YBER.EU.VET

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

CYBER.EU.VET

KA226 – Partnerships for Digital Education Readiness

Projekt Nummer: 2020-1-DE02-KA226-C31C2976

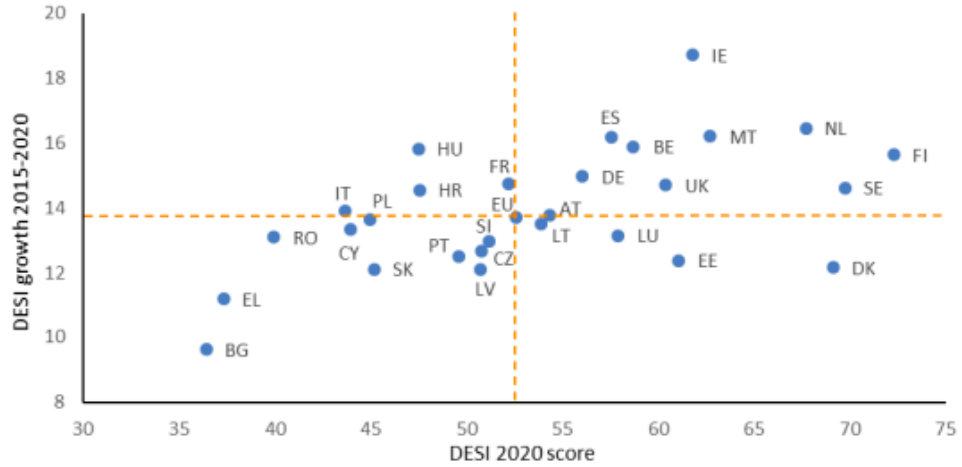
Konsortium-Bericht
über die wichtigsten Herausforderungen im Bereich der Cybersicherheit und Best Practices

Inhaltsverzeichnis

Einleitung

Da die Welt zunehmend digitalisiert wird, wird es immer offensichtlicher, dass die Praxis mit der aktuellen Politik verbunden werden sollte. Im europäischen Kontext liegt ein großer Schwerpunkt auf der Politik der digitalen Kompetenz und der Cybersicherheit. Es gibt jedoch weniger Beispiele für Initiativen, die diese Ziele im Einklang mit der entwickelten Politik erfüllen. Um genau zu beobachten, inwieweit digitale und Cybersicherheitskompetenzen ein zentrales und divergierendes Thema sind, ist es nützlich, den Index für die digitale Wirtschaft und Gesellschaft 2020 (DESI) zu betrachten.

Als Teil seines Gesamtbildes überwacht DESI die digitale Gesamtleistung Europas und misst das Niveau der digitalen Wettbewerbsfähigkeit in den EU-Ländern. Indem es Informationen über den Stand der Digitalisierung in den einzelnen Mitgliedstaaten liefert, hilft es, Bereiche für Investitionen und weitere Maßnahmen zu identifizieren. Auf dem Weg zu einer digitalen Zukunft, die auf die Bedürfnisse der Menschen zugeschnitten ist und die Grundwerte der EU respektiert, hat die Kommission im Februar 2020 eine Vision für die digitale Transformation "Shaping Europe's digital future" vorgestellt. Der DESI 2020 Bericht bewertet die digitale Wirtschaft und Gesellschaft zu Beginn der Pandemie anhand von Daten aus dem Jahr 2019.



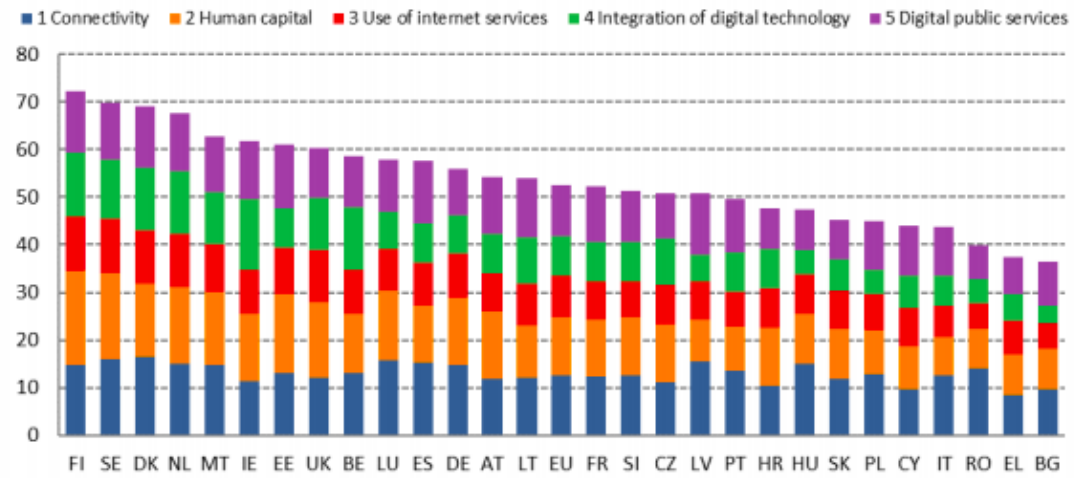
Source: DESI 2020, European Commission.

Dieser Index untersucht und sammelt die Daten über:

- Konnektivität: Die Verfügbarkeit eines schnellen und zuverlässigen Internetzugangs (einschließlich Festnetz- und Mobilfunkverbindungen) ist in der heutigen Zeit der Online-Bereitstellung wichtiger gesellschaftlicher und wirtschaftlicher Dienstleistungen von entscheidender Bedeutung;
- Humankapital: Das Rückgrat der digitalen Gesellschaft sind die digitalen Fähigkeiten der Menschen. Nutzer von digitalen Diensten und Menschen, die in ihrer Mobilität eingeschränkt sind, können über diese Geräte grundlegende Aktivitäten online durchführen;
- Nutzung des Internets: Mit dem Fortschreiten der Pandemie nutzten immer mehr Menschen das Internet. Die allgemeine Einschränkung führte zu einem regelmäßigen Zugang zu sozialen Medien und Unterhaltungsplattformen sowie zu Telearbeit und E-Commerce-Diensten;
- Integration der digitalen Technologie: Die Unternehmen haben schnell neue Arbeitsregelungen eingeführt, um sich an die Maßnahmen der Regierung anzupassen, die die soziale Interaktion einschränkten;

- Angesichts der Maßnahmen zur sozialen Distanzierung ist es notwendig, die staatlichen Aktivitäten fortzusetzen, um sicherzustellen, dass die digitalen öffentlichen Dienste Nutzen bringen. Es wird robuster digitaler öffentlicher Dienste in allen Mitgliedstaaten bedürfen, um eine erfolgreiche Ausstiegsstrategie aus der derzeitigen Pandemie zu erreichen.

Eine solche Analyse ist hilfreich, wenn man das Partnerkonsortium betrachtet, in dem die Mitgliedsländer in Bezug auf die digitale und Cybersicherheit sehr unterschiedlich sind. Drei von ihnen (in der Reihenfolge der Erstplatzierten: Irland, Spanien und Deutschland) erreichen eine bessere Bewertung als der EU-Durchschnitt, während die anderen vier (Frankreich, Lettland, Portugal und Italien) schlechter abschneiden.



Source: DESI 2020, European Commission.

Es ist wichtig zu betonen, dass die Ergebnisse des DESI 2020 keine lineare Entsprechung zwischen dem BIP eines Landes und der Verbreitung digitaler Kompetenzen zu bestätigen scheinen. So rangiert beispielsweise Spanien als 5. Volkswirtschaft der EU nur auf Platz 10 des Digital Economy and Society Index. In einigen der Länder, die dem Konsortium angehören,

wurden kürzlich mehrere Initiativen zur Verbesserung der Digitalisierung von Wirtschaft und Gesellschaft eingeführt. Als führendes Land in der EU bei der 5G-Bereitschaft hat Deutschland mehrere Maßnahmen ergriffen, um die Digitalisierung voranzutreiben, darunter Initiativen in den Bereichen IT-Sicherheit, Supercomputing, KI und Blockchain. In Frankreich wurden zahlreiche Anstrengungen unternommen, um die Digitalisierung von Unternehmen und öffentlichen Diensten zu erleichtern, darunter auch der Aufbau eines Ökosystems zur Unterstützung von Tech-Start-ups. Die italienische Regierung hat im Dezember 2020 'Italia 2025' verabschiedet, einen 5-Jahres-Plan, der Innovation und Digitalisierung in den Mittelpunkt eines "Prozesses zur radikalen und strukturellen Transformation des Landes" stellt. In den kommenden Jahren könnten diese Initiativen - die eine nachhaltige Umsetzung im Laufe der Zeit erfordern und wahrscheinlich auch Investitionen erfordern - zu Fortschritten dieser Mitgliedsstaaten bei der DESI führen.

Ein weiterer wichtiger Aspekt bei der Betrachtung des Niveaus der digitalen und Cybersicherheitskenntnisse sind die Auswirkungen der COVID-19-Pandemie auf diese Themen. Auch wenn ein solcher Zusammenhang zwischen der Gesundheitskrise und der Zahl der Cyberangriffe für die meisten Menschen nicht sofort ersichtlich ist, so hat die Pandemie doch zu einem Anstieg der Cyberangriffe geführt. Da so viele Unternehmen im Jahr 2020 zu neuen Digital-First-Strategien übergegangen sind (z. B. Remote-Arbeit), haben sie sich ungewollt einer Reihe neuer Angriffsvektoren geöffnet, die Kriminelle schnell ausnutzen konnten. Unter anderem wurde das unerwartete Auftreten von COVID-19 genutzt, um Malware zu verbreiten: z.B. E-Mails im Namen der Weltgesundheitsorganisation mit dem Hinweis, der Anhang enthalte die neuesten Informationen über die Pandemie; Links zu Diagrammen, die die Ausbreitung des Virus zeigen und deren Funktion es war, Benutzerdaten zu stehlen; bösartige E-Mails an Einrichtungen des Gesundheitswesens über die Lieferung von COVID-19-Schutzausrüstung und viele andere.

Bei der Fertigstellung dieses Forschungsberichts des Konsortiums haben wir uns auf Sekundärforschung gestützt, d.h. wir haben Daten, Veröffentlichungen, EU-Berichte, nationale und europäische Gesetzgebungen ausfindig gemacht und gesammelt, indem wir den im Bericht angegebenen Referenzen gefolgt sind. Die Studie untersuchte insbesondere die Frage der digitalen Kompetenz und der Cybersicherheit in den verschiedenen nationalen Kontexten, wobei der Schwerpunkt auf der Ausbildung von Berufsschullehrern lag. Darüber hinaus hebt dieser Forschungsbericht des Konsortiums einige der Hauptakteure hervor, die im Bereich der Cybersicherheit tätig sind, darunter die nationalen Einrichtungen und die Agentur der Europäischen Union für Cybersicherheit (ENISA), die mit den Mitgliedstaaten und den EU-Einrichtungen zusammenarbeitet und Europa bei der Vorbereitung auf künftige Herausforderungen im Bereich der Cybersicherheit unterstützt.

1.Desk-Research über die digitalen Fähigkeiten von Berufsschullehrern

Deutschland:

- Datenreport (2019) des Bundesinstituts für Berufsbildung (BIBB) zählt die "Digitalisierung" zu den drei wichtigsten Trends für Ausbildungsberufe und die Berufsbildung im Allgemeinen.
- Konkret heißt es in dem Bericht: "Die Digitalisierung wird den Strukturwandel auf dem Arbeitsmarkt verstärken", was zu einer Verlagerung der Ausbildungskapazitäten in den jeweiligen Bereichen führen wird. Infolgedessen wird der deutsche wie auch der europäische Arbeitsmarkt in Zukunft einen besonderen Bedarf an hochqualifizierten Fachkräften haben.
- Wie im Beschluss der Kultusministerkonferenz (2016-2017) - "Bildung in der digitalen Welt" - dargelegt, ist im Bereich der beruflichen Bildung die Förderung berufsbezogener Kompetenzen im Kontext digitaler Arbeits- und Geschäftsprozesse ein wesentlicher Teil der Kompetenz der Lehrkräfte als Ausgangspunkt für ihr didaktisches Handeln.
- Das Bundesministerium für Bildung und Forschung (BMBF) und das Bundesinstitut für Berufsbildung (BIBB) beschäftigen sich seit 2015 in Forschung, Entwicklung und Praxis mit Fragen der digitalen Transformation der Arbeitswelt und der beruflichen Bildung.

Irland:

- Eine der wichtigsten Strategien Irlands in Bezug auf die digitalen Fähigkeiten von Lehrkräften in der beruflichen Bildung ist die Nationale Digitale Strategie, die im Juli 2013 eingeführt wurde.
- Die Strategie konzentriert sich auf das digitale Engagement und zeigt auf, wie Irland von einer digital engagierten Gesellschaft profitieren kann.
- Die Strategie enthält eine klare Vision für den digitalen Fortschritt Irlands durch die Umsetzung einer Reihe praktischer Maßnahmen, die dazu beitragen sollen, dass sich

mehr Bürger und Unternehmen über Industrie und Unternehmen, Bürgerschulung, Schulen und Bildung online engagieren.

- Was die digitalen Fähigkeiten von Lehrkräften in der beruflichen Bildung betrifft, so zeigt sich immer deutlicher, dass die Kluft zwischen Lehrkräften, die digitale Geräte im Unterricht als Lernmittel einsetzen, und solchen, die dies nicht tun, immer größer wird.
- Viele Pädagogen haben erklärt, dass sie das Gefühl haben, dass digitale Geräte bei den Lernenden "Ablenkungen provozieren" können. Im Gegenteil, viele Pädagogen sind der Meinung, dass digitale Geräte und Apps im Rahmen von Lernaktivitäten die Lernenden stärken und sie dabei unterstützen können, sich mit den Lebenskompetenzen des 21. Jahrhunderts zu beschäftigen, wie z.B. Rechnungen online zu bezahlen oder sich auf Jobs zu bewerben.

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 beim Bildungsniveau gemacht, aber es bleibt unter dem EU-Durchschnitt. Obwohl weniger als 2015 (73,7%), lag der Anteil der Menschen mit niedrigem oder ohne Abschluss 2019 bei 50,2%, dem höchsten in der EU.

Italien:

- Im Bereich der Bildung wurden die Maßnahmen hauptsächlich durch die Umsetzung des Nationalen Plans für digitale Schulen (Piano Nazionale Scuola Digitale - PNSD) durchgeführt.
- Dies ist das Leitliniendokument des Ministeriums für Bildung, Universität und Forschung für die Einführung einer umfassenden Innovationsstrategie für die italienische Schule und für eine neue Positionierung des Bildungssystems im digitalen Zeitalter.
- Die meisten Maßnahmen zur Ausbildung des Schulpersonals zielten auf Grund- und Sekundarschulen ab, die die Mehrheit der Schulen in Italien ausmachen, während dem Bereich der beruflichen Aus- und Weiterbildung (VET) wenig Aufmerksamkeit geschenkt wurde.
- In diesem Zusammenhang wurden Projekte für postsekundäre technische Bildungseinrichtungen und Berufsbildungsinstitute (Istituti Tecnici Superiori - ITS) durchgeführt, wobei der Schwerpunkt auf der Stärkung der Fähigkeiten der Studenten lag.
- Im Jahr 2019 waren beispielsweise im Rahmen des Projekts "ITS 4.0" über 1.170 ITS-Studenten und etwa 130 Partnerunternehmen an 106 technologischen Innovationsprojekten beteiligt, die sich auf Technologien wie 3D-Druck, virtuelle Realität und Big Data konzentrieren.

Spanien:

- Die Digitale Agenda für Spanien (ADpE, Agenda Digital para España), die 2013 veröffentlicht wurde, ist der Fahrplan für die Erfüllung 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. Unter den spezifischen Maßnahmen können für die Zwecke dieser Analyse die folgenden Maßnahmen hervorgehoben werden:

- den Nationalen Katalog beruflicher Qualifikationen im Hinblick auf IKT-Fähigkeiten und -Schulungen zu aktualisieren und diese Aktualisierung in die Schulungsangebote aufzunehmen, mit denen berufliche Qualifikationen akkreditiert werden;
- Maximierung der Effizienz bei der Verwaltung und Zuteilung von Schulungsgeldern für die Weiterbildung im IKT-Bereich, sowohl für Arbeitnehmer des privaten als auch des öffentlichen Sektors, mit besonderem Augenmerk auf die Nutzung von virtuellen Online-Schulungsplattformen;
- einen Teil der für die berufliche Weiterbildung zur Verfügung stehenden Mittel für den Erwerb und die Verbesserung der digitalen Fähigkeiten von IKT-Fachkräften einzusetzen;
- die Berufsausbildung im Bereich der IKT neu zu gestalten und unter anderem Spezialisierungskurse in den Bildungsauftrag aufzunehmen;
- eine Verbesserung des Hochschulangebots zu fördern, das darauf abzielt, IKT-Fachleute durch ihre Anpassung an die Marktbedürfnisse auszubilden, neue Berufsprofile im Bereich der IKT in Betracht zu ziehen und die Effizienz des Systems zu steigern.

Frankreich:

- Betrachtet man das Tempo der Schulungen zum Einsatz von IKT an den französischen Universitäten, die dies anbieten, so stellt man fest, dass es keine klaren und nachhaltigen Strategien für die Schulung von Ausbildern zum Einsatz 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 französische Nationale Agentur für die Sicherheit von Informationssystemen (ANSSI) hat einen sehr schnellen Anstieg der Cyber-Bedrohung in Frankreich festgestellt. Die Zahl der Cyberangriffe hat sich seit 2019 explosionsartig erhöht: Die Zahl der Opfer hat sich innerhalb eines Jahres vervierfacht.
- Die Statistiken zeigen, dass die Dichte der IT-Ausbildung von einer französischsprachigen Region zur anderen variiert. Dafür gibt es mehrere Gründe, von denen die wichtigsten zweifellos mit den akademischen Einrichtungen und ihren Regierungen zu tun haben.
- Weitere Studien, um den Unterschied festzustellen, könnten zu einem späteren Zeitpunkt von den Regionalbüros oder den CNFs entsprechend ihrer eigenen lokalen oder regionalen digitalen Bildungspolitik durchgeführt werden.

Lettland:

- Obwohl es in Lettland derzeit an Forschungsstudien und Daten zur Cybersicherheit und anderen digitalen Fähigkeiten von Lehrkräften in der Berufsbildung und anderen Bildungseinrichtungen mangelt, ist es offensichtlich, dass der Übergang zum Fernunterricht aufgrund der Covid-19-Krise für viele Lehrkräfte eine große Herausforderung darstellte.
- Was die nationalen Strategien betrifft, so werden in den Planungsdokumenten für den neuen Haushaltszeitraum (2021-2027) folgende Aspekte hervorgehoben:
    - Die Entwicklung digitaler Kompetenzen im Bildungssektor (Leitlinien für die digitale Transformation 2021-2027) - sie sieht die Entwicklung digitaler Kompetenzen von Pädagogen und Leitern von Bildungseinrichtungen, die Entwicklung und Nutzung digitaler Kompetenzen im Bildungsprozess sowie die Unterstützung der Entwicklung digitaler Kompetenzen von berufstätigen Erwachsenen vor;
    - Die Entwicklung digitaler Fähigkeiten ist Teil des Programms zur Entwicklung der beruflichen Kompetenzen von Pädagogen (Education Development Guidelines

2021- 2027). Im Jahr 2020 hat das Ministerium für Bildung und Wissenschaft der Republik Lettland die Verbesserung der digitalen Kompetenz von Pädagogen als vorrangiges Ziel der beruflichen Kompetenz festgelegt und zu diesem Zweck zusätzliche Mittel (0,5 Millionen EUR) bereitgestellt;

- Die Notwendigkeit, das Bewusstsein von Lernenden und Lehrenden für Informationssicherheit, Datenschutz und die Nutzung zuverlässiger elektronischer Dienste zu schärfen (Cybersicherheitsstrategie 2019-2022, Aktionsbereich "Öffentliches Bewusstsein, Bildung und Forschung");
- Die Entwicklung digitaler Kompetenzen in der Gesellschaft (Leitlinien für die Entwicklung des Bildungswesens 2021-2027, Leitlinien für die digitale Transformation 2021-2027), da digitale Fertigkeiten inzwischen in ihrer Bedeutung mit Lese-, Schreib- und Rechenkenntnissen gleichgesetzt werden und zumindest auf der Grundstufe für jeden erforderlich sind, unabhängig vom Tätigkeitsbereich (digitale Fertigkeiten = Querschnittsfertigkeiten). Es sollten Maßnahmen ergriffen werden, um die Bevölkerung über die grundlegenden digitalen Fähigkeiten, die Medienkompetenz und die Informationskompetenz aufzuklären, die die gesamte Palette der Grundfertigkeiten, einschließlich der Cyberfähigkeiten, umfasst;

Die Aufmerksamkeit, die dem oben erwähnten DESI-Index in der Einleitung dieses Forschungsberichts gewidmet wurde, ist durch die Genauigkeit gerechtfertigt, mit der er den Stand der Technik und den abweichenden Charakter in den verschiedenen europäischen Ländern beschreibt. Eine solche Genauigkeit wird auch von den einzelnen nationalen Berichten über die digitalen Kompetenzen von Berufsschullehrern bestätigt.

Wir sind der Meinung, dass es besonders nützlich ist, die beiden Extreme des Konsortiums zu vergleichen, um zu verstehen, wie sich unterschiedliche Grade an digitalen Fähigkeiten auf die nationale Bevölkerung und speziell auf die Berufsausbilder auswirken. Wir werden zunächst Irland betrachten, das auf der DESI-Klassifizierung auf Platz 6 liegt.
Nach Angaben des irischen Zentralamts für Statistik (CSO) haben im Jahr 2018 89 Prozent der Haushalte
Internetzugang von zu Hause aus. Außerdem befinden sich über 30 Prozent aller EU-Daten in Irland, da viele der weltweit größten Technologieunternehmen ihren Hauptsitz in Europa haben. Wenn man beide Statistiken zusammennimmt, ist es selbstverständlich, dass es von entscheidender Bedeutung ist, sicherzustellen, dass Irland ein Land ist, das auf die Cybersicherheit vorbereitet ist. In diesem nationalen Bericht wird auf die wichtigsten Gesetze verwiesen, die es in Irland in Bezug auf digitale Kompetenz und
Cybersicherheit. Während sich die Welt weiterhin an das "Leben mit COVID-19" anpasst, muss sichergestellt werden, dass die Landschaft zur Bekämpfung von Cyberkriminalität und die Modelle für bewährte Verfahren weiterhin Einfluss auf Politik und Praxis haben.

Eine der wichtigsten Strategien Irlands in Bezug auf digitale Fähigkeiten ist die Nationale Digitale Strategie, die im Juli 2013 eingeführt wurde. Die Strategie konzentriert sich auf das digitale Engagement und zeigt auf, wie Irland von einer digital engagierten Gesellschaft profitieren kann. Die Strategie enthält eine klare Vision für Irlands digitalen Fortschritt durch die Umsetzung einer Reihe praktischer Maßnahmen, die dazu beitragen sollen, die Zahl der Bürger

und Unternehmen, die sich online engagieren, durch Industrie und Unternehmen, Bürgerschulung, Schulen und Bildung zu erhöhen. Für das Jahr 2021 kündigte die Bildungsministerin Norma Foley die Entwicklung einer neuen digitalen Strategie für Grundschulen an. Die Strategie soll sich in erster Linie auf den Einsatz digitaler Technologie im Bildungswesen konzentrieren und das Lernen durch die Einbindung von Technologie in die Zukunft verbessern. Im Bereich der Hochschulbildung in Irland ist eine der bemerkenswertesten Entwicklungen ein Fahrplan für digitales Lernen in der Hochschulbildung: 2015 - 2017, der entwickelt wurde, um einen "koordinierten, mehrstufigen Ansatz zur Förderung der digitalen Kompetenz, der Fähigkeiten und des Vertrauens unter den Studenten auf allen Ebenen der Bildung" zu unterstützen.

Im Bereich der Weiterbildung und Schulung wurde ein relativ neues Ministerium für Weiterbildung und Hochschulbildung, Forschung, Innovation und Wissenschaft eingerichtet. Im Rahmen der Dreijahresstrategie des Ministeriums liegt ein Schwerpunkt auf den digitalen Fähigkeiten, wobei eine neue 10-Jahres-Strategie zur Verbesserung der Lese-, Schreib- und Rechenkenntnisse sowie der digitalen Fähigkeiten umgesetzt werden soll. Außerdem konzentrieren sie sich auf
die Reform der Berufsausbildung und die Investition in die Förderung digitaler Kompetenzen. Was die digitalen Fähigkeiten von Lehrkräften in der beruflichen Bildung betrifft, so zeigt sich immer deutlicher, dass die Kluft zwischen Lehrkräften, die digitale Geräte im Unterricht als Lernmittel einsetzen, und solchen, die dies nicht tun, wächst.

Viele Pädagogen haben erklärt, dass sie das Gefühl haben, dass digitale Geräte bei den Lernenden "Ablenkungen provozieren" können. Im Gegenteil, viele Pädagogen sind der Meinung, dass digitale Geräte und Apps im Rahmen von Lernaktivitäten die Lernenden befähigen und sie dabei unterstützen können, sich mit den Lebenskompetenzen des 21. Jahrhunderts zu beschäftigen, z.B. Rechnungen online zu bezahlen oder sich für Jobs zu

bewerben. Eine letzte regierungsübergreifende Strategie, die aus irischer Sicht erwähnenswert ist, ist die Future Jobs Ireland Initiative von 2018, die eine Philosophie des lebenslangen Lernens betont. Innerhalb ihrer fünf Hauptthemen konzentriert sich die zweite Strategie auf "Innovation und Technologie, einschließlich der Vorbereitung auf den Übergang zur digitalen Wirtschaft". Die Strategie ist von zentraler Bedeutung für die Diskussionen über die Notwendigkeit weiterer Forschung und Investitionen auf dem Gebiet der digitalen Kompetenzen.

Ein solches gemeinsames Verständnis und eine solche Wertschätzung der digitalen Mittel bestätigen Irland als ein führendes Land in Bezug auf die Integration digitaler Technologie. Eine solche Integration ist unter anderem eines der Hauptthemen für den italienischen Kontext.
In Italien verfügt weniger als die Hälfte der Bevölkerung über digitale Grundkenntnisse und der Prozentsatz der IKT-Spezialisten, der nur 1% der italienischen Hochschulabsolventen ausmacht, liegt immer noch unter dem EU-Durchschnitt, obwohl er in den letzten Jahren gestiegen ist. Darüber hinaus sehen die Daten der OECD Teaching and Learning International Survey (2013) Italien an erster Stelle, was den IKT-Ausbildungsbedarf seiner Lehrer angeht. Mindestens 36% der italienischen Lehrer erklärten, dass sie nicht ausreichend auf den digitalen Unterricht vorbereitet seien, verglichen mit einem OECD-Durchschnitt von 17%, was zeigt, dass eine spezifische Ausbildung erforderlich ist.

In den letzten Jahren hat Italien im Rahmen seiner Politik Maßnahmen zur Förderung digitaler Kompetenzen in mehrere sektorale Strategien aufgenommen. Im Bildungsbereich wurden die Maßnahmen vor allem durch die Umsetzung des Nationalen Digitalen Schulplans (Piano Nazionale Scuola Digitale - PNSD) durchgeführt, der das Leitdokument des Ministeriums für Bildung, Universität und Forschung für die Einführung einer umfassenden Innovationsstrategie für die italienische Schule und für eine neue Positionierung des Bildungssystems im digitalen Zeitalter ist. Es ist ein Grundpfeiler von La Buona Scuola (Gesetz 107/2015), einer operativen Vision, die die Position der Regierung in Bezug auf die wichtigsten

Innovationsherausforderungen des öffentlichen Systems widerspiegelt und im Zentrum dieser Vision stehen die Innovation des Schulsystems und die Möglichkeiten der digitalen Bildung. Die vom PNSD identifizierten Interventionsbereiche sind: Zugang, Räume und Lernumgebungen, digitale Verwaltung, digitale Identität, Schülerfähigkeiten, Unternehmertum und Arbeitsmarkt, digitale Inhalte, Personalausbildung. In Bezug auf den letzten Punkt argumentiert die PNSD, dass die Ausbildung von Lehrern auf Bildungsinnovationen ausgerichtet sein muss, wobei digitale Technologien als Unterstützung für die Umsetzung neuer Bildungsparadigmen und die operative Planung von Aktivitäten berücksichtigt werden müssen. Die Ziele dieser Aktion sind:

- Verstärken Sie die Vorbereitung des Personals im Bereich der digitalen Fähigkeiten und erreichen Sie die gesamte Schulgemeinschaft;
- Fördern Sie die Verbindung zwischen Bildungsinnovation und digitalen Technologien;
- Entwickeln Sie im Laufe der Zeit wirksame, nachhaltige und kontinuierliche Standards für die Ausbildung in pädagogischer Innovation;
- Verstärken Sie die Ausbildung im Bereich Bildungsinnovation auf allen Ebenen (Erstausbildung, neue Mitarbeiter, im Dienst).

Um die Ausbildung von Lehrern in IT-Fächern zu fördern, wurde eine Absichtserklärung mit Ausbildungseinrichtungen unterzeichnet und es wurden finanzielle Mittel bereitgestellt, um die Teilnahme an den Kursen zu erleichtern, z.B:

- Memorandum of Understanding Nr. 785 vom 22. Januar 2021 zwischen dem Bildungsministerium und Cisco "Innovation und Verbesserung der digitalen Fähigkeiten in der Schule" und Schulungsprogramm "Vernetzte und sichere Lehrer".
- Absichtserklärung Nr. 4 vom 28. Oktober 2020 zwischen dem Bildungsministerium und S.O.S. The Telefono Azzurro Onlus zur Durchführung gemeinsamer Bildungs- und Ausbildungsaktivitäten zur Förderung der Erziehung zur digitalen Bürgerschaft und des bewussten Umgangs mit digitalen Technologien, sozialen Medien und Fortbildungskursen für Lehrer.

Bisher waren die meisten Maßnahmen zur Ausbildung des Schulpersonals 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. In diesem Zusammenhang wurden Projekte für postsekundäre technische Bildungseinrichtungen und Berufsbildungsinstitute (Istituti Tecnici Superiori - ITS) mit besonderem Schwerpunkt auf der Stärkung der Fähigkeiten der Studenten durchgeführt. Im Jahr 2019 waren beispielsweise im Rahmen des Projekts "ITS 4.0" über 1.170 ITS-Studenten und etwa 130 Partnerunternehmen an 106 technologischen Innovationsprojekten beteiligt, die sich auf Technologien wie 3D-Druck, virtuelle Realität und Big Data konzentrieren.

Ein weiteres Instrument, das zum Erwerb digitaler Kompetenzen beitragen wird, ist im Nationalen Plan für Wiederaufbau und Resilienz (Piano Nazionale di Ripresa e Resilienza - PNRR) enthalten, der Teil des EU-Programms Next Generation ist, einem 750-Milliarden-Euro-Paket, von dem fast die Hälfte aus Zuschüssen besteht, die von der Europäischen Union als Reaktion auf die Pandemiekrise vereinbart wurden. Das PNRR wird die Entwicklung digitaler Fähigkeiten von Schulpersonal fördern, um einen zugänglichen, integrativen und intelligenten Ansatz für die digitale Bildung zu unterstützen. Das Hauptziel ist die Schaffung eines Ökosystems digitaler Kompetenzen, das die digitale Transformation der Schulorganisation und der Lern- und Lehrprozesse beschleunigen kann, in Übereinstimmung mit dem europäischen Referenzrahmen für digitale Kompetenzen DigComp 2.1 (für Schüler) und DigCompEdu (für Lehrer). Die Umsetzung dieser Aktionslinie wird vom Bildungsministerium gewährleistet und betrifft etwa 650.000 Menschen, darunter Lehrer und Schulpersonal, sowie über 8.000 Bildungseinrichtungen. Die Regierung beabsichtigt, die berufliche Bildung zu stärken, insbesondere das tertiäre Berufsbildungssystem (ITS) und die MINT-Bildung, wobei die Gleichstellung der Geschlechter einen hohen Stellenwert einnimmt.

Die oben genannten Kontexte stellen zwei unterschiedliche nationale Kontexte dar. Um einen näheren Einblick in den allgemeinen europäischen Rahmen zu erhalten, kann es nützlich sein, die digitale Kompetenzlandschaft in Frankreich zu analysieren, einem Land, das auf der DESI-Skala sehr nahe am europäischen Durchschnitt liegt und diesem unmittelbar folgt.

Die französische Nationale Agentur für die Sicherheit von Informationssystemen (ANSSI) hat einen sehr schnellen Anstieg der Cyber-Bedrohung in Frankreich festgestellt. Die Zahl der Cyberangriffe hat sich seit 2019 explosionsartig erhöht: Die Zahl der Opfer hat sich innerhalb eines Jahres vervierfacht. Dies ist besonders besorgniserregend, vor allem in einem Kontext, in dem jede Cyber-Attacke aufgrund der Gesundheitskrise wahrscheinlich noch stärkere Auswirkungen haben wird. Das mangelnde Bewusstsein für Cyber-Risiken, die fehlende Kontrolle über die Informationssysteme, die Nichteinhaltung von Computer-Hygienemaßnahmen, der Mangel an Cyber-Sicherheitsexperten und bis zu einem gewissen Grad die Vergrößerung der Angriffsfläche durch die weit verbreitete Nutzung von Telearbeit sind allesamt Schwachstellen, die von Cyber-Kriminellen ausgenutzt werden. Die Angriffskampagnen, die Frankreich im Jahr 2020 getroffen haben, haben viele Unternehmen erfolgreich gestört und erhebliche finanzielle Verluste verursacht. Die massive Nutzung von ausgelagerten digitalen Diensten, die oft weniger sicher sind, ist eine weit verbreitete Praxis, die Angreifer nicht auslassen. Die Statistiken zeigen, dass die Dichte der IT-Ausbildung von einer französischsprachigen Region zur anderen variiert. Hierfür gibt es mehrere Gründe. Der wichtigste davon hängt zweifellos mit den akademischen Einrichtungen und ihren Regierungen zusammen. Weitere Studien, um den Unterschied festzustellen, könnten zu einem späteren Zeitpunkt von den Regionalbüros oder den CNFs entsprechend ihrer eigenen lokalen oder regionalen digitalen Bildungspolitik durchgeführt werden. Die Statistik zeigt, dass auch die thematischen Bedürfnisse, die Gegenstand von Schulungsworkshops waren, von Region zu Region unterschiedlich sind. Die thematische Häufigkeit hängt in diesem Sinne auch von endogenen Faktoren ab, die mit der Nachfrage und dem Angebot in Abhängigkeit von den

Bedürfnissen und dem Entwicklungsstand der lokalen Partner in den Bereichen IKT/E und ODL zusammenhängen.

2. Desk-Research über die wichtigsten Fragen der digitalen Sicherheit in den Partnerländern

Deutschland:

- Um den spezifischen deutschen Kontext zu analysieren und eine Bedarfsanalyse zu erstellen, ist die Auswertung des Digitalbarometers 2020, einer repräsentativen Online-Befragung von Privatpersonen zum Thema Cybersicherheit, die gemeinsam vom BSI und dem Kommissariat für polizeiliche Kriminalprävention der Länder und des Bundes durchgeführt wurde, besonders wichtig.
- In den letzten Jahren war die Cyberkriminalität in Deutschland und Europa die Hauptursache für die jüngsten Cyberangriffe. Der BSI-Bericht 2020 bestätigt Datenlecks und kritische Schwachstellen in Software- und Hardwareprodukten. Diese Untersuchung hat auch einen Anstieg der Massen-Cyberkriminalität festgestellt, die sich gegen Privatpersonen, Wirtschaftsunternehmen und andere Institutionen richtet und Malware einsetzt.
- Die häufigste Schwachstelle, die von Malware ausgenutzt wird, ist eine Schwachstelle im Host-System. Bei Software- oder Hardware-Produkten können Schwachstellen in Gateways gefunden werden, z. B. in Gateways zwischen Büros oder Produktionsnetzwerken, oder sie können durch menschliches Versagen beim Social Engineering verursacht werden.
- Dieser Grad der Digitalisierung ist nicht ohne Risiken und Gefahren. Einer von vier Befragten gab an, im vergangenen Jahr Opfer von Cyberkriminalität geworden zu sein. Die Gesamtrate der Cyberkriminalität bleibt im Jahr 2020 konstant. Online-Shopping und der Zugriff Dritter auf Online-Konten sind die häufigsten Betrugsarten, von denen die Opfer betroffen sind (44%) bzw. (30%).

Trotz dieser Ergebnisse wünschen sich zwei Drittel der Befragten mehr Informationen zur Vorbeugung von Datendiebstahl (66%). Am häufigsten werden praktische Tipps gesucht, z. B. wie man sichere Passwörter für mehrere Online-Konten sicherstellt (59 %), gefolgt von Ratschlägen, welche Software am besten geeignet ist, um Online-Konten zu schützen (52 %), und Ratschlägen zu den Vor- und Nachteilen von Passwortmanagern (49 %).

Irland:

- Die Bedrohungen für die Cybersicherheit in Irland nehmen weiter zu. Der jüngste Angriff auf die irische Gesundheitsbehörde Health Service Executive (HSE) fand 2021 statt und hatte und hat weiterhin verheerende Auswirkungen auf das irische Gesundheitssystem.
- Irland beherbergt mehr als 30 % der Daten der EU, da viele Cybersecurity-Zentren ihren Sitz im Land haben. Obwohl dies viele Möglichkeiten bietet, führt es auch zu einer erhöhten Bedrohung durch Cyberkriminalität. Da Irland eine offene liberale Demokratie ist, gilt es als besonders anfällig für sogenannte "Hack and Leak"-Angriffe.
- Irlands zweite nationale Cybersicherheitsstrategie 2019 - 2024 wurde ins Leben gerufen, um die Cybersicherheitsbereitschaft des Landes zu erhöhen. Die wichtigsten Ziele der Strategie sind:
    - Gewährleistung der Bereitschaft Irlands zur Cybersicherheit und Reaktion auf und Management von Cybersicherheitsvorfällen, einschließlich solcher, die die nationale Sicherheit betreffen,
    - Schutz und Bewältigung jeglicher Unterbrechung von Diensten, die kritische nationale Infrastrukturen betreffen, durch Cyberangriffe,
    - Den Cybersecurity-Sektor in Irland weiter auszubauen und zu entwickeln und cyber-ready zu sein,
    - Die besten international verfügbaren Technologien und Maßnahmen in irischen Unternehmen einzusetzen,

- Stärkung des Bewusstseins und Entwicklung von Fähigkeiten im Bereich der Cybersicherheit bei Organisationen und Privatpersonen.

- Im Jahr 2018 wurde ein Aktionsplan für Online-Sicherheit ins Leben gerufen, der fünfundzwanzig Maßnahmen im Rahmen von fünf Hauptzielen umfasst, die sich auf die Gesetzgebung zu Cyberkriminalität, die Entfernung von illegalem und schädlichem Material und die Förderung der Online-Sicherheit konzentrieren.

Portugal:

- Die wichtigsten Themen zur digitalen Sicherheit sind:
  - Stiftung Ebene
    - Ermitteln Sie die Gefährdung Ihrer schulischen Infrastruktur und Anwendungen in der Online-Umgebung und ergreifen Sie Maßnahmen zur Risikominderung (sowohl strukturell als auch verhaltensbezogen);
    - Identifizieren und entschärfen Sie Schwachstellen;
    - Identifizieren Sie persönliche Informationen im Internet, die für einen Angriff verwendet werden können;
    - Angemessene Verhaltensweisen bei der Nutzung des Cyberspace zu erlernen;
  - Mittelstufe und Fortgeschrittene:
    - Sicherheit Programmierung Technische Umgebungen
    - Social Engineering
    - Offene Datenquellen erforschen
    - Drahtlose Netzwerke
    - Verschlüsselung und Passwörter

Italien:

- Das am weitesten verbreitete Sicherheitsproblem der letzten drei Jahre in Italien ist das Passwort-Phishing, das von 48% der italienischen Manager angegeben wird, gegenüber 36% der europäischen Manager. Außerdem haben 28% der italienischen Manager Probleme im Zusammenhang mit Zugang und Identität (dies entspricht dem europäischen Prozentsatz), gefolgt von dem Problem der auf Social Engineering basierenden Malware (24%).
- Darüber hinaus verfügen nur 42% der Menschen zwischen 16-74 Jahren über digitale Grundkenntnisse und der Anteil der Hochschulabsolventen in IT- und IKT-Fächern ist im europäischen Vergleich sehr niedrig.
- Die Regierung befasst sich mit digitalen Kompetenzen in "Italia 2025", einer Fünfjahresstrategie für Innovation und Digitalisierung, die 2019 gestartet wurde. Die Strategie umfasst insbesondere die "Digitale Republik", eine Initiative, die vom Ministerium für technologische Innovation und Digitalisierung gefördert und koordiniert wird.
- Die Initiative zielt darauf ab, eine Allianz zwischen öffentlichen und privaten Organisationen und Bürgern zu bilden und sie aufzufordern, konkrete Maßnahmen zur Förderung digitaler Kompetenzen zu ergreifen. Sie konzentriert sich auf drei Aktionslinien:
    - Förderung der digitalen Grundkenntnisse;
    - Förderung der Qualifizierung und Umschulung der Arbeitskräfte;
    - die Entwicklung von Fähigkeiten im Bereich IKT und neue Technologien.
- Ein weiterer Schritt nach vorne wird mit "Italia digitale 2026" gemacht, das fünf ehrgeizige Ziele setzt, die in den kommenden Jahren erreicht werden sollen:
    - Verbreiten Sie die digitale Identität und sorgen Sie dafür, dass sie von 70% der Bevölkerung genutzt wird;

- Überwindung der digitalen Qualifikationslücke, wobei mindestens 70% der Bevölkerung über digitale Kenntnisse verfügen
  fähig;
- Bringen Sie etwa 75% der italienischen PAs dazu, Cloud-Dienste zu nutzen;
- Erreichen Sie mindestens 80% der wesentlichen öffentlichen Dienste, die online angeboten werden;
- Erreichen Sie, in Zusammenarbeit mit der Mise, 100% der italienischen Familien und Unternehmen mit Ultrabreitbandnetzen.

Spanien:

- Die spanische Aktivierungsstrategie für Beschäftigung 2017-20 zielt darauf ab, den wirtschaftlichen Aufschwung durch die Förderung von Cybersicherheitsprogrammen und -ressourcen für Berufsbildungseinrichtungen zu konsolidieren, um den Herausforderungen des heutigen und zukünftigen Arbeitsmarktes, die sich aus der Globalisierung und Digitalisierung ergeben, zu begegnen. Sie legt die Maßnahmen fest, die sowohl auf staatlicher als auch auf regionaler Ebene von den öffentlichen Arbeitsverwaltungen (PES) durchgeführt werden sollen;
- In quantitativer Hinsicht ist eines der Ziele die Schulung von mindestens 225.000 jungen Menschen in digitalen Fertigkeiten: 75% in Grundkenntnissen und 25% in fortgeschrittenen digitalen Fertigkeiten, was 40% bzw. 38% der jungen Bevölkerung unter 30 Jahren entspricht.
  - Starthilfe für technologiebasierte Projekte für junge Frauen, Bereitstellung eines Beraters, der diese Unternehmerinnen bei ihrem Geschäftsplan berät und Überwachungsdienste anbietet;
  - spezifische Ausbildungsmaßnahmen für junge Frauen aus ländlichen Gebieten in IKT-Technologien und neuen Zukunftssektoren, unter Nutzung der Möglichkeiten

der neuen Technologien und mit Ausbildern und Tutoren, einschließlich Online-Unterricht;

- Förderung des Unternehmertums, der Selbständigkeit und der neuen Beschäftigungsmöglichkeiten, die die digitale Wirtschaft und die verschiedenen Formeln der Sozialwirtschaft und der Wirtschaft der digitalen Plattformen bieten, im Rahmen von Maßnahmen zur Aktivierung der Beschäftigung;
- Verbesserung der Sichtbarkeit von bewährten Praktiken, die entwickelt wurden, um zu verstehen, was die wichtigsten Themen der digitalen Sicherheit sind.

- Nationales operationelles Programm für Jugendbeschäftigung (Budget 39 Millionen Euro). Das Programm umfasst zum Beispiel einen Ausbildungsweg zur digitalen Transformation für die Beschäftigung.
- Das von EOI in Zusammenarbeit mit Google durchgeführte Projekt zielt darauf ab, die Beschäftigungsfähigkeit von jungen Menschen zu verbessern, die die Schule frühzeitig abgebrochen haben, arbeitslos geworden sind oder Schwierigkeiten haben, eine erste Stelle zu finden.

Frankreich:

- Die Hochschulminister der französischsprachigen Welt trafen sich am 5. Juni 2015 in Paris auf gemeinsame Initiative Frankreichs, der OIF (Organisation internationale de la francophonie) und der AUF (Agence universitaire de la francophonie), um den Stand und die Perspektiven der digitalen Entwicklung des französischsprachigen Hochschul- und Berufsbildungsraums zu untersuchen.
- Das Hauptziel dieser Arbeit war es, einen Beitrag zur Ausarbeitung einer frankophonen Strategie für die Ausbildung von Ausbildern im Bereich der digitalen Bildung zu leisten und den Ausbildungsbedarf und die Erwartungen der betroffenen Zielgruppen zu bewerten und dann zu ermitteln, was erforderlich ist, um diesen Bedarf und diese

Erwartungen zu erfüllen, insbesondere in Bezug auf Dienstleistungen, Inhalte und Kompetenzen.

- Laut der Studie "Étude sur l'identification des besoins en formation tic/e dans les pays francophones du sud, 2016" sind die Bedürfnisse der Lehrkräfte stark geprägt von einem einhelligen Trend zur Ausbildung in IKT/E und zum Aufbau von Kapazitäten im Zusammenhang mit der digitalen Bildung (80,4%).
- Die digitalen Risiken sind in den Darstellungen der jungen Lehrer sehr präsent, die den Mediendiskurs leicht weitergeben. Die drei Risiken, mit denen sich die Lehrer persönlich am meisten konfrontiert sehen, sind technische (66,20%), ethische und rechtliche (55,80%) und informationelle (54,70%).

Lettland:

- Laut der nationalen Cybersicherheitsstrategie 2019-202215 ist der lettische Cyberspace weiterhin großen Bedrohungen ausgesetzt - Phishing, Erpressung und Malware, Versuche, Systeme, Netzwerke und Websites zu hacken, Denial-of-Service-Angriffe (DoS) auf kritische Informationssysteme sowie betrügerische E-Mails und Social-Engineering-Kampagnen, um persönliche Daten oder Authentifizierungsdaten abzurufen, um eine bestimmte Person, ein Unternehmen oder eine Institution zu diskreditieren oder um Verbrechen zu begehen.
- Sowohl in Europa als auch in Lettland wurden die folgenden Vorfälle aktuell - Geld-Erpressungsversuche, die in erster Linie auf Finanzinstitutionen oder Unternehmen des Privatsektors abzielten (die Angreifer führten eine Reihe von Probeangriffen durch und drohten damit, den Betrieb von Unternehmens-Websites oder anderen Ressourcen durch Angriffe mit bis zu 2 Tb/s auszusetzen).
- Im Jahr 2021 sind Betrug, Malware und Sicherheitslücken weiterhin aktiv - gestohlene WhatsApp-Konten durch Aktivierungscodes, die von gehackten Konten aus der Kontaktliste einer Person angefordert werden; eine neue Welle von Erpressungs-E-Mails

(Sextortion), die mit der Verbreitung von kompromittierendem Material drohen, wenn der E-Mail-Nutzer kein Lösegeld zahlt.

- Das Jahr 2020 mit seinen globalen Veränderungen hat gezeigt, dass es für Pädagogen in der beruflichen Bildung und in anderen Bildungseinrichtungen wichtig ist, ihre Kenntnisse/Fähigkeiten in Bezug auf die sichere Fernarbeit bei der Organisation von Online-Kursen und der Nutzung digitaler Tools (E-Mails, WhatsApp, Lernplattformen usw.) zu erweitern und sich der aktuellen Betrugsfälle, insbesondere in den sozialen Medien, bewusst zu sein, um ihre Schüler und Studenten zu sensibilisieren.

Auch wenn der Zusammenhang zwischen der COVID-19-Pandemie und der Zahl der Cyberangriffe für die meisten Menschen nicht sofort ersichtlich ist, hat die erste Pandemie in Wirklichkeit zu einem Anstieg der zweiten geführt. Cyberkriminelle sind sehr flexibel, wenn es darum geht, neue Ereignisse auszunutzen, wie wir bei dem jüngsten Gesundheitsnotstand gesehen haben. Da so viele Unternehmen in diesem Jahr zu neuen Digital-First-Strategien übergegangen sind (z. B. Telearbeit), haben sie sich ungewollt einer Reihe neuer Angriffsvektoren geöffnet, die Kriminelle schnell ausnutzen konnten.

Die nationalen Büros bieten eine vielseitige Perspektive auf die wichtigsten digitalen und Cybersicherheitsthemen. Da das Fernstudium zur neuen Normalität wird, finden Cyberkriminelle neue Wege, um Techniken wie Phishing, Ransomware, Social Engineering und mehr für ihre Angriffe zu nutzen. Hier sind einige der kritischsten Risiken, denen man begegnet.

1. Sicherer Fernzugriff

Da der Fernunterricht den physischen Unterricht ablöst, benötigen Schüler und Lehrer Zugang zu Online-Lerntools, die sich hauptsächlich in der Cloud befinden, d.h. Anwendungen für die gemeinsame Nutzung von Dateien, E-Mails und Anwendungen, und manchmal müssen sie auch

aus der Ferne auf Ressourcen im Schulnetzwerk zugreifen. Wenn der Fernzugriff nicht gesichert ist, können Hacker in das System eindringen und die Kontrolle über das gesamte Netzwerk übernehmen.

2. Zugang zu sensiblen Daten

Bildungseinrichtungen sind eine Fundgrube für sensible Daten, die im Dark Web verkauft werden können. Die persönlichen Daten von Studenten, Lehrern, Ehemaligen und Verwaltungsmitarbeitern sowie sensible Daten, die sich auf die Forschung und das geistige Eigentum einer Schule beziehen, können für einen Hacker eine wahre Fundgrube sein, die er verkaufen oder erpressen kann. Daher ist es wichtig, einen identitätsbasierten Zugang zu implementieren, der es autorisierten Benutzern ermöglicht, nur auf die Ressourcen zuzugreifen, die sie für ihre Arbeit benötigen.

3. Malware

Der Übergang zum Fernunterricht bedeutet, dass viele Geräte, die mit dem Schulnetzwerk verbunden sind, BYOD (Bring Your Own Device) sind. Es ist schwierig zu wissen, ob die verwendeten Geräte und Anwendungen ordnungsgemäß mit Patches aktualisiert sind und ob das Antivirusprogramm selbst auf dem neuesten Stand ist. Wenn diese Remote-Geräte nicht über ein VPN verbunden sind, müssen Sie sicherstellen, dass sie sicher sind, bevor sie auf Ressourcen im Schulungsnetzwerk zugreifen können. Es ist wichtig, fortschrittliche Web-Schutzfunktionen einzusetzen, die die neuesten Web-Bedrohungen erkennen und blockieren können.

4. Phishing

Social-Engineering- und Phishing-Angriffe sind ein großes Cyber-Sicherheitsrisiko für französische Schulungszentren. Ausbilder und Lehrer oder Mitarbeiter, die dazu verleitet werden, auf bösartige Links zu klicken, können Cyberkriminellen Zugang zum Netzwerk der Schule und zu wertvollen Ressourcen verschaffen. Der beste Weg, Social Engineering und Phishing-Angriffen entgegenzuwirken, ist die Sensibilisierung und Schulung der Benutzer. Wenn Sie Ihre Benutzer mit simulierten Angriffen schulen und testen, können Sie eine positive Kultur

des Sicherheitsbewusstseins aufbauen und sie weniger anfällig für verschiedene Online-Betrügereien machen.

5. Betrug

In Bezug auf Betrug wurde das Jahr 2020 als sehr intensiv beschrieben, einschließlich Social-Engineering-Angriffen. Zu den aktivsten Betrugsversuchen gehörten Erpressungskampagnen, bei denen Hacker behaupteten, das Gerät eines Benutzers gehackt und kompromittierendes Material erhalten zu haben, für das ein Lösegeld gefordert wurde; betrügerische Gewinnspiele im Namen der bekannten Marken, bei denen man die neuesten Smartphones oder andere wertvolle Preise gewinnen konnte.

Es wurde ein neuer Trend beobachtet - Erpressungs-E-Mails mit der Drohung, dass Daten durchsickern. In vielen Fällen waren Unternehmen das Ziel. Irreführende Anzeigen in sozialen Medien - unter Verwendung der Namen berühmter Personen ohne deren Wissen - forderten Internetnutzer auf, in Kryptowährungen zu investieren. Betrüger riefen auch an und versuchten, die Menschen zu Investitionen zu überreden. In einigen Fällen wurden wiederholte Betrugsversuche beobachtet, bei denen den Opfern von Finanzbetrug Hilfe angeboten wurde, um ihre verlorenen Mittel zurückzubekommen.

Telefonbetrug - indem sie die Telefonnummern verschiedener Kreditinstitute fälschten und sich als Bankvertreter ausgaben, nutzten die Betrüger das mangelnde Wissen der Öffentlichkeit über zusätzliche Authentifizierungsmethoden, um finanzielle Mittel von mehreren Tausend Nutzern zu ergaunern, was den lettischen Kreditinstituten einen Gesamtschaden von Hunderttausenden bescherte. Anpassung der Hacker an die Notwendigkeit, mit der Fernarbeit zu beginnen - in Anbetracht der Notwendigkeit für Unternehmen, schnell auf Fernarbeit umzustellen und den elektronischen Dokumentenverkehr einzuführen, nutzten die Hacker die Situation, um z.B. eine Reihe von Buchhaltern eines Unternehmens per E-Mail im Namen des Geschäftsführers oder eines anderen Mitarbeiters aufzufordern, eine dringende Zahlung zu leisten oder das Lohnkonto zu ändern.

Eingriffe in die Geschäftskorrespondenz von Unternehmen - durch die Kompromittierung der E-Mails von Unternehmen oder deren Kooperationspartnern konnten Angreifer einen geeigneten Zeitpunkt wählen, um einer der Parteien eine Rechnung mit einem geänderten Konto zu schicken.

Viele Internetnutzer wurden zur Zielscheibe von betrügerischen Nachrichten mit Shortcut-Links (ej.uz), mit denen das eigentliche Link-Ziel verschleiert wird, im Namen der staatlichen Institutionen über den Ausnahmezustand und die epidemiologische Situation im Land.

Gefälschte Online-Shops - eine besonders hohe Aktivität wurde während der Weihnachtszeit durch Werbung in den sozialen Medien und aufgrund der Covid-19-Beschränkungen beobachtet, die Unternehmen dazu zwangen, ihre Produkte online zu verkaufen.

Es kann nützlich sein, einige Daten aus den nationalen Berichten zu verwenden. In Frankreich zum Beispiel sind die digitalen Risiken in den Darstellungen junger Lehrer, die den Mediendiskurs leicht weitergeben, sehr präsent. Die drei Risiken, mit denen sich die Lehrer persönlich am meisten konfrontiert sehen, sind technische (66,20%), ethische und rechtliche (55,80%) und informationelle (54,70%). Psycho-soziale, kognitive und sozio-ökonomische Risiken scheinen sie weniger zu beunruhigen. Es besteht eine systematische Diskrepanz zwischen den Darstellungen der Risiken für sie selbst und denen für die Schüler. Die drei Risiken, denen die Lehrer ihre Schüler am meisten ausgesetzt sehen, sind psychosoziale (69,95%), informationelle (70,75%) und technische (62,80%). Die Lehrer fühlen sich also in Bezug auf die technischen Risiken genauso verletzlich wie ihre Schüler, halten ihre Schüler aber insbesondere für Probleme im Zusammenhang mit Belästigung oder falschen Informationen für stärker gefährdet. Die Verstärkung der Risiken für Schüler kann dadurch erklärt werden, dass die Lehrer sie als sehr verletzlich wahrnehmen. Eine Referendarin beschrieb ihre Schüler der vierten Klasse als sehr verletzlich, ziemlich naiv und sich der potenziellen Gefahr der Netzwerke nicht unbedingt bewusst.

Das Bundesamt für Sicherheit in der Informationstechnik (BSI) stellte in seinem Bericht fest, dass mehrere Kampagnen die Verwirrung und Angst, die durch COVID-19 entstanden sind, ausnutzten, darunter Malware- und Phishing-Kampagnen, CEO-Betrug und Betrug. Außerdem sagte das BSI, dass solche Ereignisse die Erfolgschancen solcher Angriffe aufgrund der Ängste, Sorgen und Unsicherheiten, die mit solchen Ereignissen verbunden sind, erhöht haben könnten. In den letzten Jahren war in Deutschland und Europa die Cyberkriminalität die Hauptursache für die jüngsten Cyberangriffe. Um den spezifischen deutschen Kontext zu analysieren und eine Bedarfsanalyse zu erstellen, ist die Auswertung des Digitalbarometers 2020, einer repräsentativen Online-Befragung von Privatpersonen zum Thema Cybersicherheit, die gemeinsam vom BSI und der Polizeilichen Kriminalprävention der Länder und des Bundes durchgeführt wurde, von besonderer Bedeutung. Der digitale Wandel gestaltet unseren Alltag aktiv mit - vom Online-Shopping über Wearables (wie Fitnessarmbänder, Smartwatches oder Smart Glasses) bis hin zu neuen Zahlungs- und Ausweisverfahren.

Dieser Grad der Digitalisierung ist jedoch nicht ohne Risiken und Gefahren. Einer von vier Befragten gab an, im vergangenen Jahr Opfer von Cyberkriminalität geworden zu sein. Die Gesamtrate der Cyberkriminalität bleibt im Jahr 2020 konstant. Online-Shopping und der Zugriff Dritter auf Online-Konten sind die häufigsten Betrugsarten, von denen die Opfer betroffen sind (44%) bzw. (30%). Die meisten Befragten waren mit den jüngsten Empfehlungen zur Vorbeugung von Cyberkriminalität vertraut. Diese Empfehlungen werden im Allgemeinen nur dann befolgt, wenn es für die betreffende Person sinnvoll ist (41%) oder wenn sie gerade von einem bestimmten Ratschlag erfahren hat (39%). Die Forschung zeigt, dass Menschen, die bereits mehrfach Opfer geworden sind, eher dazu neigen, Ratschläge erst dann zu befolgen, wenn ein Problem auftritt (33%), selbst wenn sie sich dessen bereits bewusst waren. Trotz dieser Ergebnisse äußerten zwei Drittel der Befragten den Wunsch nach mehr Informationen zur Vorbeugung von Datendiebstahl (66 %). Die am häufigsten nachgefragten Ratschläge sind praktische Tipps, z. B. wie man sichere Passwörter für mehrere Online-Konten sicherstellt (59

%), gefolgt von Ratschlägen, welche Software am besten geeignet ist, um Online-Konten zu schützen (52 %), und Ratschlägen zu den Vor- und Nachteilen von Passwortmanagern (49 %).

Eine weitere wichtige Perspektive bietet schließlich Irland und die Bedrohungen der Cybersicherheit im Jahr 2021. Ein massiver und koordinierter Angriff begann im Mai 2021, störte den Gesundheitsdienst und die Computersysteme im ganzen Land, stahl persönliche Daten eines hohen Prozentsatzes von Patienten und fordert weiterhin ein Lösegeld für die Rückgabe der Daten. Als Reaktion darauf musste die Health Service Executive (HSE) die IT-Systeme der Krankenhäuser und des Gesundheitswesens abschalten, um einen weiteren Datendiebstahl zu verhindern. Viele Dienste wurden unterbrochen und persönliche und medizinische Daten wurden entwendet. Es gibt jedoch keine Anhaltspunkte dafür, dass weitere Betrügereien mit den Daten der Bürger stattgefunden haben. Irland beherbergt mehr als 30 % der Daten der EU, da viele Cybersecurity-Zentren ihren Sitz im Land haben. Dies bietet zwar viele Möglichkeiten, führt aber auch zu einem erhöhten Maß an Bedrohung durch Cyberkriminalität. Da Irland eine offene liberale Demokratie ist, gilt es als besonders anfällig für sogenannte "Hack and Leak"-Angriffe. Im Allgemeinen werden diese Angriffe als politisch motiviert angesehen und konzentrieren sich auf Fehlinformationen und "Fake News", mit denen versucht wird, den Staat zu destabilisieren.

Viele, die im Bereich der Cybersicherheit tätig sind, fordern verstärkte Investitionen in staatliche Einrichtungen wie das National Cyber Security Centre (NCSC) in Irland. Andere Bedrohungen/Risiken, die nach wie vor bestehen, sind die Risiken für kritische nationale Infrastrukturen (CNI), Systeme des öffentlichen Sektors und Daten, die in den vorangegangenen Abschnitten kurz skizziert wurden. Neue Probleme tauchen im Zusammenhang mit der Einführung von 5G-Technologien auf. Obwohl dies zu neuen Technologien und Diensten führen wird, muss die Cybersicherheit im Vordergrund stehen, da viele Länder mit der Anpassung beginnen.

Außerhalb der nationalen und geschäftlichen Perspektive gibt es weiterhin täglich eine Vielzahl von Verbrechen im Bereich der Cybersicherheit, die von Durchschnittsbürgern begangen werden. Sie werden oft nicht den Strafverfolgungsbehörden gemeldet. 2019 wurden in Irland nur fünf Prozent der Cyberstraftaten bei der Polizei angezeigt. Ein von Microsoft in Irland in Auftrag gegebener Bericht für das Jahr 2019 kommt außerdem zu dem Schluss, dass Mitarbeiter immer noch als "schwaches Glied" im Sicherheitssystem angesehen werden, und zwar aufgrund mangelnder Sicherheitsschulung, schlechter Passwortverwaltung, der Verwendung privater Geräte mit arbeitsbezogenen Daten und möglicher Verstöße gegen die EU-Datenschutzgrundverordnung.

3. Beste Praktiken für Cybersicherheitsprogramme und Ressourcen für Berufsbildungseinrichtungen in der EU und in jedem Partnerland

Wie in der Einleitung erwähnt, umfasst das Cyber. EU.VET Projekt ein facettenreiches und vielfältiges Konsortium. In Bezug auf digitale und Cybersicherheitskompetenzen sind die Partnerländer des Konsortiums unterschiedlich leistungsfähig, wie der DESI-Index perfekt beschreibt.

Die akademische Analyse und Bewertung bewährter Praktiken war ein integraler Bestandteil der Forschungsarbeit, die von jedem Partner des Projektkonsortiums auf nationaler Ebene durchgeführt wurde. Diese Forschung hatte als gemeinsame Leitlinie eine Bedarfsanalyse von Berufsbildungsfragen auf lokaler und nationaler Ebene. Bei der Durchführung dieser Arbeit teilten die sieben nationalen Partner einige Schwierigkeiten im Zusammenhang mit der Suche nach Schulungsinitiativen und Cybersicherheit, die speziell für Lehrkräfte der beruflichen Bildung entwickelt wurden. Dies hat die Aufgabe zwar ziemlich schwierig gemacht, aber auch noch deutlicher gezeigt, wie wichtig und notwendig es ist, Projekte in diesem Bereich zu entwickeln. Es hat dann den äußerst innovativen Geist des CYBER.EU.VET-Projekts bestätigt. Hier finden Sie eine Sammlung der wichtigsten bewährten Verfahren, die die einzelnen Partner gefunden haben.

3.1 Deutschland - Initiative Berufsbildung 4.0

Berufsbildung 4.0 ist eine Dachinitiative, die vom Bundesministerium für Bildung und Forschung (BMBF) und dem Bundesinstitut für Berufsbildung (BIBB) ab 2016 gemeinsam entwickelt wurde und eine Vielzahl von Projekten in drei Hauptsäulen zusammengeführt hat. Säule 2 dieser umfassenden Initiative (die noch läuft) ist ganz der "digitalen Bildung/Medienkompetenz" gewidmet und zielt darauf ab, Medienkompetenzen zu definieren, die als Zugangsvoraussetzung und als Schlüsselkompetenz für alle Berufe in der Berufsbildung (für Auszubildende, Lehrer und Ausbilder) gelten sollten. Förderprogramme zur besseren Ausstattung von Ausbildungszentren und zur Unterstützung kleiner und mittlerer Unternehmen (KMU) im Hinblick auf die Digitalisierung ergänzen diesen Ansatz der Förderung von Medienkompetenz in der Berufsbildung. Mit dem Sonderprogramm Digitalisierung der ÜBS (71) tragen das BMBF und das BIBB dazu bei, die Digitalisierung der Prozesse in der Ausbildung von Auszubildenden im Kontext von 'Berufsbildung 4.0' zu beschleunigen. Das Sonderprogramm besteht aus zwei Förderlinien:

1) Gefördert wird die Anschaffung ausgewählter digitaler Ausrüstungen (digitale Geräte, Maschinen, Systeme und Software, wie z.B. Smart-Home-Technologien, 21 Industrieroboter, 3D-Drucker und digitale Lehr- und Lernmedien, wie z.B. Tablets und Touchscreens), um die Ausbildung von Lehrlingen zu modernisieren, insbesondere für diejenigen, die von KMU ausgebildet werden;
2) Das Programm fördert zudem 8 Pilotprojekte in Kompetenzzentren, die die Auswirkungen der Digitalisierung auf die beruflichen Tätigkeitsprofile identifizieren und daraus resultierende Anforderungen und Konsequenzen für die Qualifizierung von Fach- und Ausbildungspersonal ermitteln. In einem zweiten Schritt entwickeln sie innovative Lehr- und Lernkonzepte für die Berufsbildung 4.0 und verbreiten diese als Multiplikatoren. Ziel ist es, die Übertragbarkeit der Ergebnisse und ein breites Anwendungsspektrum zu gewährleisten.

Im Folgenden finden Sie einige Beispiele für die oben genannten Pilotprojekte:

- "Digitale Medien in der Berufsbildung", das bis 2022 läuft und aus mehreren Teilprogrammen mit unterschiedlichen Förderschwerpunkten besteht, finanziert nationale digitale Ausbildungsprojekte, die neue Lernszenarien und moderne Aus- und Weiterbildungskurse zur Förderung des Erwerbs digitaler Medienkompetenz entwickeln;
- "Qualifizierungsinitiative Digitaler Wandel - Q 4.0", das ab 2018 die Entwicklung und Erprobung von Weiterbildungskonzepten für betriebliche Ausbilder fördert. Das Projekt besteht aus zwei Teilprojekten: 1) MIKA-Seminare (Medien- und IT-Kompetenz für Ausbildungspersonal) zur Förderung der medienpädagogischen Basiskompetenz, der Entwicklung und Erprobung von Weiterbildungsmodulen zur Stärkung der grundlegenden Medien- und IT-Kompetenzen des Ausbildungspersonals; 2) Q 4.0 NETZWERK mit dem Ziel, den Ausbildungsprozess an den digitalen Wandel anzupassen, wobei auch regionale und branchenspezifische Unterschiede berücksichtigt werden. Bei beiden Projekten könnte das Endergebnis ein Prototyp eines getesteten Seminarangebots sein, das dem Berufsbildungspersonal bundesweit zur Verfügung gestellt werden könnte;
- "Digitalisierung II" seit 2018, um Strategien für die Gestaltung von Lernprozessen zu identifizieren, die das Potenzial digitaler Medien nutzen, um erfolgreiches Lernen zu unterstützen, sowohl für Einzelpersonen als auch für Gruppen.

3.2 Frankreich - Internet Sans Crainte

(Da es in diesem Land an bewährten Praktiken im Bereich der Berufsbildung mangelt, wurde diese Fallstudie als eine Praxis ausgewählt, die zwar die geforderten Bedingungen erfüllt, aber nicht speziell den Berufsbildungssektor betrifft).

Angesichts der ständigen Fälle von Cybermobbing, Internetsucht, gefährlichen Begegnungen im Web und deren tragischen Folgen für sehr junge Schüler ist es notwendig geworden, die Aufmerksamkeit aller auf die Rechte und Grenzen des Online-Verhaltens zu lenken und vor allem das Internet als ein Werkzeug zur Bereicherung und Unterhaltung ohne Gefahren zu präsentieren. Das im Jahr 2000 gegründete Unternehmen Tralalere, Pionier der digitalen Pädagogik und Experte für die Kommunikation mit jungen Menschen, ist ein führender Produzent von medienübergreifenden Bildungsprogrammen: Cartoons für Multimedia-Produktionen, Serious Games, mobile Apps, eBooks usw. Insbesondere hat Tralalere das nationale Programm zur Sensibilisierung für Risiken im Internet konzipiert und geleitet: www.internetsanscrainte.fr.

Internet Sans Crainte wird seit 2008 von Tralalere betrieben und ist das nationale Programm, das jungen Menschen helfen soll, ihr digitales Leben besser zu kontrollieren. Konkret bietet Internet Sans Crainte etwa hundert kostenlose, schlüsselfertige Ressourcen an, die Lehrern, Erziehern und Eltern dabei helfen sollen, junge Menschen im Alter von 6 bis 18 Jahren zu einem aufgeklärten und verantwortungsvollen Umgang mit Bildschirmen und digitalen Technologien anzuleiten. Internet Sans Crainte bietet auch Ratschläge und Fachwissen, wie man junge Menschen bei ihrer digitalen Erziehung durch thematische Dateien unterstützen kann. Tralalere und Internet Sans Crainte koordinieren auch Safer Internet France, ein nationales und europäisches Programm zum Schutz von Minderjährigen im Internet, zusammen mit der Net Ecoute (e15 Enfance) Hotline und dem Point de contact. In dieser Eigenschaft organisiert

Internet Sans Crainte den Safer Internet Day in Frankreich, einen weltweiten Tag zur Sensibilisierung junger Menschen für eine bessere Nutzung des Internets. Dieses Programm wird von der Europäischen Kommission im Rahmen des Inhope/Insafe-Netzwerks, das 38 Länder umfasst, unterstützt.

BENEFICIARIES

Internet Sans Crainte bietet das ganze Jahr über digitale Ressourcen für verschiedene Zielgruppen an,

einschließlich:

- Bildungsvermittler (Lehrer, Animateure, Bibliothekare, usw.);
- Eltern und Familien;
- Institutionen und Vereinigungen.

3.3 Irland - Cybersafe Kids

(Da es in diesem Land an bewährten Praktiken im Bereich der Berufsbildung mangelt, wurde eine Praxis ausgewählt, die die geforderten Bedingungen erfüllt, aber nicht speziell den Berufsbildungssektor betrifft).

Das Projekt Cybersafe Kids wurde 2015 ins Leben gerufen und hat sich inzwischen zu einer anerkannten Wohltätigkeitsorganisation entwickelt, die von einer Reihe irischer philanthropischer Fonds wie The Ireland Funds finanziert wird. Cybersafe Kids bietet eine Reihe von Schulungsprogrammen zum Thema Cybersicherheit in Schulen in ganz Irland an. Die Vision von Cybersafe Kids ist eine Welt, in der Kinder die Technologie auf sichere, positive und erfolgreiche Weise nutzen. Die Hauptakteure von Cybersafe Kids sind die teilnehmenden Schulen in ganz Irland (Schüler, Lehrer, Schulleiter und Erziehungsberechtigte), die Partneruniversitäten, die Geldgeber der Wohltätigkeitsorganisation und das Team, das an der

Durchführung der Programme beteiligt ist. Das Hauptziel der Wohltätigkeitsorganisation besteht darin, Kinder, Eltern und Lehrer in der Gemeinschaft zu fördern und zu schulen, um einen sicheren und verantwortungsvollen Umgang mit der Online-Welt zu gewährleisten. Was die Wirkung angeht, so hat Cybersafe Kids bisher 24.000 Kinder im Alter von 8 bis 13 Jahren über seine Schulprogramme erreicht. Allein im Jahr 2020 standen die Programme mit 5.986 Kindern und 1.554 Eltern in 56 Schulen in Irland in Kontakt. Zusätzlich wurde eine anonyme Online-Umfrage verteilt, die Daten von 3.764 Kindern im Alter von 8 bis 12 Jahren über ihre Online-Nutzung sammelte. Laut dem Bericht der Direktoren (2019) waren die wichtigsten Wirkungsbereiche die folgenden:

- Die Durchführung eines Bildungsprogramms und der Start eines Projekts zur Messung von Verhaltensänderungen in Zusammenarbeit mit der Universität Dublin und dem Children and Young Persons Committee (CYPSC);
- Durchführung einer starken Kampagne zum 'Tag des sicheren Internets';
- Einführung von Online-Inhalten und -Ressourcen, die sich an Eltern jüngerer Kinder (im Alter von 2 bis 10 Jahren) richten. In den vergangenen Jahren wurde Material für ältere Kinder veröffentlicht;
- Entwicklung einer Reihe politischer 'Fragen', die sich auf die übergreifende Politik des Landes auswirken sollen

zur Cybersicherheit.

3.4 Spanien - SPACE: Fertigkeiten für Schulfachleute gegen Cybermobbing

HINTERGRUND.

Die weite Verbreitung und Nutzung neuer Technologien ist mit dem Phänomen des Cybermobbings verbunden. Im Jahr 2009 wurden europaweit etwa 18% der europäischen Jugendlichen im Alter von 13-19 Jahren über das Internet und Mobiltelefone gemobbt/belästigt/gestalkt, die aktuellen Raten liegen zwischen 10% und 52%. Das Europäische Parlament weist darauf hin, dass Cybermobbing bei Kindern im Alter von 11-16 Jahren von 7% im Jahr 2010 auf 12% im Jahr 2014 gestiegen ist.

BEDÜRFNISSE DER ZIELGRUPPEN.

Das Projekt SPACE ist eine Antwort auf den Fortbildungsbedarf von Lehrern, damit sie Kompetenzen zur Prävention und Bekämpfung von Cybermobbing erwerben. Obwohl die EU-Mitgliedstaaten zahlreiche Initiativen und Projekte zur Vorbeugung und Bekämpfung von Cybermobbing ins Leben gerufen haben, scheint dieses Phänomen zuzunehmen: Da es sich um ein neues Phänomen handelt, fehlt es an einem organischen System von Kenntnissen, Fähigkeiten und strukturierten pädagogischen Maßnahmen, die sicherstellen, dass Lehrer das Wissen über seine Dynamik, die Beherrschung der digitalen Technologien für eine sichere Nutzung des Internets und die Kompetenzen zur Planung von Präventions-, Informations- und Schulungsmaßnahmen erwerben.

ZIELE.

Viele Ressourcen und Inhalte zum Thema Cybermobbing wurden von Schulen und Institutionen entwickelt. Allerdings handelte es sich dabei um isolierte Initiativen, die nicht in einem einzigen Webspace gesammelt und somit nicht aufgewertet wurden. SPACE hat sich dieser Herausforderung gestellt und einen MOOC - einen kostenlosen, offenen Online-Kurs - zum

Thema Cybermobbing für Lehrkräfte entwickelt sowie eine mehrsprachige öffentliche digitale Bibliothek mit offenen Bildungsressourcen zum Thema Cybermobbing. Hauptziele des Projekts:

- die Kompetenzen abzubilden und zu beschreiben, die erforderlich sind, um Cybermobbing zu verhindern und ihm entgegenzutreten;
- eine digitale Bibliothek von OER zum Thema Cybermobbing zu entwickeln, mit erweiterten Suchfunktionen;
- einen MOOC für Lehrer zum Thema Cybermobbing zu entwickeln und dabei die zuvor abgerufenen und gekennzeichneten OER zu verwenden;
- bei den beteiligten Lehrern die digitale Kompetenz zu stärken und zu verbessern, nämlich Cybersicherheit, Internetrisiken und Netzetikette;
- Unterstützung von Lehrern beim Erwerb von Kompetenzen, um im Fall von Cybermobbing in der Schule zu intervenieren und Informations- und Trainingsaktivitäten mit ihren Schülern zu planen und durchzuführen.

TEILNEHMER.

Die Hauptzielgruppe des Projekts sind die Lehrer (ISCED2 und ISCED3). Indirekte Zielgruppen waren Schulleiter und nicht unterrichtendes Personal, Schüler, Eltern, Schulbehörden und Entscheidungsträger. 139 Lehrer waren an der MOOC-Studie beteiligt und 300 nahmen an den in den Partnerländern organisierten Multiplikatorenveranstaltungen teil. Die öffentliche digitale Bibliothek wurde während der Projektlaufzeit über 8.000 Mal besucht.

AKTIVITÄTEN.

Das Projekt dauerte 24 Monate, in denen die folgenden Aktivitäten stattfanden:

- Erstellung einer Karte der Kompetenzen und eines MOOC-Modells;
- Design und Entwicklung einer digitalen Online-Bibliothek zum Thema Cybermobbing;
- Auffinden, Katalogisieren und Identifizieren von OER zum Thema Cybermobbing und Implementierung dieser Ressourcen in der digitalen Bibliothek;

- die Einrichtung und Anpassung einer CMS-Plattform zum Hosten des MOOC;
- Design, Entwicklung und Test eines mehrsprachigen MOOCs zum Thema Cybermobbing;
- Erstellung eines Toolkits mit Hinweisen, Leitlinien und Empfehlungen zum SPACE-System und den Tools;
- Durchführung von 10 Multiplikatorenveranstaltungen in den Partnerländern und einer Abschlusskonferenz;
- Durchführung von 4 Konsortialtreffen;
- Verbreitung durch die Erstellung einer Website, Broschüren, Präsentationen, Teilnahme als eingeladener Reporter an der DIDACTA-Messe in Florenz, Artikel in Zeitschriften und Zeitungen.

IMPACT.

Das Projekt hat sich positiv ausgewirkt, indem es das Bewusstsein für Cybermobbing, das Wissen über dessen Dynamik und Methoden zur Prävention und Bekämpfung sowie die Entwicklung eines multidimensionalen Sets von Wissen und Fähigkeiten in der Gruppe der beteiligten europäischen Lehrer gefördert hat. Die beteiligten Lehrer und Organisationen haben Kompetenzen erworben, um Cybermobbing vorzubeugen und zu bekämpfen, sie haben digitale Fachkompetenzen in Bezug auf Cybersicherheit, Internetrisiken und Netzetikette erworben, sie haben strategische Fähigkeiten und methodisch-didaktische Kompetenzen entwickelt, um ihre Lehrtätigkeit zu verbessern, und sie verfügen über wirksamere Instrumente, um Informations- und Schulungsmaßnahmen für ihre Schüler durchzuführen, um Cybermobbing zu verhindern.

3.5 Lettland - Programm "Verbesserung der digitalen Kompetenz von Lehrern in Form einer E-Umgebung für die Nutzung von Bildungstechnologien"

ZIEL.

Das Ziel des Programms ist es, die digitale Kompetenz von Pädagogen zu verbessern. Es geht darum, Technologien und Werkzeuge zu vermitteln, die Pädagogen helfen, ihre Arbeitsprozesse effizienter zu gestalten. Das Programm wird seit 2014 vom Ministerium für Bildung und Wissenschaft der Republik Lettland durchgeführt.

BENEFICIARIES.

Der Inhalt der Kurse im Jahr 2020 richtet sich an:

- Managementteams von Bildungseinrichtungen;
- Pädagogen von berufsbildenden (VET) und allgemeinbildenden Schulen;
- Grundschullehrer;
- Vorschullehrer;
- Lehrer für verschiedene Fächer (Mathematik, lettische Sprache, Informatik, Ingenieurwesen, Design und Technologie, Physik, Chemie und Biologie).

BESCHREIBUNG.

Im Jahr 2020 hat das Ministerium für Bildung und Wissenschaft die Verbesserung der digitalen Kompetenz von Pädagogen zu einem vorrangigen Ziel der beruflichen Kompetenz erklärt und zusätzliche Mittel bereitgestellt. Das Programm bietet kostenlose Kurse für Pädagogen mit unterschiedlichem Wissensstand, die verschiedene Fächer vertreten (ihr Fachgebiet, siehe Abschnitt Begünstigte). Die Durchführenden der Kurse haben detaillierte Lernaufgaben entwickelt und Gruppenleiter - Berater - hinzugezogen, um ein günstiges Lernregime für Pädagogen zu gewährleisten. Der Inhalt der Kurse wurde in Übereinstimmung mit den Anforderungen der modernen Lernumgebung entwickelt.

ERZIELTE ERGEBNISSE.

4339 Pädagogen haben lange teilgenommen (mit dem Recht, als Informatiklehrer zu arbeiten)

und kurze Kurse zur Entwicklung beruflicher Kompetenzen (2014-2020).

INNOVATION.
Innovativer Ansatz in der Ablauforganisation - jeder Kursteilnehmer kann die
Inhalte in einem Tempo und zu einer Zeit, die für sie günstig sind. Während des Kurses werden Technologien und Tools analysiert, die im Studienprozess eingesetzt werden können, um die Zusammenarbeit zu fördern und die Organisation des Studienprozesses/des Arbeitsprozesses der Dozenten zu vereinfachen.

3.6 Portugal

Trotz einiger Ad-hoc-Initiativen wurden keine Ausbildungsmaßnahmen im Bereich der Cybersicherheit für die berufliche Bildung ermittelt. Auf dem Markt wurden nur einige Hochschulkurse, Postgraduiertenkurse oder Kurse für Unternehmen identifiziert. Daher sollte die Ausbildung im Bereich der Cybersicherheit für die berufliche Bildung eine grundlegende Priorität sein, um die cybersichere Zukunft unseres Landes zu untermauern, d.h. in der Lage zu sein, die persönliche und geschäftliche Sicherheit zu gewährleisten.
Das Nationale Zentrum für Cybersicherheit, das die Aufgabe hat, den Wissensaustausch und eine nationale Kultur der Cybersicherheit zu fördern, hat das Programm zur Sensibilisierung und Schulung in Cybersicherheit entwickelt, mit dem die Schulung und das Bewusstsein der Bürger und der Mitarbeiter von Organisationen für die Gefahren der uninformierten Nutzung des Cyberspace massiert werden soll, indem Aktionen zur Sensibilisierung und Schulung in Cybersicherheit in verschiedenen Teilen des Landes, vom Norden bis zum Süden, über die Inseln, mit der Unterstützung von Partnern durchgeführt werden, die sich jedoch nicht an Berufsbildungseinrichtungen richten.

3.7 Italien - Docenti connessi e sicuri (Vernetzte und sichere Lehrer)

HINTERGRUND.

Das Programm hat das allgemeine Ziel, Maßnahmen zur Innovation und Stärkung der digitalen Kompetenzen in Schulen durchzuführen. Konkret zielt das Programm darauf ab, die Fähigkeiten und Kenntnisse von Lehrern in Bezug auf neue integrierte digitale Unterrichtserfahrungen, die Funktionsweise und den Nutzen des Internets der Dinge und die Bedeutung der Cybersicherheit zu verbessern. Das Programm wird im Rahmen der neuen Absichtserklärung zwischen dem italienischen Bildungsministerium und Cisco gefördert.

ZIELGRUPPEN.

Die Nutznießer des Programms sind Lehrer italienischer Schulen jeder Ordnung und Klasse.

AKTIVITÄTEN.

Das von Cisco angebotene Schulungsprogramm für Lehrer besteht aus 3 Webinaren, mit denen 3 vertiefende Kurse verbunden sind. Die Teilnahme an dem gesamten Programm ist völlig kostenlos.

1. Eine vernetzte digitale Welt Webinar "DAD und neue Erfahrungen mit integriertem digitalem Unterricht", das von Cisco-Mitarbeitern oder Cisco-Partnern gehalten wird, und damit verbundener Online-Kurs "Get Connected". Geschätzte Dauer der Teilnahme: 30 Stunden Kursübersicht: Der Kurs lehrt Sie, grundlegende digitale Kenntnisse zu entwickeln. Die besonders interaktive Kursstruktur schafft eine leicht zugängliche Umgebung für ein Publikum, das sich zum ersten Mal der Welt der IT nähert.
2. Bewusste digitale Bürger: Webinar "Smart City und Internet der Dinge: neue digitale Dienste für Bürger", gehalten von Cisco-Mitarbeitern oder Cisco-Partnern und damit verbundener Online-Kurs "Einführung in das Internet der Dinge (IoT)". Geschätzter

Zeitaufwand: 20 Stunden Kursübersicht: Der Kurs "Einführung in das Internet der Dinge (IoT)" führt Lehrkräfte in die Technologien ein, die das IoT unterstützen, sowie in die Möglichkeiten, die durch die wachsende Zahl von Netzwerkverbindungen zwischen Menschen, Prozessen, Daten und Dingen entstehen.

3. IT-Sicherheit: Webinar "Wie Sie sich vor Netzwerkbedrohungen schützen", gehalten von Cisco-Mitarbeitern oder Cisco-Partnern und verlinkter Online-Kurs "Introduction to Cybersecurity". Geschätzter Zeitaufwand: 20 Stunden. Überblick über den Kurs: Der Kurs "Einführung in die Cybersicherheit" analysiert Trends in der IT-Welt, Bedrohungen und die Tatsache, dass man im Cyberspace absolut sicher sein und seine persönlichen Daten schützen muss.

IMPACT.

Da das Projekt am 3. Juni endete, werden die Zahlen zu den ausgebildeten Lehrern noch ausgearbeitet. Das Projekt ist jedoch innovativ, da es technologiebezogene Schulungen mit digitalem Unternehmertum, aber auch mit Programmierung kombiniert.

Fazit

Die für das Projekt CYBER.EU.VET durchgeführten Recherchen ergaben, dass es an Daten und Informationen über die Kompetenzen und Herausforderungen der Lehrkräfte von Bildungseinrichtungen im Bereich der Cybersicherheit auf europäischer Ebene mangelt und dass es nur eine begrenzte Anzahl von Initiativen gibt, die sich mit Fragen der Cybersicherheit in der Berufsbildung befassen, was darauf hindeutet, dass das Projekt CYBER.EU.VET das aufkommende Thema in allen Mitgliedstaaten behandelt hat.

Dennoch sind diese bestehenden Initiativen umfassend und haben sich als effizient erwiesen (siehe Abschnitt Gute Praktiken). Derzeit konzentrieren sich die meisten Aktivitäten und Projekte auf die Sensibilisierung der Bevölkerung für die Cybersicherheit und die Verbesserung der allgemeinen dig
Laut einer nationalen Umfrage sind mehr als die Hälfte der Lehrer, die sich durch Cybermobbing gefährdet fühlen, der Meinung, dass Schulungen erforderlich sind. Für sie ist die Aus- und Weiterbildung eine Gelegenheit, Erfahrungen auszutauschen und die Methoden der beruflichen Praxis in diesem Bereich zu analysieren. Es wird immer noch geglaubt, dass der Einsatz digitaler Werkzeuge im Unterricht eine Art zu lehren oder ein Objekt ist, das den Schülern beigebracht werden soll, anstatt ein integraler Bestandteil ihrer allgemeinen Kultur zu sein.

Es sollte eine Kultur der Informationsquellen und Praktiken zu digitalen Risiken (Recherche und Überwachung) entwickelt werden. Außerdem muss die Schulung zu den Herausforderungen der digitalen Technologie und insbesondere zu den psychosozialen, ethischen, rechtlichen und technischen Problemen, die bei der Nutzung digitaler Werkzeuge auftreten können und die Lehrer so sehr beunruhigen, dass sie auf die Nutzung verzichten, intensiviert werden.

So kann das Wissen über digitale Risiken die pädagogischen Praktiken zur Vermittlung von digitaler Kompetenz an Schüler positiv beeinflussen. Ein Lehrer mit einer ausgeprägten digitalen Kultur wird eher geneigt sein, die digitale Technologie im Unterricht mit seinen Schülern zu nutzen und die digitale Technologie zu einem Lehr- und Lerngegenstand zu machen.

Der offensichtliche Einfluss der Risikodarstellung lässt sich ohne eine allgemeine und plurale digitale Kultur, die eine Informationskultur im weitesten Sinne ergänzt, nicht positiv verändern, die eine Dämonisierung des technischen Objekts vermeidet und die Nutzung des pädagogischen Potenzials ermöglicht. Es geht nicht darum, in Angst zu erziehen, sondern darum, sich durch eine kritische und aufgeklärte Wahrnehmung der digitalen Welt zu emanzipieren (und auch als Lehrer emanzipiert zu werden).

Referenzen

ADEI (2017), *El trabajo del futuro*. Technical Note.

Agence nationale de la sécurité des systèmes d'information (ssi.gouv.fr)

Andries B. et Beigbeder I. (coordonné par) (1993), *La culture scientifique et technique pour les professeurs des écoles*, Paris: Hachette éducation, CNDP.

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

Baron G.-L. et Bruillard É. (2000), *Technologies de l'information et de la communication dans l'éducation : Quelles compétences pour les enseignants? ,* Éducation et Formation, Nr. 56.

Baron G.-L. et Bruillard É. (sous la direction) (2002), *Les technologies en éducation: perspectives de recherche et questions vives*, Actes du Symposium international francophone, Paris : INRP, IUFM de Basse-Normandie, MSH.

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

Blanco, R., Fontrodona, J., Poveda, C. (2017), *La industria 4.0: el estado de la cuestión,* Revista Economía Industrial, No 406.

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.

Capelle, C., Cordier, A., Lehmans, A., (2018), *Usages numériques en éducation : l'influence de la perception des risques par les enseignants*, Open Edition Journals.

Carrizosa Prieto, E (2018), *Lifelong learning e industria 4.0. Elementos y requisitos para optimizar el aprendizaje en red.*, Revista internacional y comparada de relaciones laborales y derecho del empleo. Vol. 6, No 1.

Central Statistics Office (CSO) (2018), Statistiken zur Informationsgesellschaft - Haushalte: https://www.cso.ie/en/releasesandpublicatons/er/isshh/informationsocietystatisticshouseholds2018/ (Zugriff am 6. Juli 2021).

CEFEDOP, (2021), *Berufliche Aus- und Weiterbildung in Portugal*, EU-Agenda.

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).

Datenbank der nationalen Bildungsangebote - Niid.lv, Studiengänge in Cybersicherheit

Department of Education and Skills, Government of Ireland (2015), *Digital Strategy for Schools (2015-2020)-Enhancing Teaching, Learning and Assessment.*

Department of Education and Skills, Government of Ireland (2017), *Higher Education System Performance Framework 2018-2020.*

Ministerium für Unternehmen, Handel und Beschäftigung (2018), *Future Jobs Ireland - Preparing Now for Tomorrow's Economy.*

Ministerium für Weiterbildung und Hochschulbildung, Forschung, Innovation und Wissenschaft, Regierung von Irland (2021), *Statement of Strategy 2021-2023.*

Justizministerium (2021). Cyberkriminalität: www.justice.ie/en/jelr/pages/cybercrime (Zugriff am 2. Juli 2021).

Ministerium für Tourismus, Kultur, Kunst, Gaeltach, Sport und Medien (2019), *Aktionsplan für Online-Sicherheit 2018 - 2019.*

Dig8tal (2020), *Ist die deutsche Cybersicherheit bereit für 2021?,* https://dig8ital.com/resources/library/is-german-cyber-security-ready-for-2021

Erasmus+ Projekt DIG4VET (Digital Tools for Learning and Validation in VET and WBL: Training Program
für Berufsschullehrer, Ausbilder und potenzielle I-Coaches)

Escuela de organizacion industrial, *Activa industria 4.0.*

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

Europäische Kommission (2020), *Italien im Index für die digitale Wirtschaft und Gesellschaft*.

Europäische Kommission (2020), *Lettland im Index für die digitale Wirtschaft und Gesellschaft*.

Bundesamt für Sicherheit in der Informationstechnik, (2019),*The State of IT Security in Germany in 2019.*

Bundesamt für Sicherheit in der Informationstechnik, (2020), *The State of IT Security in Germany in 2020.*

Bundesamt für Sicherheit in der Informationstechnik, (2020). *Digitalbarometer: Bürgerbefragung zur Cyber-Sicherheit.*

Regierung von Irland (2018), *Nationale Cybersicherheitsstrategie 2019-2024.*

Regierung von Italien (2020), *Piano Nazionale di Ripresa e Resilienza -PNRR.*

Regierung von Lettland, (2019), *Informativer Bericht, Cybersecurity Strategy of Latvia.*

Regierung von Lettland, (2020), *Leitlinien für die Bildungsentwicklung 2021-2027 "Future Skills for the Future Society".*

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

Guir R. (2002), *Pratiquer les TICE : Former les enseignants et les formateurs à de nouveaux usages*, Bruxelles: De Boeck et Larcier.

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.*

Joseph, V. (2020). *Berufliche Aus- und Weiterbildung für die Zukunft der Arbeit: Frankreich*, Cedefop ReferNet thematische Perspektiven Serie.

Kultusministerkonferenz (2016), "*Bildung in der digitalen Welt: Strategie der Kultusministerkonferenz*"

Lardellier P., Moatti, D. (2014), *Les ados pris dans la Toile. Des cyberaddictions aux techno-dépendances*, Paris: Éditions Le Manuscrit, Coll. " Süchte: Plaisir, Passion, Possession "

Lettisches Zentrum für sicheres Internet (Projektplattform "Drossinternets.lv"): https://drossinternets.lv/

LIKTA (Lettischer Verband für Informations- und Kommunikationstechnologien): https://likta.lv/digitalasparmainas-izglitiba/

Likumi.lv, Noteikumi par pedagogiem nepieciešamo izglītību un profesionālo kvalifikāciju un pedagogu profesionālās kompetences pilnveides kārtību. https://likumi.lv/ta/id/301572-noteikumi-par-pedagogiem-nepieciesamo-izglitibu-un-profesionalo-kvalifikaciju-un-pedagogu-profesionalas-kompetences-pilnveides

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

Ministerium für Bildung, Universität und Forschung, Regierung von Italien, *Piano Nazionale Scuola Digitale - PNSD.*

Ministerium für Bildung, Universität und Forschung, Regierung von Italien, (2018), *La Buona Scuola* (Gesetz Nr. 107/2015)

Ministerium für Bildung, Universität und Forschung, Regierung von Italien (2020), *Accordo di collaborazione per lo svolgimento di attività didattiche e formative congiunte per promuovere l'educazione alla cittadinanza digitale e l'utilizzo consapevole delle*

tecnologie digitali e dei social media, Memorandum of Understanding n. 4 vom 28. Oktober 2020.

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 Industrie, Handel und Tourismus, Regierung von Spanien, Industria Conectada 4.0, Agenda Digital para Espana.

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

Mokhtar Ben Henda (2016), *Identification des besoins en formation tic/e dans les pays francophones du sud. Étude réalisée par: Initiatives pour le Développement numérique de l'espace universitaire francophone francophone*, [Rapport de recherche] Agence universitaire de la Francophonie.

National Centre for Vocational Education Research, (2020), *Teaching digital skills: Implications for VET educators - good practice guide.*

OECD (2021), Der digitale Wandel in Lettland

OECD, (2018), TALIS - The OECD Teaching and Learning International Survey TALIS - OECD Teaching and Learning International Survey

Pridzans, Dzerviniks (2019), *The Topicality of Educators' Digital Competence Development*, SOCIETY. INTEGRATION. EDUCATION Proceedings of the International Scientific Conference. Band V, 24. -25. Maith .

Principes et organisation de la deuxième année de la formation des enseignants stagiaires en IUFM, (2002). La circulaire du 4 avril 2002 parue au Bulletin officiel n° 15 du 11 avril 2002.

Saldus Technical School, Studienprogramm Zivile Sicherheit und Verteidigung: https://www.saldustehnikums.lv/izglitibas-iespejas/profesijas/profesionala-videja

Stolterman, E (2004), *Information Technology and the Good Life*, International Federation for Information Processing Digital Library; Information Systems Research. Band 143.

Telekommunikation: *die 5 größten Risiken für die Cybersicherheit* - Sophos News

Thélot C. (sous la direction) (2004), *Pour la réussite de tous les élèves, rapport officiel de la Commission du débat national sur l'avenir de l'École*, Paris : La documentation Française.italen Kompetenzen von Lehrkräften, was durch die rasche Anpassung an den Prozess der Fernarbeit/des Fernlernens beeinflusst wurde.

Das Partnerkonsortium ist vielfältig und ein deutlicher Ausdruck eines unterschiedlichen Ausmaßes an digitalen Kompetenzen in ganz Europa. Unabhängig von der DESI-Einstufung der einzelnen Länder kann dieser Forschungsbericht des Konsortiums jedoch genutzt werden, um aussagekräftige und gültige Hinweise für den gesamten europäischen Kontext zu erhalten.

Selbst unter den Berufsschullehrern, die bereits eine IKT-Schulung absolviert haben, ist der Bedarf an Fortbildung deutlich spürbar. Weder wird die Notwendigkeit einer Fortbildung abgelehnt, noch wird ihr Nutzen in Frage gestellt. Wir stellen außerdem fest, dass Lehrer umso mehr Fortbildungsbedarf haben, je mehr sie sich psychosozialen, ethischen, rechtlichen, technischen oder gesundheitlichen Risiken ausgesetzt sehen.

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: