DICYSTECH

DIGITAL TRAINING FOR CYBERSECURITY STUDENTS IN INDUSTRIAL FIELDS

www.dicystech.eu

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

This project has been funded with support from the European Commission. This communication reflects the views only of the author, and the Commission cannot be held responsible for any use which may be made of the information contained therein. «DICYSTECH - Digital Training for Cybersecurity Students in Industrial Fields» project number: 2020-1-ES01-KA226-HE-095291.

UPDATED CONTEXT OF THE PROJECT: THE INDUSTRY 4.0 CYBERSECURITY REALITIES AND NEEDS

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

DICYSTECH

The European Union Agency for Cybersecurity - ENISA published the 9th edition of the **Threat Landscape 2021 (ETL) report**, an annual report regarding the status of the cybersecurity threat landscape "*that identifies prime threats, major trends observed with respect to threats, threat actors and attack techniques, and also describes relevant mitigation measures*".

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

DICYSTECH

"*Cybersecurity attacks have continued* ***to increase through the years 2020 and 2021****, not only in terms of* ***vectors and numbers*** *but also in terms of their* ***impact***".

"*The* ***COVID-19 pandemic*** *has also –expectedly– had an impact on the cybersecurity threat landscape*".

"*The cybersecurity landscape has grown in terms* ***of sophistication of attacks, their complexity and their impact***".

"*The threat to supply chains and their significance due to their potentially catastrophic cascading effects has reached the highest position among major threats*".

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

DICYSTECH

While in the previous edition….

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

DICYSTECH

This year, ENISA took a step back and **consolidated threat categories in a move towards integration and better representation of similar threats.**

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

DICYSTECH

ENISA also identified the **key trends** observed in the cyber threat landscape during the reporting period such as:

- **Highly sophisticated and impactful supply chain compromises** proliferated, as highlighted by the dedicated ENISA Threat Landscape on Supply Chain. **Managed service providers** are high-value targets for cybercriminals.
- **COVID-19 drove cyber espionage** tasking and created **opportunities for cybercriminals**.
- **Governmental organisations have stepped up their game** at both national and international level. Increased efforts have been observed from governments to disrupt and take legal action against state-sponsored threat actors.
- **Cybercriminals are increasingly motivated by monetisation** of their activities, e.g. ransomware. **Cryptocurrency** remains the most common pay-out method for threat actors.
- Cybercrime attacks **increasingly target and impact critical infrastructure**.
- **Compromise through phishing e-mails, and brute-forcing on Remote Desktop Services (RDP)** remain the two most common **ransomware infection vectors**.
- The focus on **Ransomware as a Service (RaaS) type business models** has increased over 2021, making proper attribution of individual threat actors difficult.
- The occurrence of **triple extortion ransomware** schemes increased strongly over the course of 2021.

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

DICYSTECH

- **The malware decline** that was observed in 2020 continues during 2021. In 2021, we saw an increase in threat actors resorting to relatively new or uncommon programming languages to port their code.
- **Malware targeting container environments** have become much more prevalent, with novel evolutions like file-less malware being executed from memory.
- Malware developers keep finding ways to **make reverse engineering and dynamic analysis harder**.
- The volume of **cryptojacking infections** attained a **record high** in the first quarter of 2021, compared to the last few years. The **financial gain** associated with cryptojacking incentivised the threat actors to carry out these attacks.
- **The volume of Crypto mining in 2021 and cryptojacking activities are at a record high**.
- We can see that a **shift from browser to file-based cryptojacking** is taking place.
- **COVID-19 is still the dominant lure in campaigns** for e-mail attacks.
- **Business E-mail Compromise (BEC)** has **increased**, has grown in **sophistication** and become more **targeted**.
- **The Phishing-as-a-Service (PhaaS)** business model is gaining prevalence.
- Threat actors shifted their attention towards **vaccine information** in the context of threats to data and information.

- There was a **surge in healthcare sector related data breaches**.
- Traditional DDoS (Distributed Denial of Service) attacks are moving towards **mobile networks and IoT (Internet of Things)**.
- **Ransom Denial of Service (RDoS)** is the new frontier of denial of service attacks.
- **Sharing of resources in virtualised environments** acts as an amplifier of DDoS attacks.
- **DDoS campaigns** in 2021 have become more targeted and much more persistent and increasingly multivector.
- **Artificial Intelligence (AI)-enabled disinformation** supports attackers in carrying out their attacks.
- **Phishing is at the heart of disinformation attacks** and strongly exploits people's beliefs.
- **Misinformation and disinformation** are at the core of cybercrime activities and is increasing at an unprecedented rate.
- **Disinformation-as-a-Service (DaaS) business model** has grown significantly, spurred by the increasing impact of the COVID-19 pandemic and the need to have more information.
- In 2020 and 2021, we observed a **spike in non-malicious incidents**, as the COVID-19 pandemic became a multiplier for **human errors** and **system misconfigurations**, up to the point that most of the breaches in 2020 were caused by errors.
- There has been a **spike in cloud security non-malicious incidents**.

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

In February 2022, **ENISA** and **CERT-EU** strongly encouraged all public and private sector organisations in the EU to adopt a minimum set of cybersecurity best practices.

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

DICYSTECH

14 best practices suggested:

1. Ensure remotely accessible services require multi-factor authentication (MFA)
2. Ensure users do not re-use passwords, encourage users to use Multiple Factor Authentication (MFA) whenever supported by an application (on social media for instance)
3. Ensure all software is up-to-date
4. Tightly control third party access to your internal networks and systems
5. Pay special attention to hardening your cloud environments
6. Review your data backup strategy
7. Change all default credentials
8. Employ appropriate network segmentation
9. Conduct regular training
10. Create a resilient email security environment
11. Organise regular cyber awareness events
12. Protect your web assets from denial-of-service attacks
13. Block or severely limit internet access for servers
14. Make sure you have the procedures to reach out and swiftly communicate with your CSIRT

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

DICYSTECH

CYBERSECURITY EDUCATION AND TRAINING: THE CURRENT NEEDS

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

DICYSTECH

ENISA published a report in 2020, that focused on the **status of the cybersecurity education system** and the **inability to attract more students** in studying cybersecurity and to produce graduates with "***the right cybersecurity knowledge and skills***".

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

DICYSTECH

Regarding Higher Education sector, in its new report "**Addressing the EU cybersecurity skills shortage and gap through higher education**" (2021), ENISA proposed **5 recommendations to address the EU cybersecurity skills shortage and gap**:

1. Increase enrolments and eventually graduates in cybersecurity programmes
   - **the diversification of the HEIs curricula in terms of content, levels and language**
2. Support a unified approach across government, industry and HEIs
3. Increase collaborations between Member States
4. Promote analysis of the cybersecurity market needs and trends
5. Support the promotion of CyberHEAD

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

DICYSTECH

Furthermore, in the coming years **Europe will need more than one million skilled jobs in cybersecurity**. Industry is transforming to exponential technologies such as artificial intelligence (AI), advanced robotics and cognitive automation, advanced analytics, and the Internet of Things (IoT). The technologies being implemented all involve the integration of advanced ICT and global digital supply networks (DSNs) connecting an increasing number of plant processes and management systems.

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

DICYSTECH

The Fourth Industrial Revolution is creating a **mismatch between available workers and the skills necessary for open jobs**, especially concerning **cybersecurity**: indeed by 2022, the global cybersecurity workforce shortage will reach upwards of **1.8 million unfilled positions** and the most acute shortage are for highly skilled technical staff.

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

DICYSTECH

"*An area where cybersecurity remains under-developed however is in the skills present in the workforce. [...]* ***there is a lack of skilled and qualified personnel in the labour market to work in cybersecurity roles*** *and who can sufficiently address the range of cyberthreats posed*" (European Union Agency for Cybersecurity – ENISA, 2021).

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

DICYSTECH

One profile highlighted is that of **cybersecurity operator (cyber talent):** technicians specializing in the design, deployment and maintenance of cybersecurity of the whole range of industrial control systems (ICSs).

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

DICYSTECH

EDUCATIONAL INNOVATION PROVIDED BY DICYSTECH PROJECT

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

DICYSTECH

The DICYSTECH project aims to tackle this mismatch **by providing a digital training course and linked cybersecurity virtual labs for high education students and the retraining of ICT technicians in LLL courses**. Indeed, this Erasmus+ KA2 Strategic partnership project will develop an open access training modules and linked cybersecurity virtual laboratories for cybersecurity education that **serve to meet Industry 4.0 needs** and to **provide innovative educational practice in the digital era**, supporting the uptake of innovative digital technologies for teaching and learning in HVET.

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

DICYSTECH

The project is **innovative** in its **integral, digital, open educational approach to updating educational curricula on cybersecurity** for ICT students to close detected skills gaps, supporting both educational and training providers and companies.

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

DICYSTECH

DURING ITS LIFETIME (24 MONTHS IN TOTAL), THE PROJECT CONSORTIUM WILL BE INVOLVED IN THE DEVELOPMENT OF THE FOLLOWING 2 INTELLECTUAL OUTPUTS:

DICYSTECH Digital Training Course for students

DICYSTECH HUB of Cybersecurity Virtual Labs

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

DICYSTECH

An innovative and ready to use **digital training package** for HE/HVET ICT staff with IT students at EQF 5+ in formal education and with adults in upskilling/reskilling training initiatives.

It will include **5 modules** in both technical and transversal competences, available via **an open attractive e-learning platform.**

Each Module will offer l**earning challenges** and **digital tests** to support learning upon completion of the learning activities.

DICYSTECH Digital Training Course for students

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

DICYSTECH

It will offer users remote access to three fully developed partner **cybersecurity virtual laboratories** in which learners can view and experiment with high end enabling IT technology and cybersecurity measures in simulated industrial contexts.
Users will be invited to register and use them remotely **for practice and the development of learning challenges provided in the training modules**.
It will be **highly innovative** in its collaborative focus and will use of modern digital pedagogy/technology to improve access to hands on cybersecurity equipment.

DICYSTECH HUB of Cybersecurity Virtual Labs

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

DICYSTECH

TARGET GROUP

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

DICYSTECH

The project and its activities are addressed directly to **HE/HVET ICT staff** and **students** as well as **Industrial stakeholders (SMEs)** and **workers (CVET/LL learners)**, but thanks to its aims **all educational, industrial and other sectoral stakeholders with an interest in the training and certification of cybersecurity technicians** will benefit from it.

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

DICYSTECH

PARTNERS

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

DICYSTECH

The Coordinator

POLITEKNIKA IKASTEGIA TXORIERRI S.COOP.

The other partners

P.PORTO

idec

HELLENIC MEDITERRANEAN UNIVERSITY

dlearn EUROPEAN DIGITAL LEARNING NETWORK

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

DICYSTECH

DICYSTECH

CONTACT US

Coordinator: Anabel Menica TXORRIERI
amenica@txorierri.net

www.dicystech.eu

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

This project has been funded with support from the European Commission. This communication reflects the views only of the author, and the Commission cannot be held responsible for any use which may be made of the information contained therein. «DICYSTECH - Digital Training for Cybersecurity Students in Industrial Fields» project number: 2020-1-ES01-KA226-HE-095291.