Das CYBER.VET.EU-Handbuch

Verbesserung der Cybersecurity-Bereitschaft des europäischen Berufsbildungssektors

2020-1-DE02-KA226-VET-008327

TANDEM PLUS NETWORK mit dem CYBER.VET.EU-Konsortium:

Co-funded by the
Erasmus+ Programme
of the European Union

Co-funded by the
Erasmus+ Programme
of the European Union

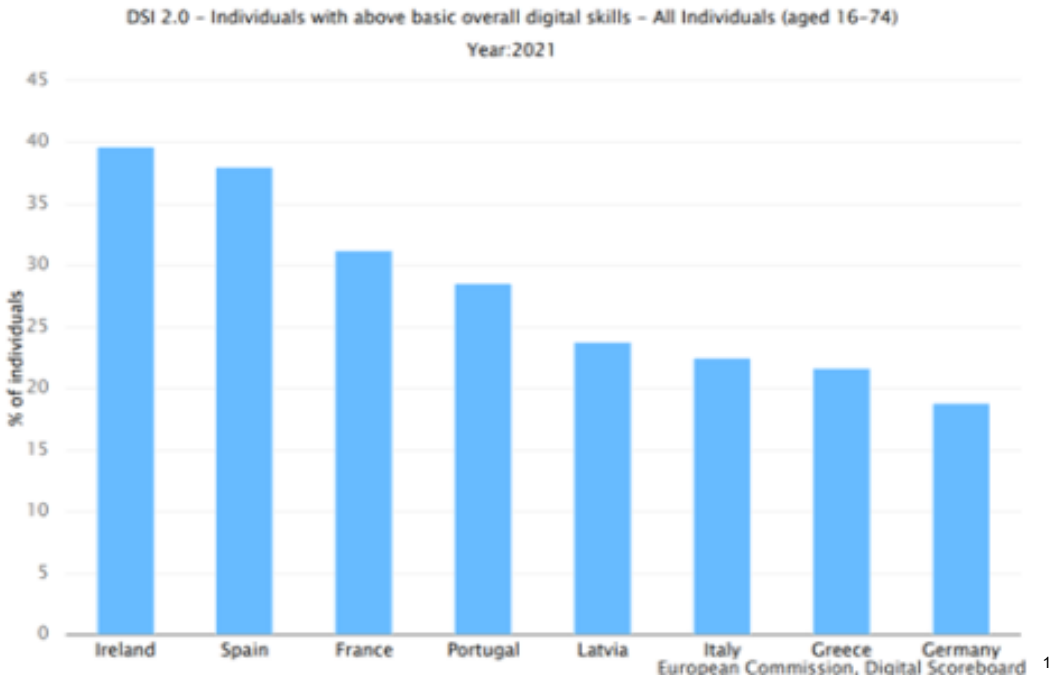
Zusammenfassung

a) Die Durchführung des CYBER.EU.VET-Projekts

Die Europäische Union steht vor einer epochalen Herausforderung, die die Covid-19-Pandemie darstellt. Viele Bereiche sind von dieser Krise stark betroffen, und die Bildung ist sicherlich einer davon.
Immer mehr Nutzer sind heute gezwungen, Online-Kurse oder -Schulungen zu nutzen. Daher ist es wichtiger denn je, die täglichen Bedrohungen für unsere Sicherheit zu erkennen. Dieses Thema wird auch von der Europäischen Kommission als grundlegend anerkannt, die jedes Jahr einen Europäischen Monat der Cybersicherheit organisiert, dessen Website bereits einige Bildungsmaterialien und spezifische Sensibilisierungskampagnen wie die "Get cyber skilled" im Jahr 2018 enthält.

Das Projekt **CYBER.EU.VET** umfasst 8 Partner:

NGO NEST BERLIN - Deutschland (Projektkoordinator)
MEATH COMMUNITY RURAL AND SOCIAL DEVELOPMENT PARTNERSHIP LIMITED – Irland
TANDEM PLUS - ein EU-Netzwerk mit Sitz in Frankreich
COFAC COOPERATIVA DE FORMACAO E ANIMACAO CULTURAL CRL – Portugal
LATVIJAS ASOCIACIJA EIROPAS KOPIENAS STUDIJAM – Lettland
ASOCIACION EDUCATIVA POR LA INTEGRACION Y LA IGUALDAD – Spanien
INERCIA DIGITAL – Spanien
EXTRAFONDENTE OPEN SOURCE - Italien



[1]

Das Hauptziel von **CYBER.EU.VET** ist es, die Fähigkeit der europäischen Berufsbildung zu stärken, Cybersecurity-Bedrohungen (z.B. Phishing-Attacken, Botnets, Finanz- und Bankbetrug, Datenbetrug) in einem historischen Kontext zu erkennen und zu bewältigen, in dem Online-Schulungen mehr und mehr genutzt werden.

i. Auswirkungen des Projekts:

Das Projekt wirkte sich auf lokaler, regionaler und nationaler Ebene aus, indem es verschiedene Ebenen von Interessenvertretern einbezog und Lösungen anbot, die auf die Anforderungen der lokalen Ebene zugeschnitten, aber auf einer höheren Ebene abgestimmt sind, indem es im Rahmen der Partnerschaft EU-weit anwendbares Schulungsmaterial und Standards entwickelte.

Die Auswirkungen auf die direkten Teilnehmer und die Hauptzielgruppen waren besonders groß:

- Lehrkräfte in der beruflichen Bildung - Stärkung der Lehrkapazität, indem sie ihre Kenntnisse über die wichtigsten digitalen Sicherheitsbedrohungen erweitern.

[1] ESMS-Indikatorprofil (ESMS-IP) Erstellende Stelle: Eurostat, das statistische Amt der Europäischen Union.

- Lehrende und Lernende in der beruflichen Bildung - verbesserte digitale Kompetenzen dank des Schulungsmaterials.
- Lehrende und Lernende in der beruflichen Bildung: eine stärkere Sensibilisierung für die Bedrohungen und ihre tatsächlichen Risiken, sowohl in wirtschaftlicher als auch in sozialer Hinsicht.
- Berufsbildungseinrichtungen werden mit den CYBER.VET.EU-Instrumenten sowohl für ihre Lehrkräfte als auch für ihre Schüler besser auf die Risiken der Cybersicherheit vorbereitet sein.

ii. Projektziel

Es wird erwartet, dass das Projekt positive und langfristige Auswirkungen auf die verschiedenen am Projekt beteiligten Akteure haben wird:

- - Studenten der beruflichen Bildung
- - Freiwillige Cybersecurity-Experten
- - Netzwerke von Berufsbildungseinrichtungen
- Politische Entscheidungsträger

iii. Ziele des Projekts CYBER.EU.VET:

- Das erste spezifische Ziel besteht darin, die Ausbilder in der beruflichen Bildung besser auf die Bewältigung von Cybersicherheitsbedrohungen vorzubereiten, da sie eine zentrale Rolle bei der Vermittlung von bewährten Verfahren und Fähigkeiten an ihre Schüler spielen.
- Das zweite spezifische Ziel ist die Sensibilisierung von Lehrkräften in der beruflichen Bildung, Schülern und ihren Angehörigen für die Bedeutung der Erkennung solcher täglichen Risiken, die sowohl wirtschaftliche als auch soziale Auswirkungen auf alle europäischen Bürger haben können.
- Das dritte spezifische Ziel besteht darin, öffentliche Einrichtungen und Berufsbildungseinrichtungen zu unterstützen, damit sie besser auf derartige Herausforderungen vorbereitet sind, und ihnen Leitlinien für künftige Umsetzungen an die Hand zu geben.

iv. Intellektuelle Leistungen:

- O1: Forschungsanalyse: wichtigste Herausforderungen im Bereich der Cybersicherheit und bewährte Verfahren (verantwortlicher Partner: NGO NEST BERLIN - E10166639)
- O2: Schulungsmaterial zum Thema Cybersicherheit für den Berufsbildungssektor (verantwortlicher Partner: INERCIA DIGITAL SL (E10145080)
- O3: Toolkit für die Ausbildung von Ausbildern (verantwortlicher Partner INERCIA DIGITAL SL (E10145080)
- O4: Das Cybersicherheitshandbuch für Berufsbildungseinrichtungen: bewährte Verfahren, Schulungsmaterial und Leitlinien für künftige Implementierungen (Verantwortlicher Partner TANDEM PLUS - E10103913)

Parallel zur Entwicklung der intellektuellen Ergebnisse besteht das andere Ziel des Projekts in der EU-weiten Verbreitung unserer Ergebnisse an potenzielle Teilnehmer, Multiplikatoren und interessierte Stakeholder, um die Wirkung und Relevanz von CYBER.EU.VET zu steigern.

v. Was ist Cybersicherheit?

Die formale Definition von **Cybersicherheit** im EU-Recht findet sich im Text des EU-Cybersicherheitsgesetzes: "*Cybersicherheit bezeichnet die Maßnahmen, die zum Schutz von Netz- und Informationssystemen, der Nutzer solcher Systeme und anderer Personen, die von Cyberbedrohungen betroffen sind, erforderlich sind*" (Artikel 2 Absatz 1).

Das EU-Recht verfolgt zwar den Ansatz des "*Schutzes von Netz- und Informationssystemen*", betont aber auch, dass die Cybersicherheit nicht nur Informationssysteme, sondern auch (und vielleicht noch wichtiger) Personen schützt, unabhängig davon, ob die Nutzer solcher Systeme oder Dritte in irgendeiner Weise von Cyberbedrohungen betroffen sind.

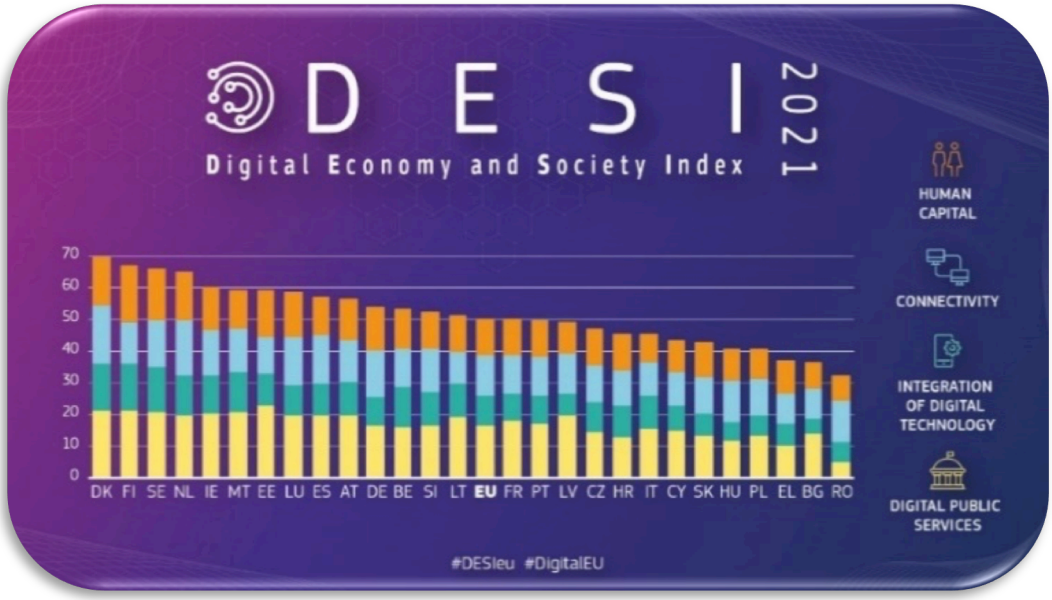
Im Dezember 2020 stellten die Europäische Kommission und der Europäische Auswärtige Dienst (EAD) eine neue EU-Cybersicherheitsstrategie vor, die darauf abzielt, die

Widerstandsfähigkeit gegenüber Cyberbedrohungen zu erhöhen und sicherzustellen, dass Bürger und Unternehmen von vertrauenswürdigen digitalen Technologien profitieren.

Mit der Verordnung (EU) 2021/887 zur Einrichtung des Europäischen Kompetenzzentrums für Cybersicherheit in Industrie, Technologie und Forschung und des Netzes der nationalen Koordinierungszentren werden das Europäische Kompetenzzentrum für Cybersicherheit (ECCC) und das Netz der nationalen Koordinierungszentren (das "Netz") eingerichtet und die Regeln für die nationalen Koordinierungszentren (NCC) und die Einrichtung der Kompetenzgemeinschaft für Cybersicherheit festgelegt.

Das Europäische Kompetenzzentrum für Cybersicherheit hilft der EU, ihre Führungsrolle im Bereich der Cybersicherheit[2] zu stärken, indem es das Vertrauen und die Sicherheit, einschließlich der Vertraulichkeit, Integrität und Zugänglichkeit von Daten, verbessert und die Widerstandsfähigkeit und Zuverlässigkeit von Netzen und Informationssystemen, einschließlich kritischer Infrastrukturen und häufig verwendeter Hard- und Software, unterstützt.

[2] Verordnung (EU) 2021/887 des Europäischen Parlaments und des Rates vom 20. Mai 2021 zur Einrichtung des Europäischen Kompetenzzentrums für Cybersicherheit in Industrie, Technologie und Forschung sowie des Netzes der nationalen Koordinierungszentren (ABl. L 202 vom 8.6.2021, S. 1-31)



vi. Die größte Herausforderung für digitale Kompetenzen in Europa

- Etwa 70 Millionen Europäer verfügen nicht über ausreichende Lese-, Schreib- und Rechenkenntnisse
- 24 % der EU-Bevölkerung hat keinen Abschluss der Sekundarstufe II
- 13 % der Europäer haben das Internet noch nie genutzt
- 43 % der EU-Bevölkerung und 35 % der EU-Arbeitskräfte verfügen über unzureichende digitale Kompetenzen
- 42 % der Personen ohne digitale Kenntnisse sind arbeitslos
- Digital Natives ≠ digitale Kompetenz[3]

[3] Referenzen: DESI-Bericht 2018 - Humankapital; Bildungs- und Ausbildungsmonitor 2017, Skills Communication 2016, ICILS 2013

vii. Hintergrund

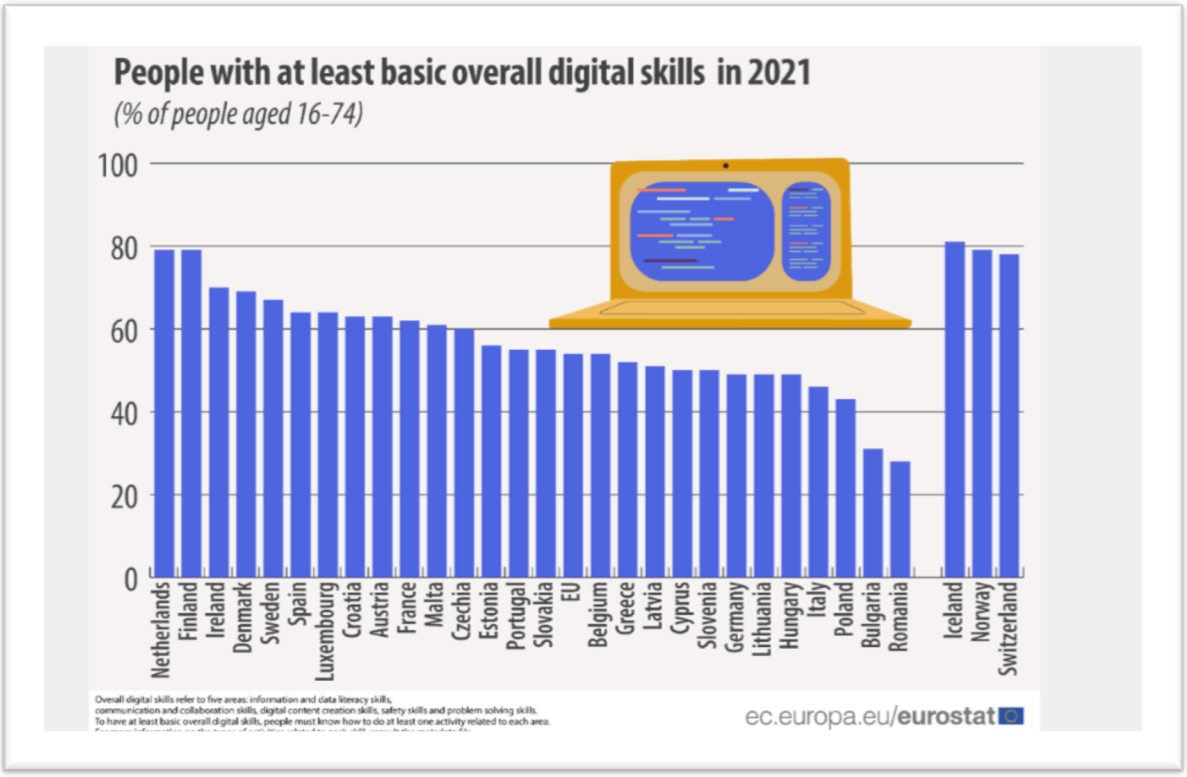
Über 70 % der Unternehmen gaben an, dass der Mangel an Mitarbeitern mit angemessenen digitalen Fähigkeiten ein Investitionshindernis darstellt. Auch in Europa mangelt es an digitalen Experten, die Spitzentechnologien zum Nutzen aller Bürgerinnen und Bürger entwickeln können.

Eine starke digitale Wirtschaft, die von Europäern mit digitalen Fähigkeiten angetrieben wird, ist entscheidend für Innovation, Wachstum, Arbeitsplätze und die europäische Wettbewerbsfähigkeit. Die Verbreitung digitaler Technologien hat massive Auswirkungen auf den Arbeitsmarkt und die Art der in Wirtschaft und Gesellschaft benötigten Qualifikationen. Die Mitgliedstaaten, Unternehmen, Bildungsanbieter, die Europäische Kommission und andere Organisationen müssen zusammenarbeiten, um die digitale Qualifikationslücke zu schließen. Um die Entwicklung des digitalen Wandels und der digitalen Qualifikationslücke zu verfolgen, veröffentlicht die Kommission jährlich den DESI [Digital Skills Indicator]. Darin werden die digitalen Leistungen der Mitgliedstaaten in verschiedenen Bereichen verfolgt, um die Fortschritte zu überwachen und festzustellen, wo weitere Anstrengungen erforderlich sind.

Im Jahr 2021 verfügten 54 % der Menschen in der EU im Alter von 16 bis 74 Jahren zumindest über grundlegende digitale Kenntnisse.

Im Jahr 2021 war der Anteil der 16- bis 74-Jährigen, die zumindest über grundlegende digitale Kenntnisse verfügten, in den Niederlanden und Finnland (beide 79%) am höchsten, gefolgt von Irland (70%). Der niedrigste Anteil wurde dagegen in Rumänien (28 %) verzeichnet, gefolgt von Bulgarien (31 %) und Polen (43 %).

Indikatoren für digitale Kompetenzen gehören zu den wichtigsten Leistungsindikatoren im Rahmen der Digitalen Dekade, in der die Vision der EU für den digitalen Wandel dargelegt wird. Im Digitalen Kompass wird das Ziel formuliert, dass bis 2030 80 % der EU-Bürgerinnen und -Bürger im Alter von 16 bis 74 Jahren zumindest über digitale Grundkenntnisse verfügen sollen.



Zurück zum Inhalt ☐

b) Digitale Fähigkeiten von Lehrkräften in der Berufsbildung - ein Einblick des Konsortiums

i. Deutschland:

Der vom Bundesinstitut für Berufsbildung (BIBB) erstellte Berufsbildungsdatenreport (2019) stellt fest, dass "die Digitalisierung den Strukturwandel auf dem Arbeitsmarkt verstärken wird", was eine Verlagerung der Ausbildungskapazitäten in den jeweiligen Bereichen erforderlich macht.

Wie im Beschluss der Kultusministerkonferenz (2016-2017) für den Bereich der beruflichen Bildung dargelegt, ist die Förderung berufsbezogener Kompetenzen im Kontext digitaler Arbeits- und Geschäftsprozesse ein wesentlicher Teil der Kompetenz der Lehrkräfte als Ausgangspunkt für ihre didaktische Tätigkeit.

ii. Irland:

Eine der wichtigsten Strategien Irlands in Bezug auf die digitalen Kompetenzen von Lehrkräften in der beruflichen Bildung ist die nationale digitale Strategie, die im Juli 2013 ins Leben gerufen wurde. Die Strategie konzentriert sich auf das digitale Engagement und zeigt auf, wie Irland von einer digital engagierten Gesellschaft profitieren kann.

In Bezug auf die digitalen Kompetenzen von Lehrkräften in der beruflichen Bildung wird immer deutlicher, dass die Kluft zwischen Lehrkräften, die digitale Geräte in ihrem Unterricht als Lernmittel einsetzen, und solchen, die dies nicht tun, immer größer wird.

iii. Portugal:

Das nationale Qualifikationssystem hat die Berufsbildung zu einem einzigen System umgestaltet, in dem die Programme zu einer doppelten Zertifizierung führen. Die Berufsbildung für Erwachsene ist ein integraler Bestandteil des nationalen Qualifikationssystems, mit Bildungs- und Ausbildungsprogrammen für Erwachsene und der Anerkennung und Validierung früherer Lernerfahrungen als Schlüsselelemente. Portugal hat erhebliche Fortschritte bei den Bildungsabschlüssen gemacht, die jedoch weiterhin unter dem EU-Durchschnitt liegen. Obwohl weniger als 2015 (73,7 %), lag

der Anteil der Menschen mit niedrigem Niveau oder ohne Qualifikation 2019 bei 50,2 % und war damit der höchste in der EU.

iv. Italien:

Im Bildungsbereich wurden die Maßnahmen hauptsächlich durch die Umsetzung des nationalen Plans für digitale Schulen durchgeführt. Mit den Leitlinien des Ministeriums für Bildung, Universität und Forschung wurde eine umfassende Innovationsstrategie für die italienische Schule und für eine Neupositionierung des Bildungssystems im digitalen Zeitalter eingeleitet. Die meisten Maßnahmen zur Schulung des Schulpersonals waren auf Grund- und Sekundarschulen ausgerichtet, die die Mehrheit der Schulen in Italien ausmachen, während dem Bereich der beruflichen Aus- und Weiterbildung (VET) wenig Aufmerksamkeit geschenkt wurde.

v. Spanien:

Die 2013 veröffentlichte Digitale Agenda für Spanien (ADpE, Agenda Digital para España) ist der Fahrplan für die Verwirklichung der in der Digitalen Agenda für Europa festgelegten Ziele für 2015 und 2020 sowie für die Erreichung spezifischer Ziele für die Entwicklung der Wirtschaft und der digitalen Gesellschaft in Spanien. Er ist in sechs Hauptziele und mehrere spezifische Pläne gegliedert. Das sechste Ziel betrifft die Förderung der digitalen Integration und der digitalen Kompetenz sowie die Ausbildung neuer IKT-Fachleute.

vi. Frankreich

Betrachtet man das Tempo der IKT-Schulungen an den französischen Universitäten, die diese anbieten, so stellt man fest, dass es keine klaren und nachhaltigen Strategien für die Schulung der Ausbilder in der Nutzung von IKT/E gibt. Etwa 58 % geben an, nur eine Schulung pro Jahr zu absolvieren, gegenüber 7,4 % pro Monat und 0,5 % pro Woche.

Die Statistiken zeigen, dass die Dichte der IT-Ausbildung in den einzelnen französischsprachigen Regionen unterschiedlich ist. Dafür gibt es mehrere Gründe, von denen der wichtigste zweifellos mit den akademischen Einrichtungen und ihren Regierungen zusammenhängt.

vii. Lettland

Im Jahr 2020 hat das Ministerium für Bildung und Wissenschaft der Republik Lettland die Verbesserung der digitalen Kompetenz von Pädagogen als ein vorrangiges Ziel der beruflichen Kompetenz festgelegt und zu diesem Zweck zusätzliche Mittel (0,5 Mio. EUR) bereitgestellt. Die Notwendigkeit der Sensibilisierung von Lernenden und Lehrenden für die Informationssicherheit, den Schutz der Privatsphäre und die Nutzung zuverlässiger elektronischer Dienste (Cybersicherheitsstrategie 2019-2022, Aktionsbereich "Öffentliches Bewusstsein, Bildung und Forschung").

viii. Griechenland

Obwohl der Erwerb digitaler Fertigkeiten eine Komponente ist, die im pädagogischen Instrumentarium von Berufsausbildern nicht fehlen sollte, lässt sich bei der Beobachtung des derzeitigen Bildungssystems in Griechenland eine große Lücke feststellen. Trotz der vielen Reformen der Lehrpläne gibt es Hinweise darauf, dass die Ausbilder nicht ausreichend mit IKT-Kenntnissen ausgestattet sind und es ihnen daher an pädagogischen, digital ausgerichteten Werkzeugen und Techniken fehlt, die den Lehrprozess verbessern könnten (Bildungsministerium, 2019).

Ergebnisse

Die für das Projekt CYBER.EU.VET durchgeführten Untersuchungen ergaben, dass es auf europäischer Ebene an Daten und Informationen über die Cyber-Sicherheitskompetenzen und -Herausforderungen von Pädagogen in Bildungseinrichtungen mangelt und dass es nur eine begrenzte Anzahl von Initiativen gibt, die sich auf Cyber-Sicherheitsfragen innerhalb der Berufsbildung konzentrieren. Derzeit konzentrieren sich die meisten Aktivitäten und Projekte auf die Sensibilisierung der allgemeinen Bevölkerung für Cybersicherheit und die Verbesserung der allgemeinen digitalen Kompetenzen von Lehrkräften, was durch die rasche Anpassung an den Fernarbeits-/Lernprozess beeinflusst wurde.

Das Partnerkonsortium ist vielfältig und ein deutlicher Ausdruck eines unterschiedlichen Ausmaßes an digitalen Kompetenzen in Europa. Unabhängig vom DESI-Ranking der einzelnen Länder lassen sich aus diesem Konsortialforschungsbericht jedoch aussagekräftige und valide Hinweise für den gesamten europäischen Kontext ableiten. Das Gefühl, dass

Fortbildungsbedarf besteht, ist deutlich, selbst bei denjenigen Berufsschullehrern, die bereits in IKT geschult sind. Es gibt weder eine Ablehnung des Ausbildungsbedarfs noch eine Infragestellung der Nützlichkeit der Ausbildung. Wir stellen auch fest, dass die Lehrkräfte umso mehr Fortbildungsbedarf sehen, je mehr sie sich psychosozialen, ethischen, rechtlichen, technischen oder gesundheitlichen Risiken ausgesetzt sehen. Laut einer nationalen Umfrage ist mehr als die Hälfte der Lehrer, die sich durch Cybermobbing gefährdet fühlen, der Meinung, dass eine Schulung erforderlich ist. Für sie ist die Aus- und Fortbildung eine Gelegenheit, Erfahrungen auszutauschen und Methoden der beruflichen Praxis in diesem Bereich zu analysieren. Es wird immer noch geglaubt, dass der Einsatz digitaler Werkzeuge in der Bildung eine Art zu lehren oder ein Objekt ist, das den Schülern beigebracht werden soll, und nicht ein integraler Bestandteil ihrer allgemeinen Kultur. Es sollte eine Kultur der Informationsquellen und Praktiken zu digitalen Risiken (Forschung und Überwachung) entwickelt werden. Auch die Schulung über die Herausforderungen der digitalen Technologie und insbesondere über die psychosozialen, ethischen, rechtlichen und technischen Probleme, die bei der Nutzung digitaler Werkzeuge auftreten können und die Lehrkräfte so sehr beunruhigen, dass sie auf die Nutzung verzichten, muss intensiviert werden.

Das Wissen über digitale Risiken kann sich also positiv auf die pädagogischen Praktiken auswirken, mit denen Schülern digitale Kompetenzen vermittelt werden. Eine Lehrkraft mit einer ausgeprägten digitalen Kultur wird eher geneigt sein, die digitale Technologie im Unterricht mit ihren Schülern zu nutzen und die digitale Technologie zu einem Lehr- und Lerngegenstand zu machen.

Der offensichtliche Einfluss der Risikodarstellung kann ohne eine allgemeine und plurale digitale Kultur, die eine Informationskultur im weitesten Sinne ergänzt, nicht positiv verändert werden, da sie die Dämonisierung des technischen Objekts vermeidet und die Nutzung des pädagogischen Potenzials ermöglicht.

Es geht nicht darum, in Angst zu erziehen, sondern sich zu emanzipieren (und auch als Lehrer emanzipiert zu sein), indem man die digitale Welt kritisch und aufgeklärt wahrnimmt.

Zurück zum Inhalt ☐

c) CYBER.EU.VET Toolkit

Laut dem Plan für digitale Bildung 2021-2027 haben digitale Kompetenzen und Lernherausforderungen ebenfalls hohe Priorität auf der europäischen Agenda. Die Europäische Kommission ist entschlossen, die Lücke bei den digitalen Kompetenzen zu schließen und Projekte und Strategien zu fördern, um das Niveau der digitalen Kompetenzen in Europa zu verbessern. Alle Europäer brauchen digitale Fähigkeiten, um zu studieren, zu arbeiten, zu kommunizieren, auf öffentliche Online-Dienste zuzugreifen und vertrauenswürdige Informationen zu finden. Viele Europäer verfügen jedoch nicht über angemessene digitale Fähigkeiten. Der Index für die digitale Wirtschaft und Gesellschaft (DESI) zeigt, dass vier von zehn Erwachsenen und jeder dritte Berufstätige in Europa nicht über grundlegende digitale Fähigkeiten verfügen. Auch der Anteil der Frauen in technikbezogenen Berufen und Studiengängen ist gering: Nur einer von sechs IKT-Spezialisten und einer von drei Absolventen von Naturwissenschaften, Technik, Ingenieurwesen und Mathematik (MINT) sind Frauen.

Die Europäische Kommission hat in der Europäischen Kompetenzagenda und im Aktionsplan für digitale Bildung Ziele festgelegt, die sicherstellen sollen, dass 70 % der Erwachsenen bis 2025 über digitale Grundkenntnisse verfügen. Diese Initiativen zielen darauf ab, den Anteil der 13- bis 14-Jährigen mit unzureichenden Computerkenntnissen und digitalen Fähigkeiten von 30 % (2019) auf 15 % im Jahr 2030 zu senken. Die Europäische Plattform für digitale Kompetenzen und Arbeitsplätze ist eine neue Initiative, die im Rahmen des Programms der Fazilität "Connecting Europe" gestartet wurde. Sie bietet Informationen und Ressourcen zu digitalen Kompetenzen sowie Schulungs- und Finanzierungsmöglichkeiten.[4]

i. JRC/EC Rahmen für digitale Kompetenz

- Digitaler Kompetenzrahmen für Bürger (DigComp)
- Rahmen für digitale Kompetenz für Pädagogen (DigCompEdu)
- Rahmen für digitale Kompetenz für Bildungsorganisationen (DigCompOrg) und ein Selbstreflexionsinstrument für Schulen (SELFIE)

Warum all diese Rahmenwerke?

- Aufbau von Kapazitäten für die digitale Transformation von E&T und für die Bewältigung der Herausforderungen des 21. Jahrhunderts.

[4] Digitale Kompetenzen und Arbeitsplätze | Die digitale Zukunft Europas gestalten (europa.eu)

- Bezugsrahmen, die ein umfassendes, vollständiges und gemeinsames Verständnis ermöglichen: eine gemeinsame Sprache.

Wie?

- Konzeptuelles Modell, Kompetenzstufen und (Selbst-)Bewertungsmodule.
- Kompetenz definiert als Wissen, Fähigkeiten und Einstellungen.

ii. TheDigComp 2.2

Mehr als 250 neue Beispiele für Wissen, Fähigkeiten und Einstellungen, die Bildungs- und Ausbildungsanbieter dabei unterstützen, ihre DigComp-Lehrpläne und -Kursmaterialien zu aktualisieren, um den heutigen Herausforderungen gerecht zu werden

Die Liste der DigComp-Kompetenzen und -Bereiche bleibt unverändert:

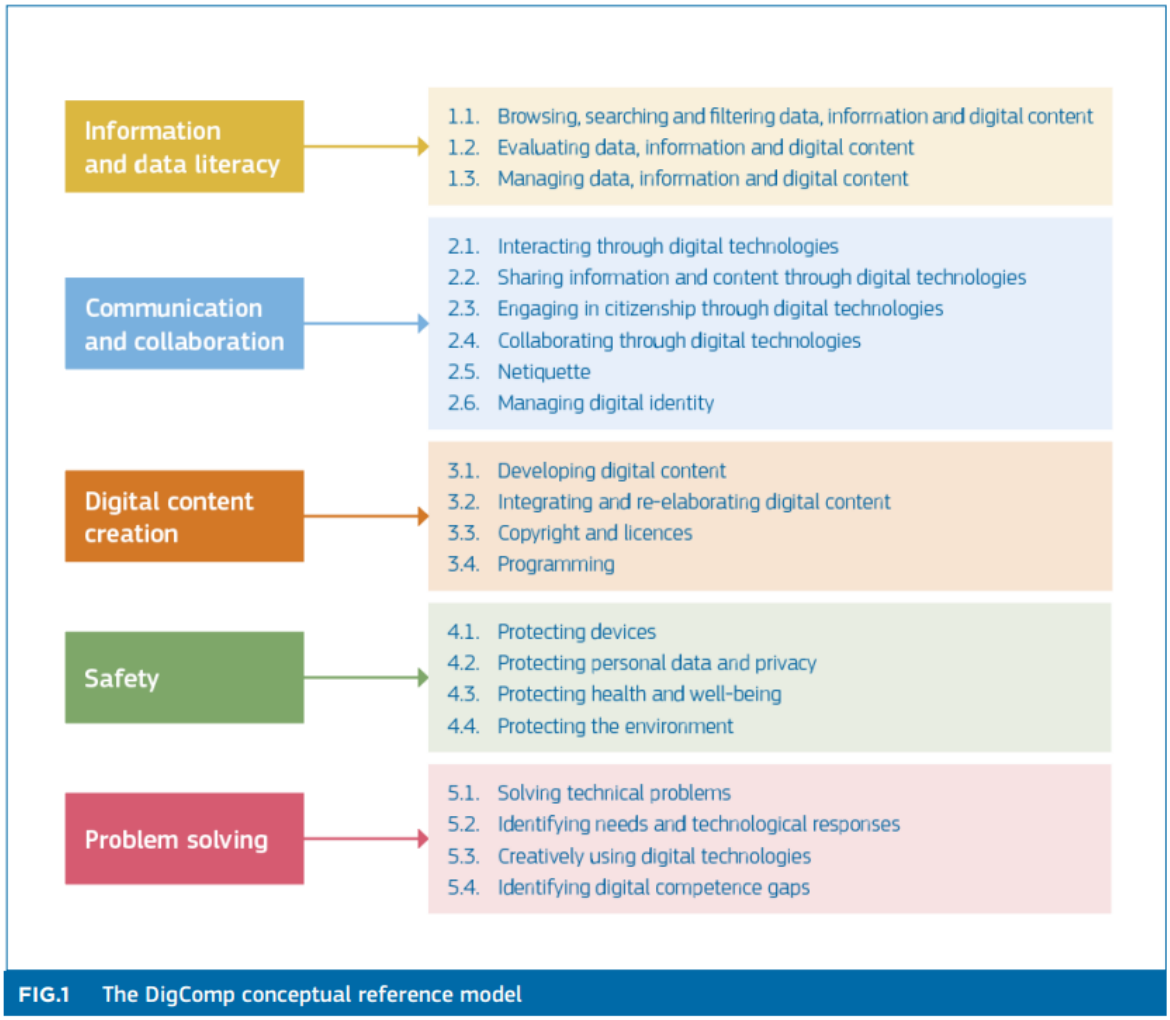


FIG.1 The DigComp conceptual reference model [5]

Eines der Hauptthemen der DigComp 2.2 Aktualisierung ist das Wohlbefinden und die Sicherheit. In jedem Bereich gibt es 10-15 Aussagen pro Kompetenz, um aktuelle Themen zu illustrieren. Sie stellen keine erschöpfende Liste dessen dar, was die Kompetenz selbst beinhaltet, und sie sind nicht auf Leistungsniveaus ausgerichtet, obwohl einige komplexer

[5] Europäische Kommission, Gemeinsame Forschungsstelle, Vuorikari, R., Kluzer, S., Punie, Y., DigComp 2.2, The Digital Competence framework for citizens : with new examples of knowledge, skills and attitudes, Amt für Veröffentlichungen der Europäischen Union, 2022, https://data.europa.eu/doi/10.2760/115376

sind als andere, aber sie sind nützlich für die Planung und Aktualisierung von Lehrplänen und die Entwicklung von DigComp-Ausbildungslehrplänen oder Kursinhalten.

SICHERHEIT: "Geräte und digitale Inhalte schützen und Risiken und Bedrohungen in digitalen Umgebungen verstehen. Kenntnisse über Sicherheitsmaßnahmen und die gebührende Berücksichtigung von Zuverlässigkeit und Privatsphäre.[6]

DIMENSION 1 • COMPETENCE AREA
4. SAFETY

DIMENSION 2 • COMPETENCE
4.1 PROTECTING DEVICES

To protect devices and digital content, and to understand risks and threats in digital environments.

To know about safety and security measures and to have a due regard to reliability and privacy.

DIMENSION 3 • PROFICIENCY LEVEL

FOUNDATION	1	At basic level and with guidance, I can:	• **identify simple** ways to protect my devices and digital content, and • differentiate simple risks and threats in digital environments. • choose simple safety and security measures, and • **identify simple** ways to have due regard to reliability and privacy.
	2	At basic level and with autonomy and appropriate guidance where needed, I can:	• **identify simple** ways to protect my devices and digital content, and • differentiate simple risks and threats in digital environments. • follow simple safety and security measures. • **identify simple** ways to have due regard to reliability and privacy.
INTERMEDIATE	3	On my own and solving straightforward problems, I can:	• **indicate well-defined and routine** ways to protect my devices and digital content, and • differentiate well-defined and routine risks and threats in digital environments, and • **select well-defined and routine** safety and security measures. • **indicate well-defined and routine** ways to have due regard to reliability and privacy
	4	Independently, according to my own needs, and solving well-defined and non-routine problems, I can:	• **organise** ways to protect my devices and digital content, and • **differentiate** risks and threats in digital environments. • **select** safety and security measures. • **explain** ways to have due regard to reliability and privacy.
ADVANCED	5	As well as guiding others, I can:	• **apply different** ways to protect devices and digital content, and • **differentiate a variety** of risks and threats in digital environments. • **apply** safety and security measures. • **employ different** ways to have due regard to reliability and privacy.
	6	At advanced level, according to my own needs and those of others, and in complex contexts, I can:	• **choose the most appropriate** protection for devices and digital content, and • **discriminate** risks and threats in digital environments. • **choose the most appropriate** safety and security measures. • **assess the most appropriate** ways to have due regard to reliability and privacy.
HIGHLY SPECIALISED	7	At highly specialised level, I can:	• **create solutions to complex problems with limited definition** that are related to protecting devices and digital content, managing risks and threats, applying safety and security measures, and reliability and privacy in digital environments. • **integrate my knowledge to contribute to professional practice and knowledge and guide others** in protecting devices.
	8	At the most advanced and specialised level, I can:	• **create solutions to solve complex problems with many interacting factors** that are related to protecting devices and digital content, managing risks and threats, applying safety and security measures, and reliability and privacy in digital environments. • **propose new** ideas and processes to the field.

7

[6] Luxemburg: Amt für Veröffentlichungen der Europäischen Union, 2018 KE-01-18-834-EN-N.pdf
[7] Ibidem

iii. Die DigCompEdu

Der Europäische Rahmen für die digitale Kompetenz von Pädagogen (DigCompEdu) ist ein wissenschaftlich fundierter Rahmen, der beschreibt, was es für Pädagogen bedeutet, digital kompetent zu sein. Er bietet einen allgemeinen Referenzrahmen zur Unterstützung der Entwicklung von bildungsspezifischen digitalen Kompetenzen in Europa. DigCompEdu richtet sich an Pädagogen auf allen Bildungsebenen, von der frühen Kindheit bis zur Hochschul- und Erwachsenenbildung, einschließlich der allgemeinen und beruflichen Bildung, der Sonderpädagogik und des nicht-formalen Lernens.

Der DigCompEdu-Rahmen spiegelt die auf internationaler Ebene unternommenen Anstrengungen zur Erfassung und Definition der spezifischen digitalen Kompetenzen wider digitale Kompetenzen von Lehrern und Ausbildern.

Ziel ist es, einen Rahmen für diejenigen zu schaffen, die im Bildungs- und Hochschulbereich arbeiten und für die Entwicklung digitaler Kompetenzmodelle zuständig sind, z. B. die politischen Entscheidungsträger in den Mitgliedstaaten, regionale/lokale Behörden, Bildungseinrichtungen, (öffentliche oder private) Institutionen, die Aus- und Weiterbildungsdienstleistungen anbieten.

Der Mehrwert des DigCompEdu-Rahmens besteht also darin, dass er einen Mehrwert bietet:

- einen soliden Hintergrund, der die Politik auf allen Ebenen leiten kann;
- eine Vorlage, die es den lokalen Akteuren ermöglicht, schnell ein konkretes Konzept zu entwickeln
- ein auf ihre Bedürfnisse zugeschnittenes Instrument zu entwickeln, ohne dafür eine konzeptionelle Grundlage entwickeln zu müssen;

- eine gemeinsame Sprache und Logik, die die Diskussion und den Austausch bewährter Verfahren erleichtern können;
- einen Bezugspunkt für die Mitgliedstaaten und andere Beteiligte zur Validierung der Vollständigkeit und
- Ansatz für ihre eigenen bestehenden und künftigen Instrumente und Rahmenwerke[8]

iv. AUSBAU DER DIGITALEN FÄHIGKEITEN VON BERUFSSCHULLEHRERN

Die Verwendung oder Entwicklung von Selbstbewertungsrahmen oder -instrumenten ist ein guter Weg, um das Ausgangsniveau der digitalen Fähigkeiten eines Lehrers zu bestimmen. Von dort aus können gezielte Weiterbildungsmaßnahmen geplant werden. Mit der zunehmenden Notwendigkeit, Technologien in der Unterrichtspraxis einzusetzen, geht auch die Notwendigkeit einher, die Pädagogik zu ändern, um sicherzustellen, dass digitale Werkzeuge nicht nur im Unterricht, sondern auch bei der Kursgestaltung und -bewertung effektiv eingesetzt werden. Der Europäische Rahmen für die digitalen Kompetenzen von Pädagogen (DigCompEdu) umreißt die wichtigsten Kompetenzbereiche, die Pädagogen benötigen, wenn sie sich intensiver mit digitalem Lernen und digitalem Unterricht beschäftigen. Die Schlüsselkompetenzen sind in der folgenden Abbildung dargestellt (Redecker 2017)

[8] Redecker, C. European Framework for the Digital Competence of Educators: DigCompEdu. Punie, Y. (ed). EUR 28775 DE. Amt für Veröffentlichungen der Europäischen Union, Luxemburg, 2017, ISBN 978-92-79-73494-6, doi:10.2760/159770, JRC107466

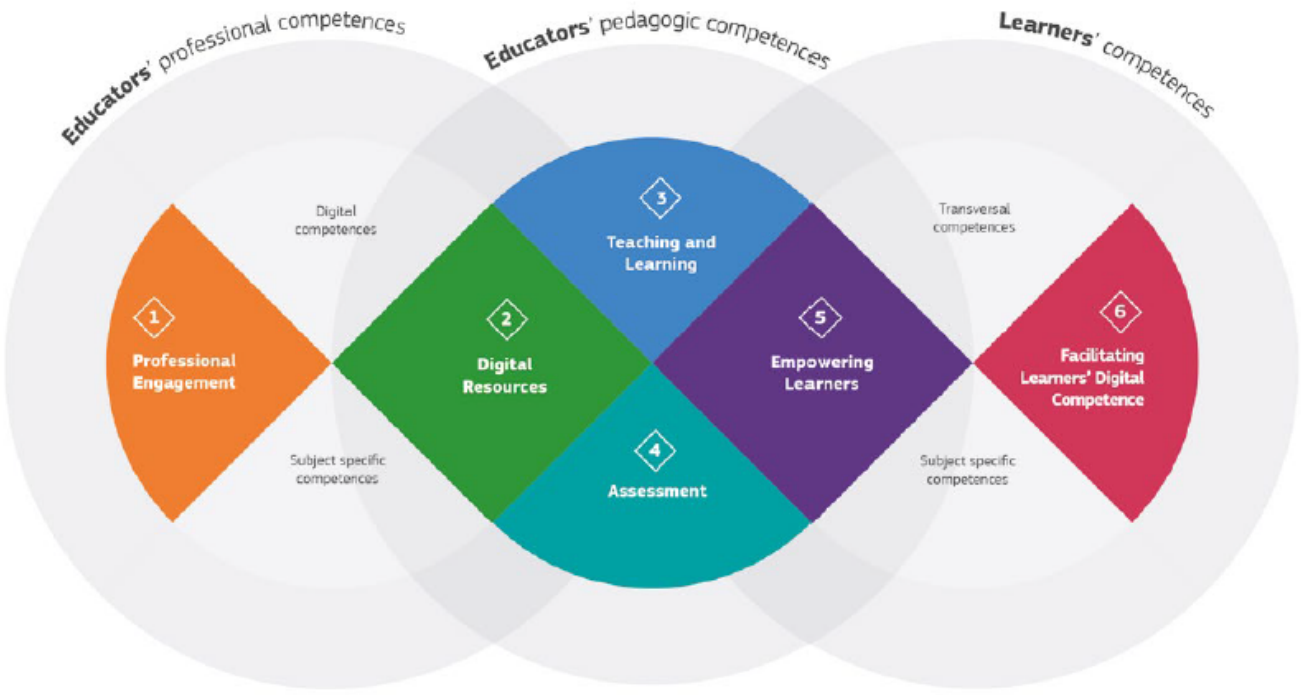


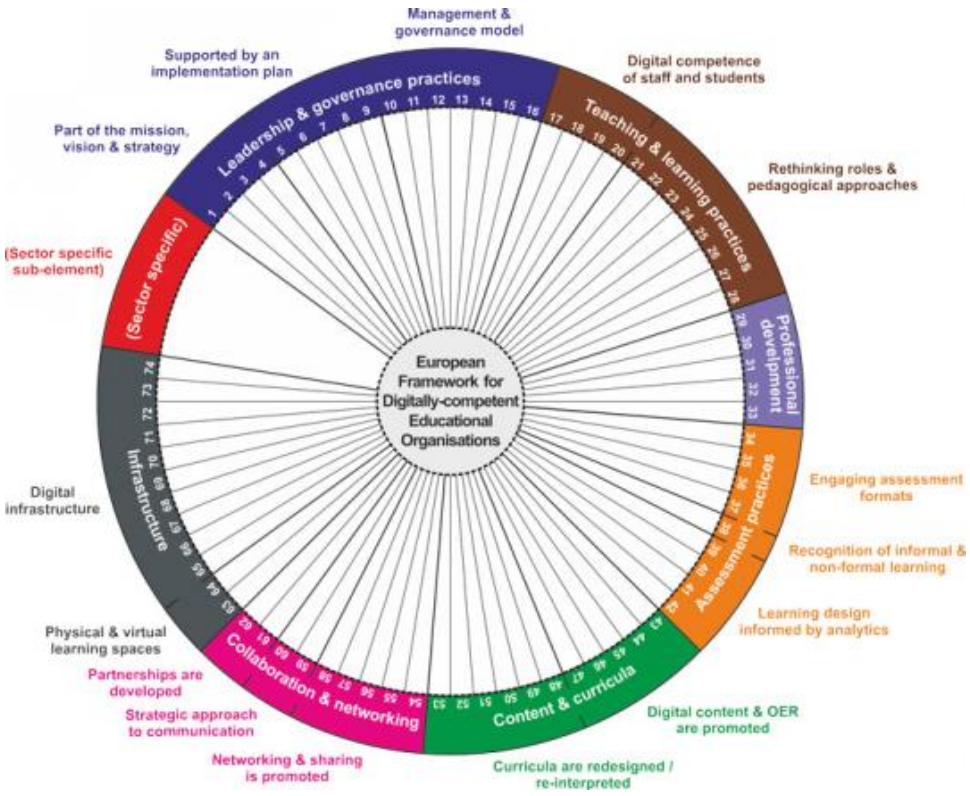
FIGURE 2: DIGCOMPEDU AREAS AND SCOPE

v. Das DigCompOrg-Rahmenwerk

In einer Reihe von europäischen Ländern werden verschiedene Rahmen und Selbstbewertungsinstrumente verwendet, aber bisher wurde noch kein Versuch unternommen, einen gesamteuropäischen Ansatz für die digitale Kapazität von Organisationen zu entwickeln. Ein europäischer Referenzrahmen, der einen systemischen Ansatz verfolgt, kann durch die Förderung von Transparenz, Vergleichbarkeit und Peer-Learning einen Mehrwert schaffen. Der **DigCompOrg-Rahmen** kann von Bildungsorganisationen (d. h. Grund-, Sekundar- und berufsbildenden Schulen sowie Hochschuleinrichtungen) genutzt werden, um einen Prozess der Selbstreflexion über ihre

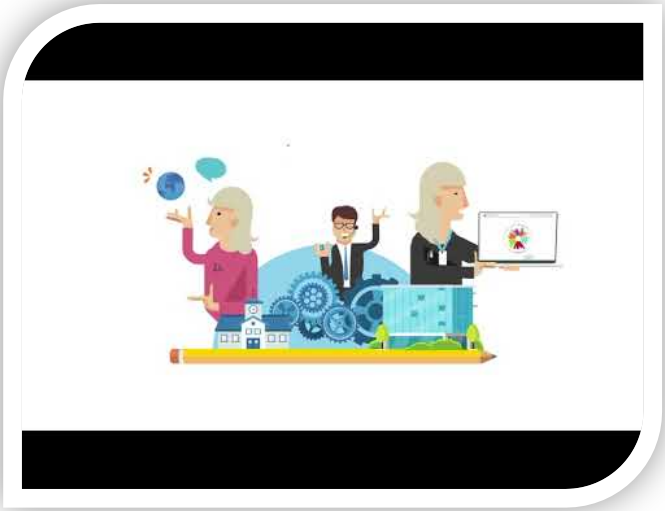
Fortschritte bei der umfassenden Integration und dem effektiven Einsatz digitaler Lerntechnologien anzuleiten.

Darüber hinaus kann es die Transparenz und Vergleichbarkeit zwischen verwandten Initiativen in ganz Europa erleichtern und auch eine Rolle dabei spielen, die Fragmentierung und ungleiche Entwicklung in den Mitgliedstaaten zu bekämpfen. Der DigCompOrg-Rahmen kann auch als strategisches Planungsinstrument für politische Entscheidungsträger genutzt werden, um umfassende Strategien für die effektive Einführung digitaler Lerntechnologien durch Bildungsorganisationen auf regionaler, nationaler und europäischer Ebene zu fördern. Er kann auch als Mittel zur Sensibilisierung für den systemischen Ansatz genutzt werden, der für eine effektive Nutzung digitaler Lerntechnologien erforderlich ist.



Die Hauptziele von DigCompOrg sind:

- Förderung der Selbstreflexion und Selbstbewertung innerhalb von Bildungseinrichtungen, die sich schrittweise mit digitalem Lernen und Pädagogik beschäftigen;
- die politischen Entscheidungsträger (auf lokaler, regionaler, nationaler und internationaler Ebene) in die Lage zu versetzen, ;
- Programme, Projekte und politische Maßnahmen zur Integration digitaler Lerntechnologien in Systeme der allgemeinen und beruflichen Bildung zu konzipieren, umzusetzen und zu bewerten.



vi. SELFIE

SELFIE für berufsbezogenes Lernen (WBL) ist ein kostenloses Online-Tool, das berufsbildende Schulen und Unternehmen dabei unterstützt, das Beste aus digitalen Technologien für das Lehren, Lernen und die Ausbildung zu machen. SELFIE WBL unterstützt Schulen und Unternehmen dabei, fit für das digitale Zeitalter zu werden. Auf diese Weise unterstützt es den digitalen Wandel, eine der wichtigsten politischen Prioritäten der Europäischen Kommission. Diese Anpassung von SELFIE an die spezifischen Anforderungen von WBL ist ein notwendiger Schritt**, um berufsbildende Schulen zu unterstützen**. [9]

Insgesamt waren rund **35.000 Teilnehmer** aus etwa **150 berufsbildenden Schulen** und **250 Unternehmen** in Frankreich, Deutschland, Ungarn, Polen, Rumänien, Georgien, Montenegro und der Türkei an der Pilotierung beteiligt. Die Ergebnisse dieser Pilotprojekte stehen zum Download zur Verfügung [LINK zu den Ressourcen]. [10]

[9] SELFIE für arbeitsbasiertes Lernen | Europäischer Bildungsraum (europa.eu)
[10] SELFIE Ressourcen | Europäischer Bildungsraum (europa.eu)

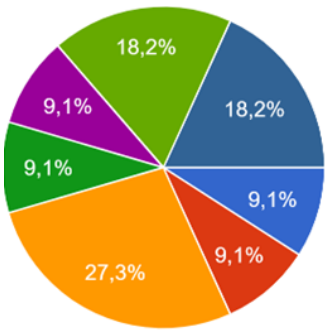
Das Europäische Forum für technische und berufliche Bildung (EfVET) und die Europäische Stiftung für Berufsbildung (ETF) leisteten während der gesamten Zeit unschätzbare Unterstützung.

Zurück zum Inhalt ☐

d)CYBER.EU.VET-Leitlinien

Das Projekt CYBER.EU.VET sollte dazu beitragen, die Fähigkeit der europäischen Berufsbildung zu stärken, Cybersecurity-Bedrohungen (z.B. Phishing-Attacken, Botnets, Finanz- und Bankbetrug, Datenbetrug) zu erkennen und zu bewältigen, und zwar in einem historischen Kontext, in dem Online-Schulungen mehr und mehr genutzt werden.
Zu diesem Zweck wurden die Fähigkeiten und Kompetenzen von Lehrkräften in der beruflichen Bildung in Bezug auf den Umgang mit Cybersicherheitsbedrohungen verbessert, da sie eine zentrale Rolle bei der Weitergabe von bewährten Praktiken und Fähigkeiten an ihre Schüler spielen. Außerdem wurden Lehrkräfte in der beruflichen Bildung, Schüler und ihre Familien dafür sensibilisiert, wie wichtig es ist, solche täglichen Risiken zu erkennen, die sowohl wirtschaftliche als auch soziale Auswirkungen auf alle europäischen Bürger haben können. Das Projekt stützte sich auf eine gemeinsame lokale, nationale und transnationale Verbreitung von Kapazitäten und Fachwissen sowie auf einen guten Zugang zu digitalen Informationen und deren Nutzbarkeit.

8 Gamejam-Sitzungen mit 54 Studenten und 15 landesspezifische Schulungen für Ausbilder wurden organisiert, um die Forschungsergebnisse, die gemeinsam genutzten und die neu geschaffenen digitalen Tools zu diskutieren und Erfahrungen und Überlegungen auszutauschen, um eine Art "thematische kollektive Erzählung" zu entwickeln, die den Übergang von der Erkundung und Analyse zur Verwaltung und digitalen Problemlösung vorbereitet.



Diese Veranstaltungen ermöglichten es den Jugendlichen, zusammenzuarbeiten und zu zeigen, dass auch Institutionen, die als

bürgerfern gelten (z. B. die EU-Kommission), interessante Möglichkeiten für die junge Bevölkerung bieten.

Eine **Trainingseinheit** wird in diesem Leitfaden als eine einzelne Trainingseinheit definiert, die im Laufe eines Tages oder eines Teils eines Tages stattfindet. Sie kann 30 Minuten, eine Stunde oder sogar einen ganzen Tag dauern. Eine Schulungssitzung kann im Laufe des Tages Pausen einschließen und ein oder mehrere Themen behandeln. Eine Schulung kann in einem Klassenzimmer, in einer kleinen Gruppe mit einer einzelnen Familie oder sogar unter vier Augen stattfinden. Ein Schulungsprogramm im Sinne dieses Leitfadens ist eine Sammlung von Schulungssitzungen, die einen Schulungszyklus abschließen. Eine Einrichtung könnte beispielsweise ein 8-wöchiges Schulungsprogramm einmal pro Woche anbieten. Das Schulungsprogramm könnte dann für eine neue Gruppe von Personen wieder aufgenommen werden. (*Workshops und Kurse, 2021*)

I. Die Basis eines Workshops: Wissen, Fertigkeiten und Haltungen

Dieser Leitfaden folgt einem Rahmen für die Sensibilisierung der Lernenden für digitale Bedrohungen, der auf Wissen, Fähigkeiten und Kompetenzen basiert. In ähnlicher Weise verbessern Programmverantwortliche und Lehrkräfte/Trainer ihre Kenntnisse, Fähigkeiten und Einstellungen, um effektiver zu sein. Dieser Abschnitt befasst sich mit dem Wissen, den Fähigkeiten und der Einstellung von Lehrern und Ausbildern.

Wissen, Fähigkeiten und Einstellungen sind die Grundlagen einer effektiven Schulung. Effektive Trainer verfügen über Kenntnisse, Fähigkeiten und Einstellungen in Bezug auf Schulungen und die Themen, die sie vermitteln, und die Schulungsprogramme und -sitzungen, die sie durchführen, sollten Kenntnisse, Fähigkeiten und Einstellungen für Teilnehmer enthalten, die sich auf das Thema und den Inhalt konzentrieren.

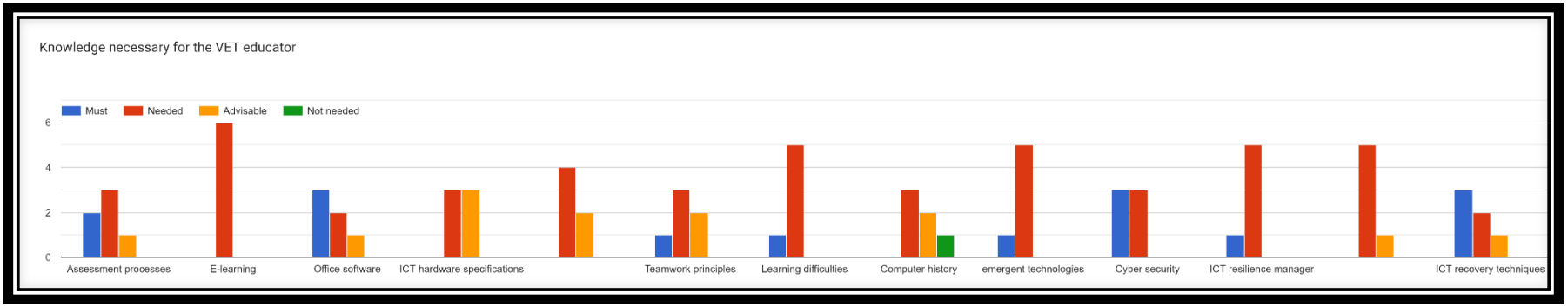
Frage an mich selbst: An wen können Sie sich wenden, wenn Sie als Berufsbildungsanfänger Fragen zu Programmstandards und -inhalten haben?

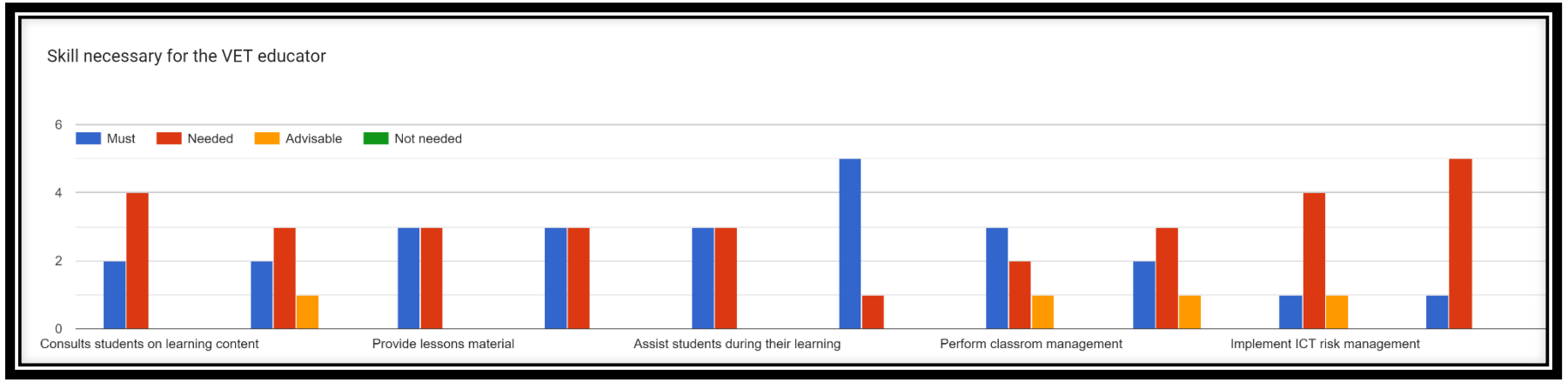
Die Ausbilder müssen über ein umfassendes Verständnis der Kerninhalte verfügen, um auf auftretende Fragen reagieren zu können. Wenn ein Ausbilder die Antwort auf eine Frage nicht

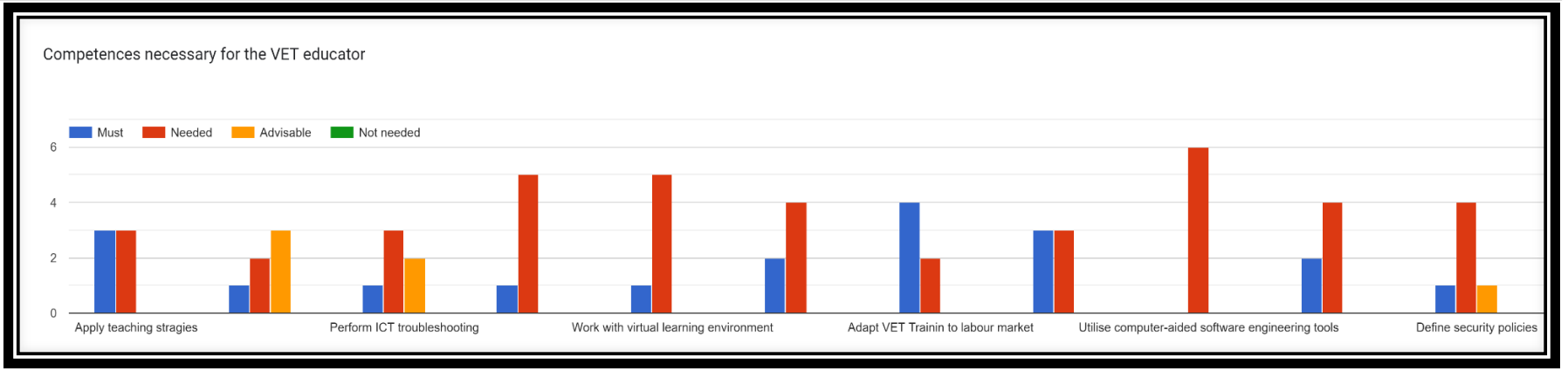
weiß, ist es wichtig, dass der Ausbilder mitteilt, dass er die Antwort nicht kennt, aber der Sache nachgehen und Bericht erstatten wird. Praktiker sollten keine falschen Informationen geben oder Antworten erfinden, um das Wohlbefinden und das Verständnis der Teilnehmer zu gewährleisten. Es liegt in der Verantwortung eines Trainers, Nachforschungen anzustellen, Antworten zu finden und mit den Teilnehmern nachzufragen, um sicherzustellen, dass sie korrekte Informationen erhalten.

Möchten Sie mehr darüber erfahren, was ein Lehrer im Umgang mit dem Thema tun kann?

Im Folgenden sind Beispiele für geeignete Kenntnisse, Fähigkeiten und Einstellungen aufgeführt, über die ein effektiver Ausbilder nach Ansicht der Partner des Konsortiums verfügen sollte.







Co-funded by the
Erasmus+ Programme
of the European Union

Aktivität: Was sind Beispiele für Ihr Wissen, Ihre Fähigkeiten und Ihre Einstellungen als Lehrkraft/Ausbilder/in? Füllen Sie die Lücken in der Tabelle aus. Ein Beispiel ist gegeben.

Beispiele für Wissen	Beispiele für Fähigkeiten	Beispiele für Haltungen
Ich kenne mich mit Cybersicherheit und aufkommenden Technologien aus.	Ich kann digitale Bildungsmaterialien entwickeln und den Unterricht an die Zielgruppe anpassen.	Es ist mir ein Anliegen, die Sitzungen für unsere Teilnehmer so effektiv wie möglich zu gestalten, und ich setze mich dafür ein.

- **Wissen**: Ergebnis der Aneignung von Informationen durch Lernen. Wissen ist die Gesamtheit der Fakten, Grundsätze, Theorien und Praktiken in Bezug auf ein Studien- oder Arbeitsgebiet.
- **Geschicklichkeit**: Fähigkeit, Wissen und Know-how anzuwenden, um Aufgaben zu erledigen und Probleme zu lösen.
- **Kompetenz**: **Die** Fähigkeit, die Lernergebnisse in einem bestimmten Kontext (Ausbildung, Arbeit, persönliche oder berufliche Entwicklung) angemessen anzuwenden. [11]

[11] Der Europäische Qualifikationsrahmen für lebenslanges Lernen (EQR)

Co-funded by the Erasmus+ Programme of the European Union

Zurück zum Inhalt ↑

II. Die Website CYBER.EU.VET

Das Projektkonsortium hat bereits in der ersten Phase des Projekts eine spezielle Website erstellt, die mit Open-Source-Technologien (Wordpress) und einem modularen Ansatz entwickelt wurde, der es neuen Partnern aus verschiedenen Ländern ermöglicht, ihre eigenen Inhalte hinzuzufügen und zu verwalten (sobald sie die von den Projektpartnern festgelegten Bedingungen akzeptieren). Digitale Plattformen wie CYBER.EU.VET können auf zwei Arten geöffnet werden, um Innovation und Wertschöpfung zu fördern (Boudreau 2010).

Natürlich können digitale Plattformen, und in diesem speziellen Fall die als Open Educational Resource konzipierte Plattform, für Folgeaktivitäten weiter genutzt werden. Dieses neue System ermöglicht es, die traditionelle physische Welt mit einer digitalen Schnittstelle zu verbinden, die in der Lage ist, die Nachfrage und das Angebot eines Werkzeugs oder einer Dienstleistung in einem einzigen virtuellen Raum zu verbinden und zu organisieren.

Karhu, Gustafsson, and Lyytinen: *Exploiting and Defending Open Digital Platforms*
Information Systems Research, 2018, vol. 29, no. 2, pp. 479–497, © 2018 The Author(s)

Table 1. Two Forms of Platform Openness and Related Resources

Platform openness	Boundary resources	Shared resources	Actor who shares	Type of sharing	Platform owner's rationale
Access openness	API, app store	Complement, e.g., apps	Complementor	Shared for distribution	Generate network effects, and extract value from complementarities
Resource openness	Open-source license	Platform core, e.g., AOSP	Platform owner	Shared IPR	Strategic forfeiture of IPR while recovering costs from somewhere else

Diese Plattformen schaffen Netzwerke, die Menschen und Dienste über die Zeit hinweg miteinander verbinden.

Die Integrität des Netzes hängt nicht nur von den Faktoren der Informationsinfrastruktur, ihrer Sicherheit und dem Datenfluss innerhalb des

Netzes ab, sondern auch von den sozialen und umweltbedingten Veränderungen, die sich auf die menschlichen Komponenten auswirken.

Aus diesem Grund wurde eine Multiplikatorenkampagne organisiert, um die entwickelten technologischen Werkzeuge und das Handbuch CYBER.EUY.VET zu verbreiten und bekannt zu machen.

Ziel dieser Kampagne war es auch, Lehrkräfte in der beruflichen Bildung, Schüler und deren Angehörige dafür zu sensibilisieren, wie wichtig es ist, solche täglichen Risiken zu erkennen, die sowohl wirtschaftliche als auch soziale Auswirkungen auf alle europäischen Bürger haben können.

IKT-Systeme, die den sich abzeichnenden "Netzwerkeffekt" nutzen, indem sie offene soziale Online-Medien, verteilte Wissensbildung und Daten aus dem realen Umfeld kombinieren, um **ein Bewusstsein für Probleme und mögliche Lösungen zu schaffen, die kollektive Anstrengungen erfordern und neue Formen der sozialen Innovation ermöglichen.**

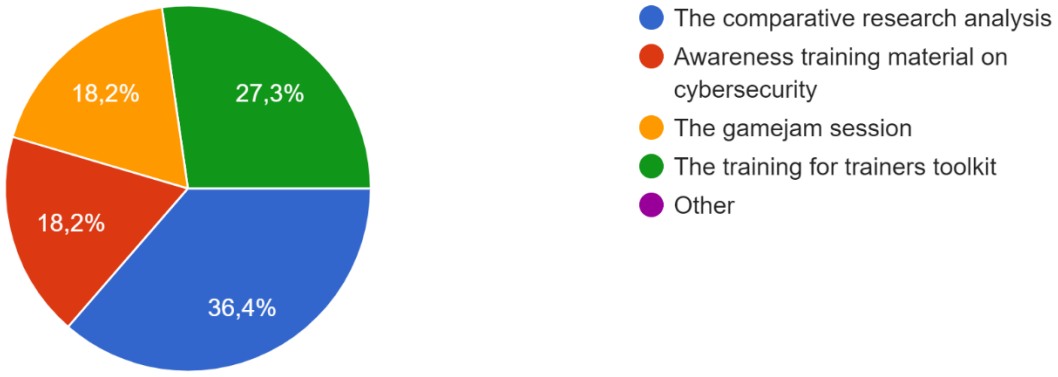
III. "Ein praktischer Einblick"

Partner und Praktiker, die am CYBER.EU.VET-Projekt beteiligt waren, gaben an, dass sie von ihren Forschungszielen durch ein besseres Verständnis der Wahrnehmung von Studenten der Cybersicherheit im lokalen und europäischen Kontext profitieren konnten. Der Austausch zwischen so unterschiedlichen Interessenvertretern war eine Gelegenheit, unterschiedliche Perspektiven und Ansätze zu gemeinsamen Themen zu gewinnen und zu lernen, wie man sie in eine gemeinsame Sprache übersetzt. Mit den Worten unseres Partners*: "Es war sehr nützlich, mehr über den aktuellen Stand der Technik im Bereich der Cybersicherheit und die wichtigsten Cyberbedrohungen in den Partnerländern zu erfahren. Es ist auch interessant, die Trends bei den Cyberangriffen zu erkennen und zu verfolgen, die in allen Ländern sehr ähnlich zu sein scheinen"*. 81,8 % der Partner gaben an, dass sie beabsichtigen, das im Rahmen des Projekts ausgetauschte oder erstellte Material in Zukunft zu verwenden, 36,4 % auf lokaler, 36,4 % auf nationaler und 27,3 % auf internationaler Ebene, in Schulungen und Workshops, Foren und natürlich in den sozialen Medien.

Der Kontext der am Projekt beteiligten Länder ist sehr unterschiedlich, obwohl sie als europäische Länder gewisse Gemeinsamkeiten haben. Die Cybersicherheit ist sehr wandelbar,

da sich die Bedrohungen im Laufe der Zeit ändern. Daher ist es interessant, dass die erzielten Ergebnisse sowohl von den Ausbildern als auch von den Forschern aktualisiert werden, damit sie zu dem Zeitpunkt, zu dem sie verwendet werden, gültig sind.

Aufschlussreich ist die Grafik, die zeigt, welche gemeinsamen Instrumente für die Betreiber der verschiedenen Dienste der 8 Konsortialpartner am nützlichsten waren:



IV. Eine letzte Anmerkung

Das CYBER.EU.VET Handbuch wurde entwickelt, um Berufsausbilder und digitale Praktiker bei der Verwendung von Werkzeugen für die Cybersicherheit zu unterstützen und Anweisungen zur Nutzung des im Anhang aufgeführten CYBER.EU.VET Materials zu geben. Es enthält Vorschläge, wie die Ausbildung gestaltet werden kann, sowie praktische Empfehlungen, die es den Praktikern ermöglichen, den Schülern das Wissen und die Werkzeuge zu vermitteln, die sie benötigen, um Bedrohungen der Cybersicherheit zu erkennen. Dieses E-Book wurde zum Nutzen von Berufsbildungslehrern, Berufsbildungsschülern, Familien von Schülern und Berufsbildungseinrichtungen auf internationaler oder lokaler Ebene entwickelt. Praktiker (oder Sachbearbeiter/Manager), die Schulungen und Orientierungsmaßnahmen durchführen, Aufsichtspersonen oder Schulungskoordinatoren und diejenigen, die Orientierungsmaßnahmen durchführen, wie z. B. Freiwillige, Praktikanten, anderes Unterstützungspersonal für die Neuansiedlung, andere Dienstleister und Gemeindemitglieder, können alle davon profitieren. Eine stärkere Sensibilisierung für die Risiken, die durch

Datenbetrug, Malware und andere Online-Sicherheitsbedrohungen verursacht werden, auf allen Ebenen, von der Leitung der Berufsbildungseinrichtung bis hin zu den Familien der Auszubildenden, ist ein grundlegender Schritt, um die EU-Bürger in einer Zeit, die bereits durch eine epochale Krise gekennzeichnet ist, vor Schäden durch Cyber-Sicherheitsbedrohungen zu schützen.

Dieses E-Book enthält eine Reihe von Vorschlägen, von denen wir hoffen, dass sie Lehrkräfte und Praktiker in der beruflichen Bildung dazu anregen, die Ziele ihrer Ausbildung zu überdenken und zu überlegen, wie sie die Qualität der Ausbildung durch die Entwicklung innovativer Methoden des e-Learning verbessern können.

e) Anhang

I. Glossar
II. Der CYBER.EU.VET Userguide - Orientierungshilfe für zukünftige Implementierungen

I. GLOSSAR

DATEN
eine Abfolge von einem oder mehreren Symbolen, die durch einen oder mehrere spezifische Interpretationsakte eine Bedeutung erhalten (Daten haben keine eigene Bedeutung). Daten können analysiert oder verwendet werden, um Erkenntnisse zu gewinnen oder Entscheidungen zu treffen. Digitale Daten werden im Gegensatz zu ihrer analogen Darstellung mit dem binären Zahlensystem von Einsen (1) und Nullen (0) dargestellt. [12]

DIGITALE KOMMUNIKATION
Kommunikation mit digitaler Technologie. Es gibt verschiedene Arten der Kommunikation, z. B. synchrone Kommunikation (Kommunikation in Echtzeit, z. B. über Skype, Videochat oder Bluetooth) und asynchrone Kommunikation (nicht gleichzeitige Kommunikation, z. B. E-Mail, SMS), z. B. mit Eins-zu-Eins-, Eins-zu-Vielen- oder Viele-zu-Vielen-Modi.[13]

DIGITALE KOMPETENZ
Digitale Kompetenz kann im weitesten Sinne als selbstbewusste, kritische und kreative Nutzung von IKT definiert werden, um Ziele in Bezug auf Arbeit, Beschäftigungsfähigkeit, Lernen, Freizeit, Integration und/oder Teilhabe an der Gesellschaft zu erreichen.[14]

DIGITALER INHALT
Jede Art von Inhalt, der in Form digitaler Daten vorliegt, die in einem maschinenlesbaren Format kodiert sind und mit Hilfe digitaler Technologien erstellt, angezeigt, verbreitet, geändert und gespeichert werden können. Beispiele für digitale Inhalte sind: Webseiten und Websites, soziale Medien, Daten und Datenbanken, digitale Audiodateien wie mp3s und E-Books, digitale Bilder, digitale Videos, Videospiele, Computerprogramme und Software. Im Rahmen von DigCompEdu werden digitale Inhalte in digitale Ressourcen und Daten unterteilt.[15]

DIGITALE UMGEBUNG
ein Kontext oder ein "Ort", der durch Technologie und digitale Geräte ermöglicht wird, die häufig über das Internet oder andere digitale Mittel, z. B. das Mobilfunknetz, übertragen werden. Die Aufzeichnungen und Beweise der Interaktion einer Person mit einer digitalen Umgebung stellen ihren digitalen Fußabdruck dar. In DigComp wird der Begriff digitale Umgebung als Hintergrund für digitale Aktionen verwendet, ohne eine bestimmte Technologie oder ein bestimmtes Werkzeug zu nennen.

DIGITALE DIENSTLEISTUNG
ermöglicht es einem Nutzer (Bürger, Verbraucher), Daten in digitaler Form zu erstellen, zu verarbeiten, zu speichern oder darauf zuzugreifen und Daten in digitaler Form, die von ihm oder anderen Nutzern dieses Dienstes hochgeladen oder erstellt wurden, zu teilen oder damit zu interagieren (Richtlinie (EU) 2019/770).

DIGITALE TECHNOLOGIE

12 Geändert von: de.wikipedia.org/wiki/Data_(computing)
13 Quelle: *DigComp Framework* https://ec.europa.eu/jrc/digcomp
14 *Ibidem*
15 Redecker, C. European Framework for the Digital Competence of Educators: DigCompEdu. Punie, Y. (ed). EUR 28775 DE. Amt für Veröffentlichungen der Europäischen Union, Luxemburg, 2017, ISBN 978-92-79-73494-6, doi:10.2760/159770, JRC107466

Jedes Produkt, mit dem Informationen elektronisch in digitaler Form erstellt, angezeigt, verteilt, geändert, gespeichert, abgerufen, übertragen und empfangen werden können. Zum Beispiel PCs und andere Geräte (z. B. Desktop, Laptop, Netbook, Tablet-Computer, Smartphones, PDA mit Mobilfunkfunktion, Spielkonsolen, Mediaplayer, E-Book-Reader), digitales Fernsehen, Roboter.[16]

DIGITALE WERKZEUGE

Digitale Technologien, die zu einem bestimmten Zweck oder zur Ausführung einer bestimmten Funktion eingesetzt werden, z. B. zur Informationsverarbeitung, Kommunikation, Erstellung von Inhalten, Sicherheit oder Problemlösung.[17]

BILDUNGSINHALT

(Digitale) Inhalte, die auf die eine oder andere Weise für den Bildungskontext relevant sind. Dieser Begriff ist weiter gefasst als
"Bildungsressource" insofern, als sie auch Inhalte am Rande des Unterrichtsprozesses umfasst, z. B. die Kommunikation mit Schülern, Eltern, Kollegen, Verwaltungsinhalte usw.[18]

BILDUNGSRESSOURCEN

Ressourcen (digital oder nicht), die für Bildungszwecke konzipiert und bestimmt sind.[19]

MEDIENKOMPETENZ

bezieht sich auf Fähigkeiten, Wissen und Verständnis, die es den Bürgern ermöglichen, Medien effektiv und sicher zu nutzen. Damit die Bürgerinnen und Bürger Zugang zu Informationen haben und Medieninhalte verantwortungsvoll und sicher nutzen, kritisch bewerten und erstellen können, müssen sie über fortgeschrittene Medienkompetenz verfügen. Medienkompetenz sollte sich nicht auf das Erlernen von Werkzeugen und Technologien beschränken, sondern darauf abzielen, die Bürger mit der Fähigkeit zum kritischen Denken auszustatten, die erforderlich ist, um ein Urteilsvermögen zu entwickeln, komplexe Realitäten zu analysieren und den Unterschied zwischen Meinung und Tatsache zu erkennen. [20]

OFFENE BILDUNGSRESSOURCEN

Lehr-, Lern- und Forschungsmaterialien in jedem Medium, digital oder anderweitig, die gemeinfrei sind oder unter einer offenen Lizenz veröffentlicht wurden, die den kostenlosen Zugang, die Nutzung, die Anpassung und die Weiterverbreitung durch andere ohne oder mit begrenzten Einschränkungen erlaubt. [21]

SELBSTEINSCHÄTZUNG

Selbstbeurteilung bedeutet die Fähigkeit, die eigene Leistung realistisch einzuschätzen. Befürworter der Selbstbewertung weisen darauf hin, dass sie viele Vorteile hat, z. B.: Sie bietet zeitnahes und effektives Feedback und ermöglicht es den Studierenden, ihr eigenes Lernen schnell zu bewerten; sie ermöglicht es den Lehrkräften, das Lernen zu verstehen und schnelles Feedback zu geben; sie fördert die akademische Integrität durch die Selbstdarstellung des Lernfortschritts durch die Studierenden; sie fördert die Fähigkeiten der reflektierenden Praxis und der Selbstüberwachung; sie entwickelt selbstgesteuertes Lernen; sie steigert die Motivation der Studierenden; sie verbessert die Zufriedenheit mit der Teilnahme an einer kollaborativen Lernumgebung; sie hilft den Studierenden, eine Reihe von persönlichen, übertragbaren Fähigkeiten zu entwickeln, um die Erwartungen künftiger Arbeitgeber zu erfüllen.[22]

---

[16] Geändert von Quelle: http://www.tutor2u.net/business/ict/intro_what_is_ict.htm
[17] *Ibidem*
[18] *Ibidem*
[19] *Ibidem*
[20] Quelle: Richtlinie über audiovisuelle Mediendienste der EU (2018)
[21] Quelle: UNESCO-Definition http://www.unesco.org/new/en/communication-and-information/access-to-knowledge/open-educational-resources/what-are-open-educational-resources-oers/
[22] Quelle: *Cornell University Centre for Teaching Excellence* http://www.cte.cornell.edu/

SOZIALE EINGLIEDERUNG Der Prozess der Verbesserung der Bedingungen für Einzelpersonen und Gruppen, um an der Gesellschaft teilzuhaben (von der Weltbank). Soziale Eingliederung zielt darauf ab, arme und marginalisierte Menschen in die Lage zu versetzen, die aufkeimenden globalen Chancen zu nutzen. Sie stellt sicher, dass die Menschen ein Mitspracherecht bei Entscheidungen haben, die ihr Leben betreffen, und dass sie gleichen Zugang zu Märkten, Dienstleistungen und politischen, sozialen und physischen Räumen haben.[23]

STRUKTURIERTES UMFELD
bei denen sich die Daten in einem festen Feld innerhalb eines Datensatzes oder einer Datei befinden, z. B. in relationalen Datenbanken und Tabellenkalkulationen. Technologische Antwort/Lösung bezieht sich auf den Versuch, Technologie (und/oder Technik) zur Lösung eines Problems einzusetzen.

[23] Quelle: *DigComp Framework* https://ec.europa.eu/jrc/digcomp

Referenzen

Nationale Agentur für die Sicherheit von Informationssystemen (ssi.gouv.fr)

Ala-Mutka, K. (2011). Mapping Digital Competence: Towards a Conceptual Understanding. (JRC Technical Notes No. JRC67075). IPTS.

Baron G.-L. und Baudé J. (1992), L'intégration de l'informatique dans l'enseignement et la formation des enseignants, Tours: EPI - INRP.

BIBB (2016), "Wirtschaft 4.0 braucht Bildung 4.0", Stärkung der Medienkompetenz von Ausbildungspersonal und Auszubildenden.

https://doi.org/10.13140/RG.2.2.18046.00322
Brodnik, A., Csizmadia, A., Futschek, G., Kralj, L., Lonati, V., Micheuz, P., & Monga, M. (2021). Programmieren für alle: Understanding the Nature of Programs. ArXiv:2111.04887 [Cs].

http://arxiv.org/abs/2111.04887
Buisán García,M.; Valdés, F. (2017), La industria Conectada 4.0., Revista de economía, No 898.

Bihouix P, Mauvilly, K (2016), Le Désastre de l'école numérique, Le Seuil.

Carretero, S., Vuorikari, R., & Punie, Y. (2017). DigComp 2.1: Der digitale Kompetenzrahmen für Bürgerinnen und Bürger mit acht Kompetenzstufen und Anwendungsbeispielen. Publica-tions Office of the European Union. https://data.europa.eu/doi/10.2760/38842

Cyber Ireland, (2021), Cyber Security Skills Report 2021: National Survey: https://www.cyberireland.ie/wp-content/uploads/2021/02/Cyber-Ireland-Skills-Report2021.pdf (Zugriff am 3. Juli 2021).

EFVET (2021), Digitales Gleichgewicht: Balance zwischen digitalen Kompetenzen und Wohlbefinden.

Europäische Kommission. (2022). Übersetzungen von DigComp 2.0 in der Europäischen Klassifikation der Fertigkeiten, Kompetenzen und Berufe (ESCO). Amt für Veröffentlichungen der Europäischen Union. DOI:10.2767/316971

Europäische Union. (2018). Empfehlung des Rates vom 22. Mai 2018 zu Schlüsselkompetenzen für lebenslanges Lernen (ST/9009/2018/INIT).

https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=uriserv:O-J.C_.2018.189.01.0001.01.ENG
Ferrari, A. (2012). Digitale Kompetenz in der Praxis: An anal-ysis of frameworks. Amt für Veröffentlichungen der Europäischen Union.

https://data.europa.eu/doi/10.2791/82116
Ferrari, A. (2013). DIGCOMP: Ein Rahmen für die Entwicklung und das Verständnis digitaler Kompetenz in Europa. Publications Office. doi:10.2788/52966

Ferrari, A., Brecko, B., & Punie, Y. (2014). DIGCOMP: a Framework for Developing and Understanding DigitalCompetence in Europe. ELearning Papers, 38, 1-14.

Ferrari, A., Punie, Y., & Redecker, C. (2012). Das Verständnis digitaler Kompetenz im 21. Jahrhundert: An analysis of current frameworks. In EC-TEL 2012: 21st Century Learning for 21st Century Skills (S. 79-92).

Regierung von Lettland, (2020), Leitlinien für die digitale Transformation 2021-2027.

Huismann, A. (2020), Berufliche Aus- und Weiterbildung für die Zukunft der Arbeit: Deutschland, Cedefop ReferNet thematic perspectives series.

Information Technology Security Incident Response Institution, (2021), CERT.LV Jahresbericht 2020.

Izglītības un zinātnes ministrija (2017), Informatīvais ziņojums "Priekšlikumi konceptuāli jaunas kompetencēs balstītas izglītības prasībām atbilstošas skolotāju izglītības nodrošināšanai Latvijā.

Izglītības un zinātnes ministrija (2020), Pedagogiem nodrošināta iespēja bez maksas pilnveidot digitālās prasmes.

Janssen, J., & Stoyanov, S. (2012). Online-Konsultation zu den Ansichten von Experten über digitale Kompetenz. Amt für Veröffentlichungen der Europäischen Union. https://publications.jrc.ec.europa.eu/repository/handle/JRC73694

Kampylis, P, Punie, Y & Devine, J 2015, Promoting effective digital-age learning: a European framework for digitally competent educational organisations, Amt für Veröffentlichungen der Europäischen Union, Luxemburg

Microsoft Digital Defense Report. https://www.microsoft.com/de/security/business/security-intelligence-report

Ministerium für Bildung, Universität und Forschung, Italienische Regierung (2021), Innovare e potenziare le competenze digitali nella scuola, Memorandum of Understanding n. 785 vom 22. Januar 2021

Ministerium für technologische Innovation und digitalen Wandel (2020), 2025 - Strategia per l'innovazione tecnologica e la digitalizzazione del Paese.

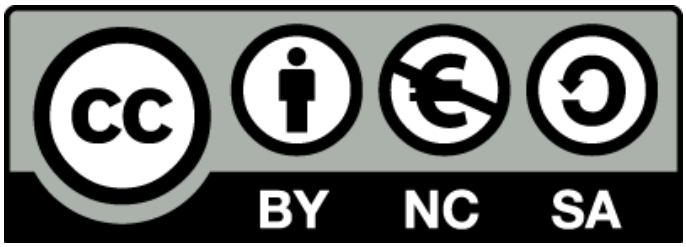
OECD. (2014). Bewertung der Problemlösungskompetenz in PISA 2012. In PISA 2012 Results: Creative Problem Solv-ing (Volume V): Students' Skills in Tackling Real-Life Problems. OECD Publishing, Paris. DOI: http://dx.doi.org/10.1787/9789264208070-6-en

Vuorikari, R., Punie, Y., Carretero Gomez, S., & Van den Brande, L. (2016). DigComp 2.0: The Digital Competence Framework for Citizens. Update Phase 1: the Conceptu-al Reference Model. Amt für Veröffentlichungen der Europäischen Union. https://publications.jrc.ec.europa.eu/repository/handle/JRC101254

DISCLAIMER

The European Commission support for the production of this publication does not constitute an endorsement of the contents which reflects the views only of the authors, and the Commission cannot be held responsible for any use which may be made of the information contained therein.

Es ist möglich, das Dokument über den folgenden QR-Code zu verfolgen:



Zurück zum Inhalt ☐