 Kommentare • 55 x geteilt

Autorinnen

Angela Merkel sowie ihre Amtskolleginnen Kaja Kallas (Estland), Sanna Marin (Finland) und Mette Frederiksen (Dänemark) einen "Aktionsplan für mehr digitale Souveränität".


eu20
20.de

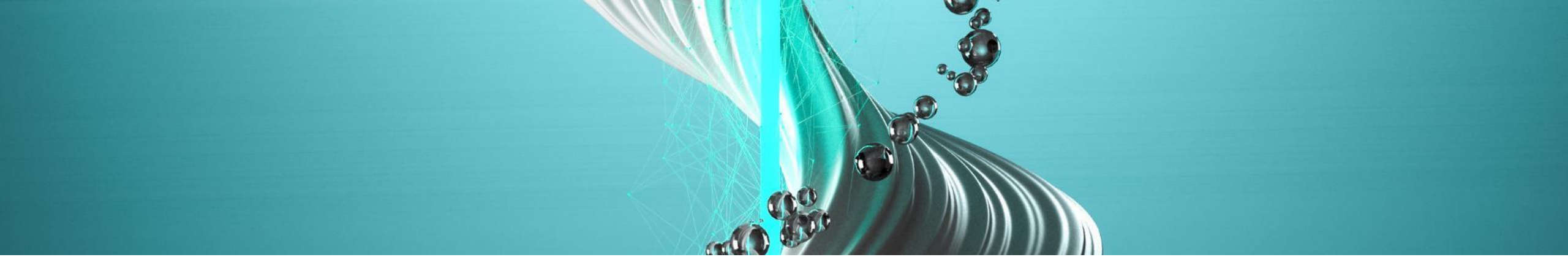
*„**Das übergreifende Ziel** bleibt dabei, **Europa schnell** und erfolgreich zu einer **Gigabit-Wirtschaft** und -**Gesellschaft** zu entwickeln. […]*

*Für diesen Wandel ist **eine sichere** und **souveräne**, **in Europa verortete**, **widerstandsfähige** und **nachhaltige digitale Infrastruktur** unabdingbar.*

„[…] Wenn die EU in einer Technologiesparte, die von den Vereinigten Staaten und China dominiert wird, wettbewerbsfähig bleiben möchte, ist die Schaffung dieses dediziert europäischen digitalen Wirtschaftsraums von zentraler Bedeutung.“

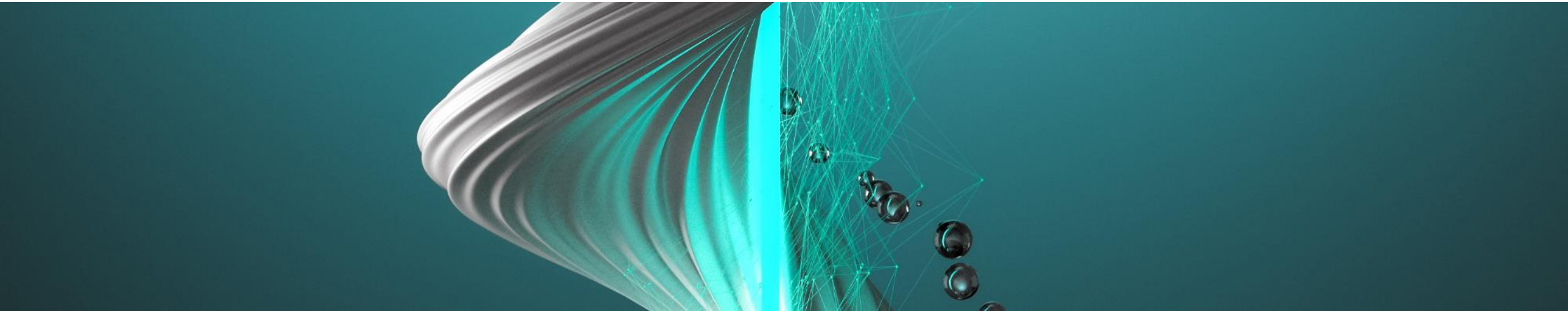
eu2020.de

Bundesministerium für Wirtschaft und Energie

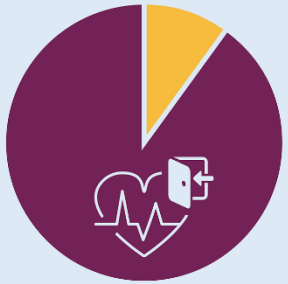


Erwartungshaltung EU-Bürger

Beispiel HC



Was EU-Bürger von der Digitalisierung im Gesundheitswesen erwarten



90%

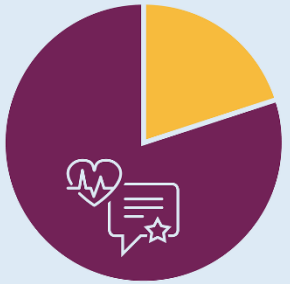
der Europäer

haben die Erwartung, dadurch Zugang zu ihren eigenen Gesundheitsdaten zu haben, wofür kompatible und hochwertige Gesundheitsdaten notwendig sind

80%

der Europäer

würden ihre Daten zur Verfügung stellen, wenn Datenschutz und Datensicherheit gewährleistet wären



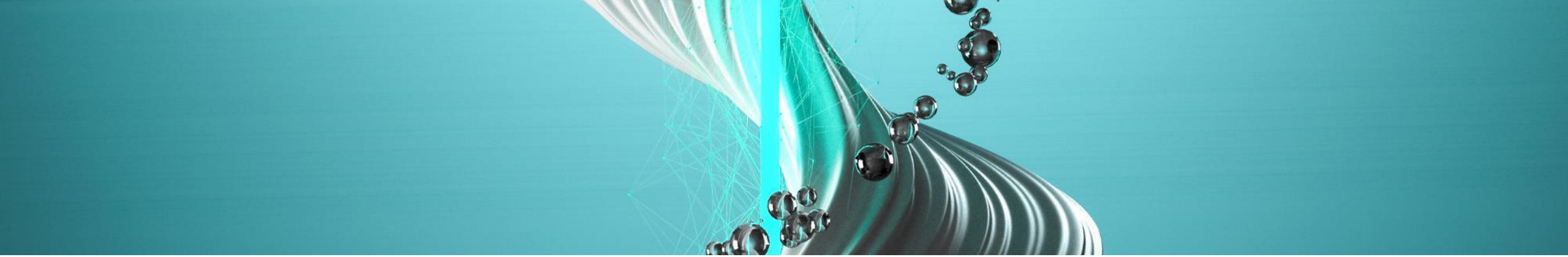
80%

der Europäer

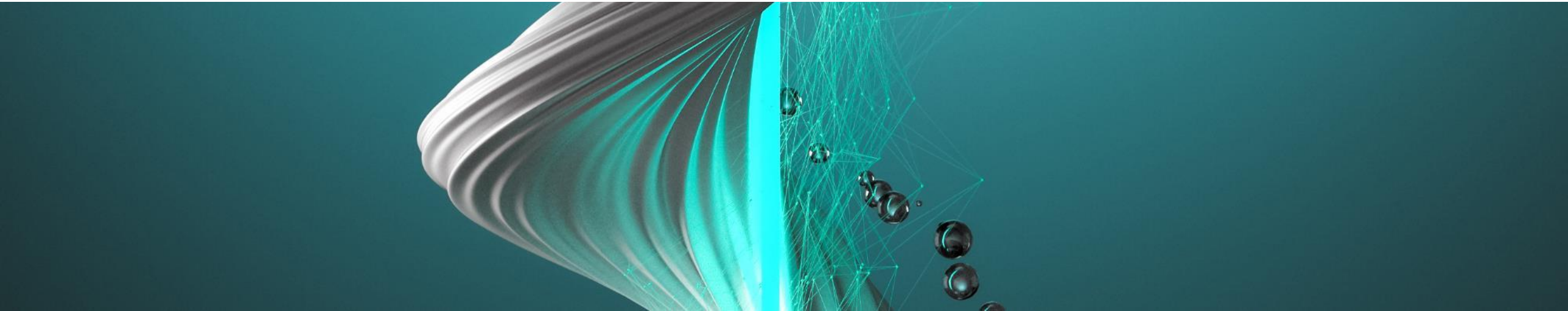
würden eine Bewertung hinsichtlich der Qualität medizinischer Behandlungen abgeben, wenn es derartige digitale Möglichkeiten und die entsprechende Infrastruktur für ein patientenzentriertes Gesundheitswesen gäbe

Quelle: Europäische Kommission/GD Steuern und Zollunion

eu2020.de

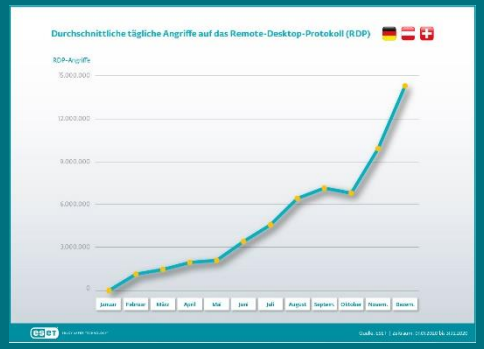


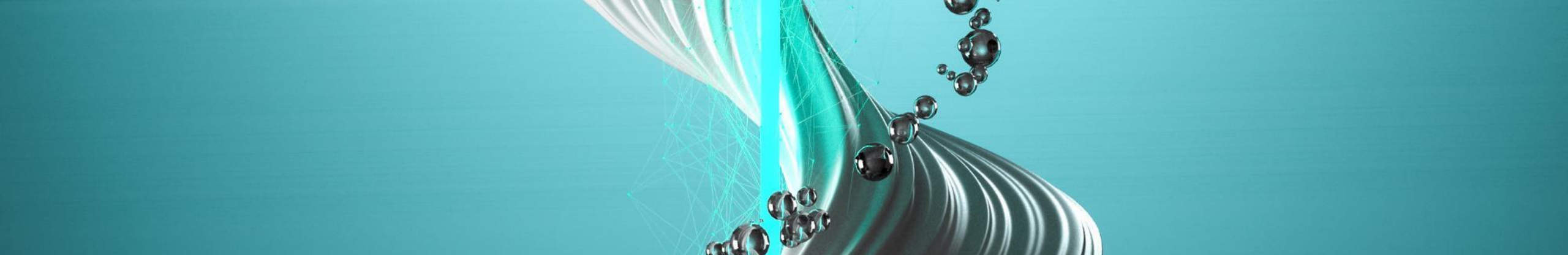
OHNE EIGENE/ WERTEBASIERTE IT-SECURITY-INDUSTRIE NICHT REALISIERBAR!



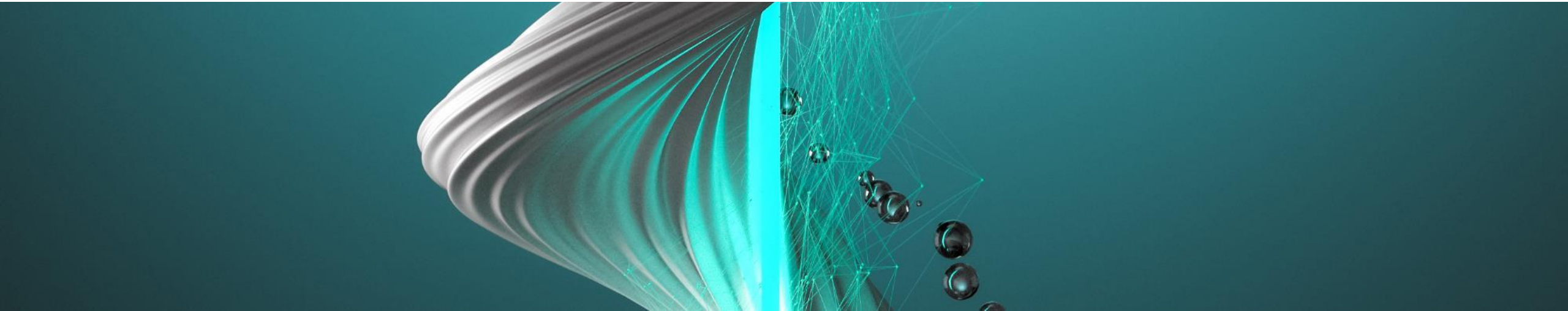
Home-Office unter Beschuss

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





ITSMIE



TeleTrust-Initiative „IT Security made in EU“

1. Der **Unternehmenshauptsitz** muss in der **EU** sein.
2. Das Unternehmen muss **vertrauenswürdige IT-Sicherheitslösungen** anbieten
3. Die angebotenen Produkte dürfen **keine versteckten Zugänge** enthalten (keine "Backdoors").
4. Die **IT-Sicherheitsforschung und -entwicklung des Unternehmens** muss **in der Europäischen Union** stattfinden.
5. Das Unternehmen muss sich verpflichten, den Anforderungen der **EU-Datenschutz-Grundverordnung** zu genügen.

Vielen Dank!
ESET Deutschland
Thorsten Urbanski, Head of Communication DACH
Thorsten.Urbanski@eset.de
www.eset.de
Tel. 036 41.31 14 261

ESET Security-Blog: www.welivesecurity.de

Stay Safe !

CYBERSECURITY EXPERTS ON YOUR SIDE

Vielen Dank!

ESET Deutschland
Thorsten Urbanski, Head of Communication DACH
Thorsten.Urbanski@eset.de
www.eset.de
Tel. 036 41.31 14 261

ESET Security-Blog: www.welivesecurity.de

- März 2021:
  Covid-19 Pandemie als Kriminalitätstreiber
- Bis Ende 2020 Steigerung: von 768% bei Attacken per RDP allein in DACH
- Zunahme von Watering Hole Attacken auf Regierungen (Asien)
- Allein in Q4 2020 so viele Supply-Chain-Attacken wie zuvor jährlich (SolarWinds, Microsoft Exchange/SharePoint, Centreon)
- 23% aller erfolgreichen Angriffe von Insidern - (Ex-)Beschäftigte & Partner, Anstieg der Fallzahlen um 47% von 2018 zu 2020