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

YBER.VET.EU

VERBESSERUNG DER CYBERSECURITY-BEREITSCHAFT DES EUROPÄISCHEN BERUFSBILDUNGSSEKTORS

LEHR- UND ANSCHAUUNGS MATERIALIEN

SCHULUNGS- UND LEHRMATERIAL FÜR DEN BERUFSBILDUNGSSEKTOR ZUM THEMA CYBERSICHERHEIT

NGO NEST Berlin
AEII
tandemplus network
Latvian European Community Studies Association
COFAC
EOS
inerciadigital
meath partnership

EINFÜHRUNG IN DIE MATERIALIEN

GAME JAMS

INTRO

Vom Herbst 2021, im Zusammenhang mit dem Europäischen Monat der Cybersicherheit, bis zum Frühjahr 2022 organisierten die Partner des CYBER.VET.EU Projekts mehrere GameJams in den Ländern der Partner. Junge Menschen waren daran beteiligt, um ihnen die Möglichkeit zu geben, sich mit Themen der Cybersicherheit auseinanderzusetzen und neue Werkzeuge zu erlernen.

Das Hauptziel bestand darin, das Bewusstsein für die Cybersicherheit zu schärfen. Wir wendeten uns dem Prozess der "Gamification" zu, um eine Lösung zu erhalten, die einfach zu übernehmen, schnell zu implementieren, mit der Zeit skalierbar und integrativ ist. Der Prozess der "Gamification", definiert als "die Anwendung von Spielmechanismen in nicht spielerischen Kontexten mit dem Ziel, das Engagement zu fördern und die Motivation zu steigern", ist eine bewährte Methode, um die BenutzerInnen bei Lernaktivitäten zu halten, mit großartigen Ergebnissen auch über kurze Zeiträume hinweg, dank der Nutzung von Unterhaltung, die die TeilnehmerInnen motiviert, sich mehr mit dem Material zu beschäftigen und zu üben. Diese Ausgabe ist eine Kombination aus Leitfaden, Schulung und Übung und lässt sich leicht aktualisieren, wenn neues Material hinzugefügt werden soll.

ERGEBNISSE VON AKTIVITÄTEN / GAME JAMS

- Erhöhtes Bewusstsein für digitale Sicherheit
- Stärkung des Bewusstseins für digitale Sicherheit im Umfeld der Teilnehmer (Familie, Freunde, Kollegen)
- Verringerung der Malware-Erfolgsrate innerhalb der Institutionen
- Verringerung der Datenlecks
- Erhöhtes Interesse für den Cybersicherheitssektor als Beschäftigungsmöglichkeit

AEII / INERCIA DIGITAL [ES]

AKTIVITÄTEN

Die wichtigsten Aktivitäten, die von den spanischen Partnern AEII und Inercia Digital durchgeführt wurden, waren: Hackathon
GameJams
Info-Tage
Internationale Konferenz
Verbreitungsveranstaltung

ERGEBNISSE

Die GameJam-Sitzungen in Spanien lieferten einige nützliche Ergebnisse, die hier eingesehen werden können:
https://scratch.mit.edu/projects/611211889/
https://scratch.mit.edu/projects/611201682/
https://www. youtube. com/watch? v=3QFI9iB0iJU& t=124s

ON SCRATCH

https://scratch.mit.edu/projects/611211889/
Cybersecurity - Under Attack

https://scratch.mit.edu/projects/610354561/
Spanisch

https://scratch.mit.edu/projects/611201682/
https://scratch.mit.edu/projects/714361293/
Spanisch
https://scratch.mit.edu/projects/714362963/
Spanisch
https://scratch.mit.edu/projects/714362911/
on phishing - a remix
https://scratch.mit.edu/projects/606933322
on phishing - Englisch

AEII / INERCIA DIGITAL [ES]

GAME JAM

Gamejam in Cyber.EU.VET

20 visualizaciones Fecha de estreno: 3 dic 2021 The main objective of CYBER.EU.VET is to strengthen the European VET capacity to recognize and manage cybersecurity threats (e.g. ...más

0 No me gusta Compartir Descargar Guardar ...

Gamejam in Cyber.EU.VET

20 visualizaciones Fecha de estreno: 3 dic 2021 The main objective of CYBER.EU.VET is to strengthen the European VET capacity to recognize and manage cybersecurity threats (e.g. ...más

0 No me gusta Compartir Descargar Guardar ...

Gamejam in Cyber.EU.VET

20 visualizaciones Fecha de estreno: 3 dic 2021 The main objective of CYBER.EU.VET is to strengthen the European VET capacity to recognize and manage cybersecurity threats (e.g. ...más

0 No me gusta Compartir Descargar Guardar ...

AEII / INERCIA DIGITAL [ES]

Hackathon

Die spanischen Partner AEII und Inercia Digital nahmen vom 20. bis 22. Oktober 2021 an einem Online-Hackathon mit 47 Teilnehmern teil, darunter viele IT-Experten. https://www.comprometidosporelfuturo.com/proyectos# unterstützt von Boehringer Ingelheim in Spanien.

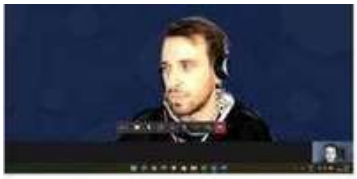
ZU LÖSENDES PROBLEM

Cybermobbing ist eine der größten Internetgefahren für junge Menschen. Häufig finden sich Beiträge mit beleidigendem Inhalt, die dazu benutzt werden, die Opfer zu belästigen und zu verhöhnen.
Cybermobbing verursacht bei den Opfern häufig schwere Störungen wie posttraumatische Belastungsstörungen, Depressionen, Selbstmordgedanken und -verhalten oder Angstzustände.

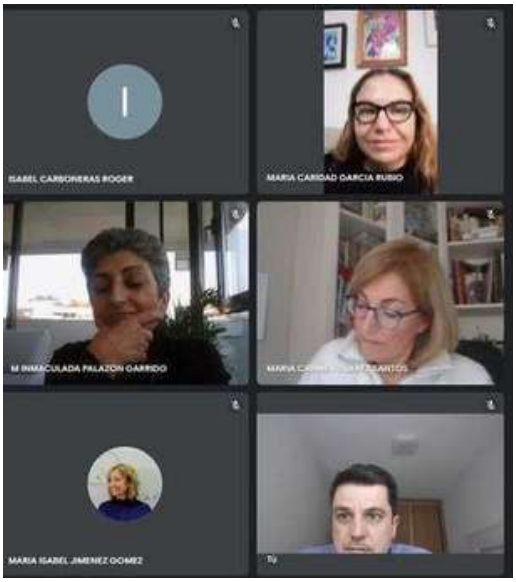
Die Aufgabe hier war, zu untersuchen und zu analysieren, was junge Menschen über Sicherheit wissen, und sie anschließend für die Risiken zu sensibilisieren, denen sie in ihren Bildungseinrichtungen und im täglichen Leben ausgesetzt sind.
Ziel war es, mittels 'Gamification' das Bewusstsein von Schülern und Lehrern für Fragen der Sicherheit bei der Nutzung der neuen Technologien im Alltag zu schärfen.

ERGEBNISSE

- Spiel und Animation im Zusammenhang mit Cybersicherheit in der Bildung
- Einbeziehung von öffentlichen Verwaltungen, berufsbildenden Schulen, IT-Experten, Lehrern, Schülern und Projektpartnern
- Erstellung von kurzen interaktiven Videos



AEII / INERCIA DIGITAL [ES]



Zahlreiche Umfragen haben gezeigt, dass das Wissen über Cybersicherheit bei Lehrern und Schülern in den Berufsbildungszentren in Spanien im Allgemeinen immer noch gering ist. Aus diesem Grund sind dieses Projekt und andere ähnliche Projekte in Spanien sehr wichtig.

NGO NEST BERLIN [DE], EOS [IT] + IASIS [GR]

GAME JAM

NGO Nest Berlin, Extrafondente Open Source - EOS und IASIS haben im Februar 2022 gemeinsam eine GameJam Session durchgeführt. Der GameJam begann am Samstag, den 12. Februar, und dauerte insgesamt 6 Tage. Die nationalen Teams entwickelten und arbeiteten gemeinsam an einem Spielentwurf (für ein Online- oder Brettspiel).

Eine unabhängige Jury wurde einberufen und gebeten, den Spielentwurf nach gemeinsamen Leitlinien und einer Bewertungsvorlage zu bewerten.

Das Siegerteam erhielt ein sechsmonatiges Mentoring sowie technische Ressourcen, um die Spielidee weiterzuentwickeln.

ÜBER DAS SPIEL

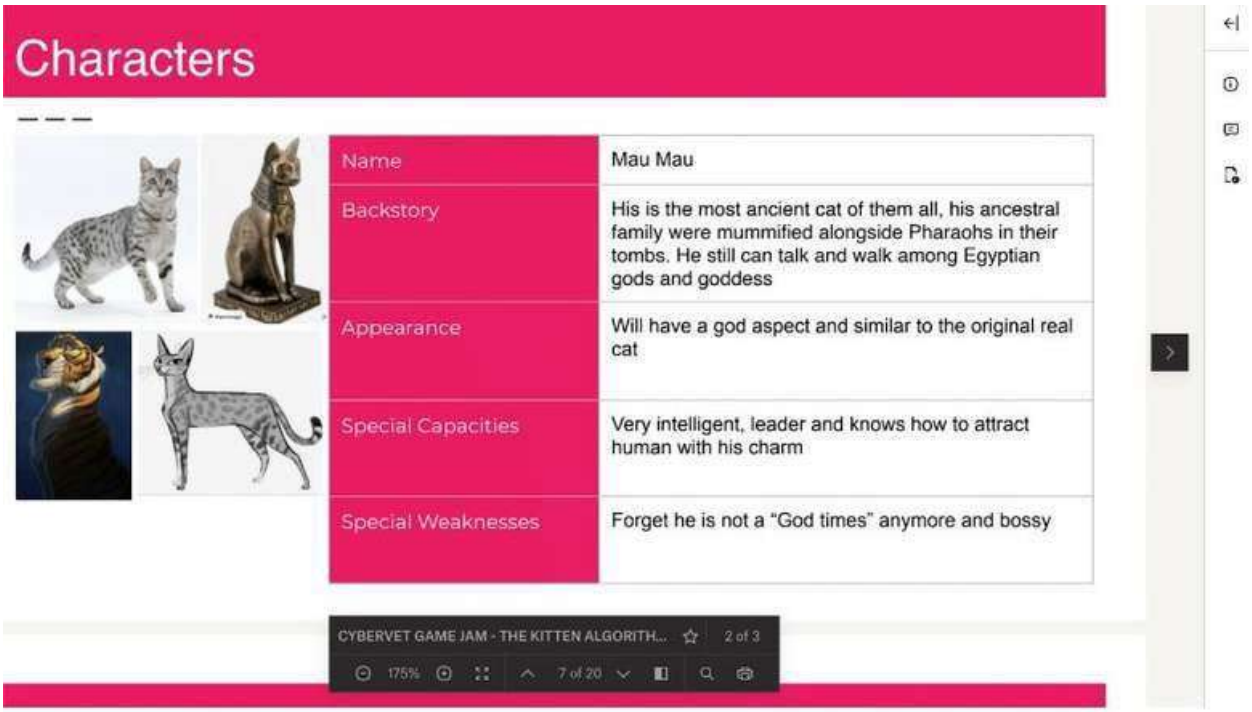
Es handelt sich um ein strategisches Brettspiel für 2 bis 6 Spieler, das etwa 30 bis 60 Minuten Spielzeit benötigt. In diesem Spiel trickst du die Menschen aus, um sie davon zu überzeugen, dass du die beste Katze bist und mehr Prestige bekommst, indem du so viele menschliche Katzendiener wie möglich bekommst. Halte die Augen offen, denn die anderen Boss-Katzen werden aktiv versuchen, deinen Weg zu den Menschen zu sabotieren und den Ruhm für sich selbst zu erobern. Traue ihren niedlichen Gesichtern nicht!

Du verlierst das Spiel, wenn du nicht eine hohe Anzahl von Menschen als Diener hast oder die 10. Runde vorbei ist und keiner der Spieler mindestens 4 Menschen unter seinem Kommando hat.

Die Schwierigkeit besteht darin, dass es 6 Bosse gibt, die versuchen, die Menschen auszutricksen, damit sie ihre Diener werden und die Bosse sie kontrollieren können, aber alle haben das gleiche Ziel und einige könnten den Menschen sogar helfen, sich von der Kontrolle der Katzen zu befreien.

NGO NEST BERLIN [DE], EOS [IT] + IASIS [GR]

Mau Mau



LECSA (LV)

GAME JAM

Der lettische Partner LECSA organisierte vom 27. September bis 1. Oktober 2021 eine GameJam-Session. Aufgrund der pandemischen Einschränkungen und der unterschiedlichen Standorte der Teilnehmer wurde die Veranstaltung als Hybridveranstaltung organisiert (vor Ort in der Technischen Schule Saldus und über die Plattform Zoom). Während der Veranstaltung wurden 6 Teams (4-5 Personen pro Team) gebildet, die an der Entwicklung von Spielprototypen arbeiteten. Um greifbare Ergebnisse zu erzielen, sah das Game Jam-Konzept die Entwicklung von zwei Arten von Spielen vor - Computer- und Brettspiele.

AKTIVITÄTEN

August - September 2021 war der Planung und Organisation der Veranstaltung gewidmet (Suche nach Experten für Cybersicherheit und Spielentwicklung, Informationsverteilung an potenzielle Teilnehmer, Planung der Tagesordnung und Festlegung von Kriterien für das Spiel, usw.)

Multiplikator-Veranstaltung - Aktuelles zu Cyberangriffen (27.09.2021): Vorstellung des CYBER.EU.VET-Projekts und Vortrag über die Trends bei Cyberangriffen mit Herrn Armins Palms, Cybersecurity-Experte von CERT.LV (IT Security Incident Response Institution of the Republic of Latvia)
Anzahl der Teilnehmer: 26 Personen
Ort: Technische Schule Saldus (Stadt Saldus) und ZOOM-Plattform

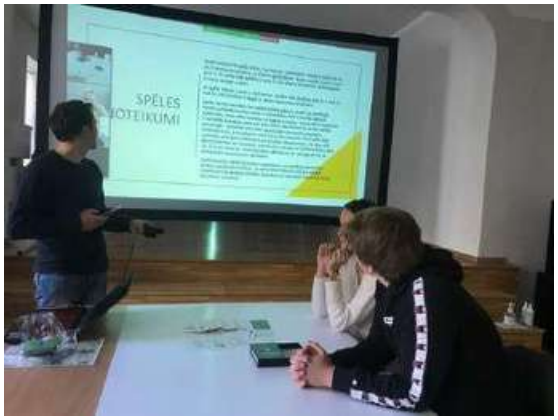
Ankündigung des Game Jame (27.09.2021): Definition und Diskussion über die aktuellen Herausforderungen im Bereich der Cybersicherheit (Bedarfsanalyse); Bildung von Teams, Treffen mit Mentoren und Diskussion über die weitere Arbeit (Workshop zur Spiele-Engine Unity), Brainstorming zur Spielidee und zum Konzept. Game Jam-Aktivitäten im Gange (28.09-30.09.2021): Teams arbeiteten an der Entwicklung von Prototypen, bei Bedarf wurde Rücksprache mit Mentoren gehalten.
Pitching über den Fortschritt (30.09.2021): Pitching über die Konzepte des Spiels und den Arbeitsfortschritt, um Anregungen der Mentoren zu erhalten.

Großes Finale (01.10.2021): Vier Teams haben ihre Ergebnisse präsentiert und die Mentoren haben eine Bewertung abgegeben. Ein Team, das ein Computerspiel entwickelt hat, ist ausgeschieden. Abschluss der Veranstaltung und informelle Diskussion.
Anzahl der Teilnehmer: 30
Ort: Technische Schule Saldus und ZOOM-Plattform

LECSA (LV)

ERGEBNISSE

1. Prototyp des Online-Spiels - The Virus
2. Brettspiel - Karten über Sicherheit
3. Brettspiel - Cyberwar
4. Kartenspiel - Cyber Mind



BEISPIEL Cyber Mind - ein Kartenspiel für 2 oder 4 Spieler

Cyber Mind ist ein pädagogisches Kartenspiel mit Quiz-Elementen. Die Hauptaufgabe des Spiels besteht darin, die Grundlagen der alltäglichen Sicherheit im Internet zu vermitteln und aufzuzeigen, was man sich durch unbedachte Handlungen im Internet antut. Es behandelt Themen wie Internetsicherheit und Datenschutz im Zusammenhang mit der Nutzung sozialer Netzwerke. Im Ergebnis des Spiels sollen die Menschen (Spieler) in der Lage sein, Betrugsversuche im realen Leben zu erkennen.

Entwickelt vom Team Veiksminieki (aus dem Lettischen: Erfolgreiche Menschen), Studenten der Technischen Schule Saldus während des Game Jam in Lettland (Oktober 2021): Renars Ricards Hartmanis, Estere Ozoliņa, Sindija Diāna Valtere & andere.

Niveau: grundlegend (für Anfänger). Zielgruppe: Schüler, Studenten, Lehrer und Eltern

Das Spiel enthält: 50 Karten, 2 Gesundheitspads (zum Zählen der Gesundheit der Spieler), 2 Würfel und Regelkarte.

LECSA (LV)

GAME JAM

ÜBER

Die Versuche von Cyberangriffen in der Welt nehmen täglich zu. Deshalb hat die Weltregierung die Idee, ein Turnier zu veranstalten, um Personen zu identifizieren, die Cyberrisiken mit sich bringen, und ihnen entgegenzuwirken.

Lernspiel, das dabei hilft, die wichtigsten Arten von Cyberangriffen, Vorbeugungs- und Beseitigungsmethoden kennenzulernen, indem man sich selbst oder sein Team schützt und einen Gegenangriff auf den Gegner startet. Ziel des Spiels ist es, dem/den Gegner/n das Leben zu nehmen.

WIE MAN SPIELT - SPIELE + REGELN

Anzahl der Spieler: 2 oder 4 Personen (1 gegen 1 oder 2 gegen 2).

Jeder Spieler oder jedes Team (bei 2 gegen 2) hat zu Beginn des Spiels "100 Leben" (Health=HP). Das Zählen der Lebenspunkte erfolgt mit Hilfe von schwarzen Notizblöcken oder anderen verfügbaren Notizen.

Beauftragen Sie, wenn möglich, eine separate Person, die den Verbrauch von Energie und Gesundheit der Spieler verfolgt und berechnet. Andernfalls müssen die Spieler dies selbst tun.

Jeder Spieler erhält 5 Karten. Wenn das Spiel 2 gegen 2 gespielt wird, haben beide Spieler "eine gemeinsame Hand" im Team oder 10 Karten zusammen.

Es gibt drei Arten von Karten: Angriffskarten (rot), Schildkarten (gelb) und Lebens- oder Heilungskarten (grün).

Das Spiel wird in Runden gespielt. Der Spieler/das Team, der/das die höchste Zahl würfelt, beginnt das Spiel.

Jede Karte kostet Energie. Zu Beginn jeder Runde würfelt der Spieler mit 2 Würfeln, um eine Energie zu bestimmen, die oben auf der Karte (in blau) angegeben ist. Die Karten müssen gespielt werden, damit die gewürfelte Energiemenge nicht überschritten wird. Der Spieler/das Team, der/das die Runde anführt, kann angreifen (mit Angriffskarten), sich schützen (Schildkarten) oder Leben hinzufügen (Heilungskarten), während Zweitplatzierte nur Angriffs- und Schildkarten verwenden können, um ihre Lebensschwäche zu minimieren.

Beachten Sie, dass die maximale Anzahl von Leben pro Spieler/Team während des Spiels 100 HP betragen kann (z.B. wenn die Summe von Leben und Energie nach der Runde insgesamt 110 HP ergibt, bleibt Ihre Anzahl von Leben trotzdem - 100 HP). Das Spiel endet, sobald ein Spieler/Team keine Leben mehr hat (0 Leben). Wenn das Spiel keine Karten mehr hat, müssen Sie die Karten vom Stapel neu mischen.

LECSA (LV)

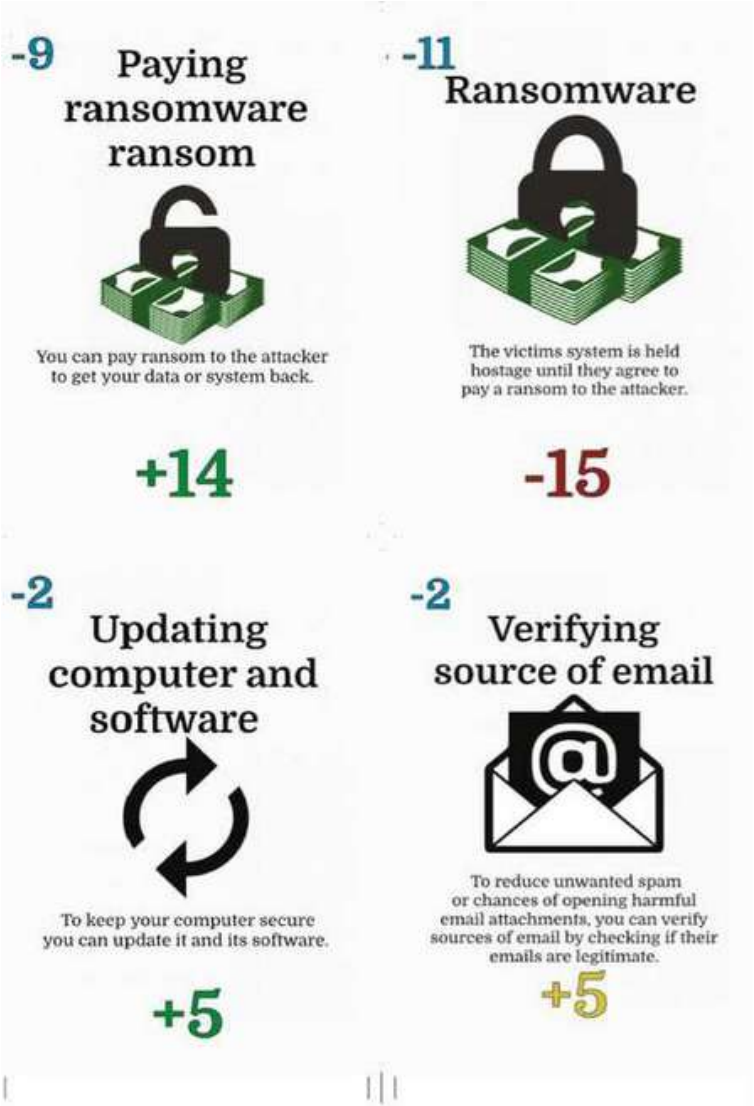
Beispiele für Karten

In **Blau** - Energie

In **Rot** - Angriffskarten

In **gelb** - Schildkarten

In **grün** - Heilkarten



Beispiel für die Berechnung der HP (Health Points)

BEISPIEL Cyberwar - ein Brettspiel

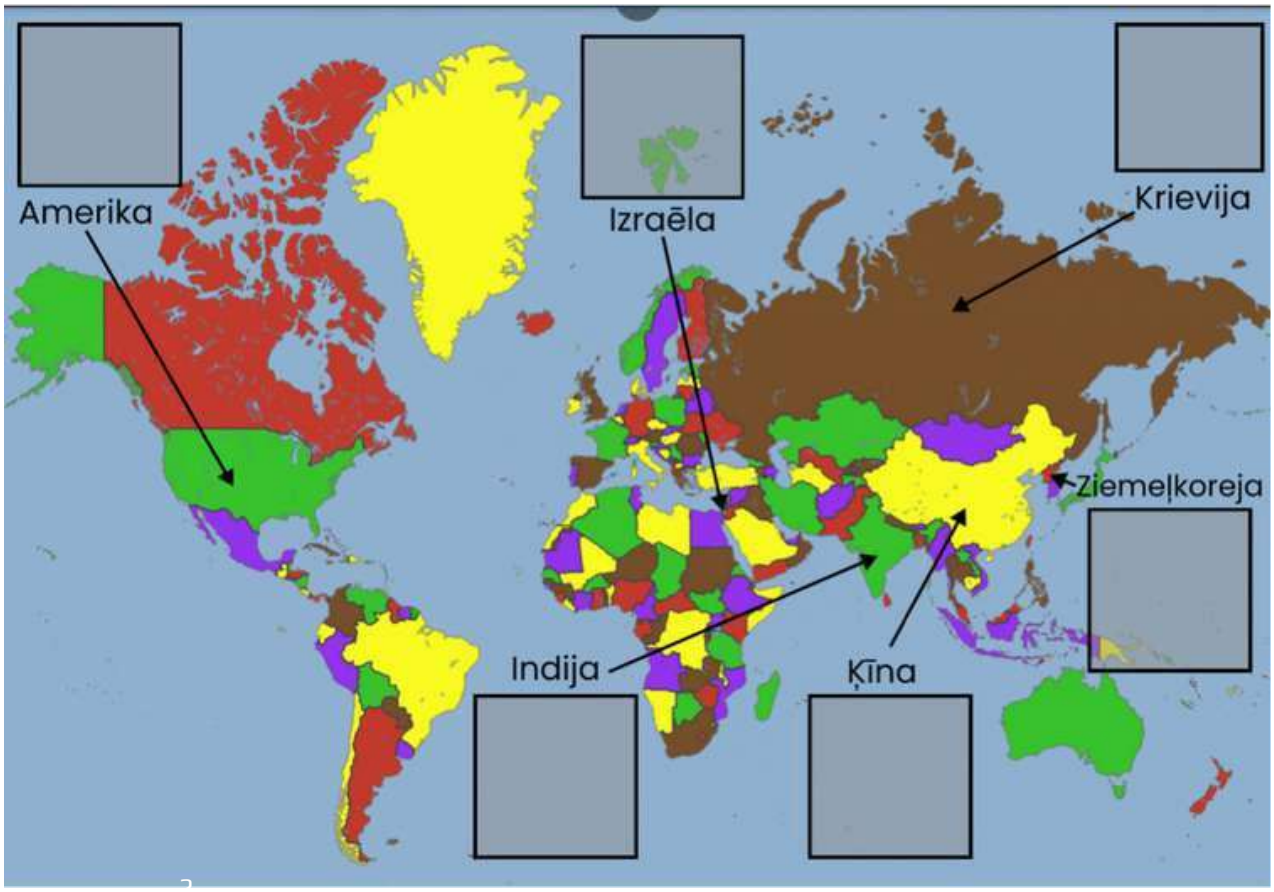
Entwickelt vom Team Exodus (Studenten der Technischen Schule Saldus)
Leiter des Teams: Valdemārs Šperbergs.

2-6 Spieler < - > Geeignet für Personen ab 15 Jahren
Ein Brettspiel mit starker Betonung auf Taktik und Zufall (Chance).

Niveau: Lernspiel für jene, die schon etwas über Cybersicherheit wissen.
Das **Spiel enthält:** Weltkarte, 2 Würfel, Server, Karten mit den Funktionen "Angriff", "Verteidigung" oder "Reaktion", Legende der Schwachstellen.

ÜBER DAS SPIEL

Das Ziel des Spiels ist es, das vom Spieler vertretene Land zu schützen und andere Länder anzugreifen, um den Cyberwar zu gewinnen. In Cyberwar muss jeder Spieler ein Land wählen, das er vertritt. Jeder Spieler hat einen Server mit 3 Sicherheitslücken. Das Ziel des Spielers ist es, die Server anderer Länder zu hacken, indem er zwei von drei Schwachstellen ausnutzt, oder zwei von drei Schwachstellen auf seinem eigenen Server zu beheben.



LECSA (LV)

WIE GESPIELT WIRD

Die Spieler wählen das Land aus, das sie vertreten wollen, und platzieren ein Serverobjekt an einem bestimmten Ort auf der Karte. Jedes Land hat seine eigenen Boni.

Jeder Spieler zieht (nimmt) zufällig 3 Schwachstellen - eine aus jeder Schwierigkeitsstufe - und legt sie verdeckt an die entsprechenden Stellen auf seinen Serverfeldern. Die Schwachstellen sind den Spielern nicht bekannt.

Schwachstellen haben 3 Schwierigkeitsgrade. Der Schwierigkeitsgrad bestimmt auch, wie viele Angriffe erforderlich sind, um eine Schwachstelle auszunutzen (siehe "Angriffe"), und wie viele Züge es braucht, um die Schwachstelle zu beheben (siehe "Verteidigung").

Das Spiel findet in Runden statt, in denen folgende Aktionen (Züge) ausgeführt werden können - **Scannen**, **Angriff** und **Verteidigung**. Die Spieler bestimmen die Reihenfolge der Spieler, indem sie zwei Würfel werfen.

START

Jeder Spieler erhält zu Beginn jeder Runde 4 Karten. Am Ende der Runde ist es möglich, 2 Karten zu behalten oder sie gegen vorhandene auszutauschen.

Die 1. Runde ist eine Scanning-Runde, in der keine Angriffs- oder Verteidigungskarten erlaubt sind. In den folgenden Runden können die Spieler wählen, ob sie scannen oder angreifen oder versuchen, ihre Schwachstellen zu reparieren (siehe Verteidigung). Das Spiel wird Runde für Runde fortgesetzt, bis eine Siegbedingung erreicht ist.

Scannen

Der Angreifer wählt ein Land aus, das er auf seine Verwundbarkeit hin überprüft (z. B. "Ich überprüfe eine russische Verwundbarkeit der Stufe 2"). Der Spieler führt ein Scanning durch - würfelt mit zwei Würfeln und wendet die Boni seines Landes an, vergleicht mit dem Schwierigkeitsgrad der Verwundbarkeit + Boni des Landes des Opfers.

Wenn der Angreifer eine Zahl gewürfelt hat, die dem Schwierigkeitsgrad der Schwachstelle des Opfers entspricht oder darüber liegt, kann der Angreifer die gescannte Schwachstelle betrachten. Länderboni werden nicht hinzugefügt, wenn Sie selbst scannen.

Schwierigkeitsgrade

1. - Spieler muss mindestens die Zahl 4 würfeln (ohne Länderbonus)
2. - Spieler muss mindestens die Zahl 8 würfeln (ohne Länderbonus)
3. - Der Spieler muss mindestens 11 würfeln (ohne Länderbonus).

ANGRIFF

Der Spieler nennt das Ziel des Angriffs (z.B. "Ich greife eine russische Schwachstelle der Stufe 2 an") und deckt die Angriffskarte für alle Spieler auf und legt sie neben die Schwachstelle.

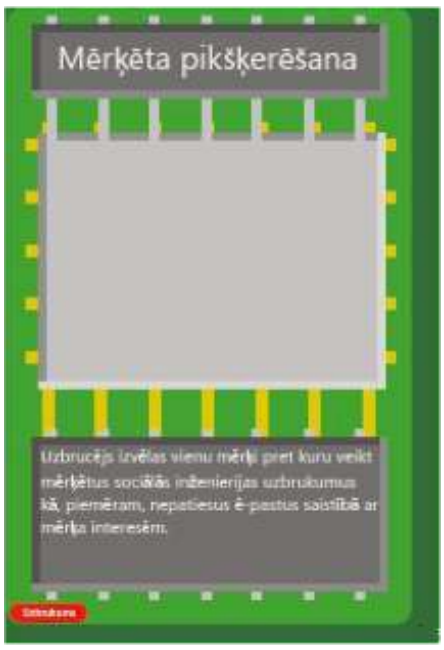
Der Spieler würfelt, um zu sehen, ob der Angriff funktioniert, indem er den Wurf mit der Verwundbarkeitsschwierigkeit + Boni vergleicht (wenn die gewürfelte Zahl + Boni mit der Schwierigkeit übereinstimmt oder diese übersteigt, ist der Angriff erfolgreich).

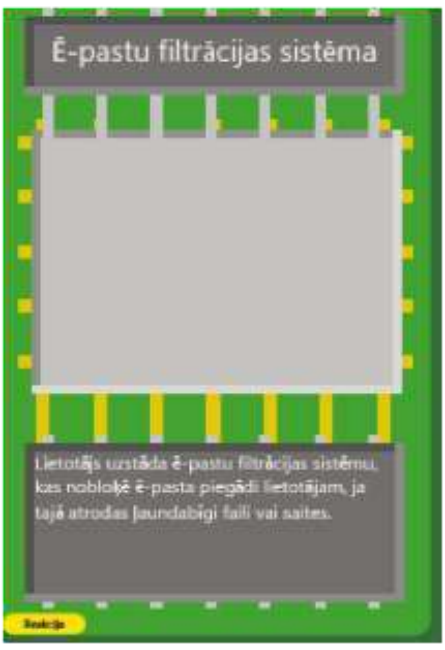
Angriffe können mit der Reaktionskarte, die für den jeweiligen Angriff vorgesehen ist, zurückgedrängt werden. Jeder Angriff hat seine eigene Art von Reaktion, die gespielt werden kann, und seine eigene Art von Verwundbarkeit, für die sie funktioniert.

Wenn der Angriff fehlschlägt oder durch eine Reaktionskarte blockiert wird, bleiben die ausgespielten Angriffs- und Reaktionskarten bis zum Ende der nächsten Runde auf dem Tisch liegen und verhindern, dass andere Spieler mit demselben Angriff für dieselbe Schwachstelle angreifen können. Nach dem Zug kommen beide Karten zurück auf den Stapel.

Schwierigkeitsgrade

1. - Spieler muss mindestens die Zahl 4 würfeln (ohne Länderbonus)
2. - Spieler muss mindestens die Zahl 8 würfeln (ohne Länderbonus)
3. - Spieler muss mindestens 11 würfeln (ohne Länderbonus)





LECSA (LV)

VERTEIDIGUNG

Verteidigung - die Wahl der richtigen Methode gegen eine bestimmte Schwachstelle. Reaktionskarten stoppen (annullieren) den eingehenden Angriff (und alle anderen Angriffe, die auf dieselbe Schwachstelle abzielen) für 1 Runde.

Um einen eingehenden Angriff abzubrechen, legt der Spieler eine Reaktionskarte, die dem Angriffstyp entspricht (siehe Tabelle mit den Verwundbarkeiten), auf die Angriffskarte, sobald der Angriff gespielt wird.

Um eine Verletzung zu reparieren, legt der Spieler eine Verteidigungskarte neben die zu reparierende Verletzung.

Andere Spieler können diese Verletzung angreifen, solange sie sich in Verteidigung befindet (bevor der Verteidigungszug zu Ende ist). Wenn der Spieler versucht, eine Verletzung auf seinem Server mit einer Défense-Karte zu reparieren, kann sie nicht angreifen, aber er kann versuchen, Angriffe mit Reaktionskarten zu verhindern. Für eine vollständige Reparatur wird |Schwierigkeitsgrad + 1| Runde benötigt. Während der Reparaturphase ist die Aktion Scannen erlaubt.

Wenn die Verteidigungsmethode nicht korrekt ist, überspringt der Spieler 3 Runden und kann in dieser Zeit keine Verteidigungskarten einsetzen (Reaktionen und Abtastaktionen sind erlaubt).

Bonus-Punkte der Länder

USA: +2 beim Scannen

Russland: +2 für Angriffe

China: +2 zur Abwehr von Angriffen

Nordkorea: +2 für Verteidigung gegen Scanning

Indien: +1 bei allen Angriffen, -1 gegen Angriffe

Israel: +3 bei allen Angriffen, -3 gegen Angriffe

Schwachstellen nach Ebenen

Vulnerability	Attacks	Défense	Reaction
1st vulnerability level			
SSH server with username	Password guessing	Usage of the public key	Settings of Blocked Period
Administration Panel with User Name	Password guessing	Blocking external requests	Settings of Blocked Period
Untrained employee	Phishing campaigns	IT security trainings	Filtration system of e-mails; Implementation of e-mail SPAM list
Vulnerable SMB protocol	Exploitation of EternalBlue	Fixing vulnerability CVE-2017-0144	n/a
XSS vulnerability	Code injection;	Introductory	Introduction of the

SQL injection	Code injection; Code injection using Polyglot	Introductory synthesis	Introduction of the symbol blacklist
Router panel with default username and password	Using default data	Complete replacement of authentication data	One session limit
2nd vulnerability level			
SSH server	Password guessing	Usage of the public key	Settings of Blocked Period
Administration Panel	Username guessing	Blocking external requests	Settings of Blocked Period
XSS vulnerability with filter	Code injection using Polyglot	Introductory synthesis	Introduction of the symbol blacklist
SQL injection with filter	Code injection using Polyglot	Introductory synthesis	Introduction of the symbol blacklist
Incompletely configured firewall	Packet fragmentation	Repair configuration	IDS implementation
WiFi network with WEP security	Packet Phishing	Using the WPA2 standard	RADIUS implementation
Busy CEO/boss	Phishing – catching the big fish	IT security trainings	Filtration system of e-mails; implementation of e-mail SPAM list
3rd vulnerability level			
Service failure	DDoS	IP address blocking and load limiting	Load balancers
Vulnerable OpenSSL program	Heartbleed exploitation	Repair of CVE-2014-0160	n/a
Vulnerable Print Spooler program	PrintNightmare exploitation	Repair of CVE-2021-36958	n/a
Buffer overflow vulnerability	Buffer overflow	Introduction of buffer limits	Increasing the buffer
Weak hashing algorithm	Decryption of the hash value	Improving the hash algorithm	Usage of a strong and long password
Lazy IT expert	Targeted phishing	IT security trainings	Filtration system of e-mails; implementation of e-mail SPAM list

LECSA (LV)

SSH serveris

SSH serveris ar lietotājvārdu

Administrācijas panelis

Administrācijas panelis ar lietotājvārdu

Neapmācīts darbinieks

Ievainojams SMB protokols

XSS ievainojums

SQL injekcija

Rūtera panelis ar noklusējuma lietotājvārdu un paroli

XSS ievainojums ar filtru

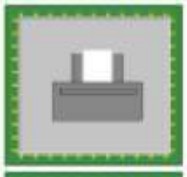
SQL injekcija ar filtru

Nepilnīgi nokonfigurēts ugunsmūris

WiFi tīkls ar WEP drošību

Pakalpojuma atteices kļūda

Ievainojama OpenSSL programma

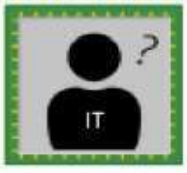


Ievainojama Print Spooler programma

Bufera pārpildes ievainojums

Vājš jaucējvērtības algoritms

Aizņemts priekšnieks



Slinks IT speciālists

LECSA (LV)

GAME JAM

LECSA (LV)

TIPPS & ERFAHRUNGEN VOM GAMEJAM IN LETTLAND

Während der 2-tägigen Veranstaltung kann kein echtes Computerspiel entwickelt werden, sondern nur ein erster Prototyp, der je nach Motivation der Teilnehmer weiterentwickelt werden kann oder nicht.
Preise oder andere Arten von Vorteilen können dazu beitragen, mehr Teilnehmer einzubeziehen und am Ende bessere (greifbarere) Ergebnisse zu erzielen (in unserem Fall wurden Pizza und Getränke am Ende der Veranstaltung bereitgestellt, weitere Unterstützung durch Mentoren (z. B. Platzierung von Spielen auf der Plattform).
Mentoren, die sich mit der Entwicklung von Spielen und mit Fragen der Cybersicherheit befassen, spielen eine wichtige Rolle beim Game Jam, indem sie die Teilnehmer beraten und unterstützen.
Planung im Voraus - da es sich um eine recht komplexe Veranstaltung handelt, die eine sorgfältige Planung erfordert. Die Organisatoren müssen bedenken, dass einige Teams aus dem Wettbewerb ausscheiden könnten (aufgrund der begrenzten Zeit).

Schau Dir auch die Facebook-Beiträge mit den Ergebnissen der Veranstaltung an:
https://www.facebook.com/cybereuvetproject.eu/posts/138127645211214
https://www.facebook.com/saldustehnikums/posts/1780232175520378

Die Veranstaltung wurde von LECSA in Zusammenarbeit mit der Latvijas Universitāte | Ekonomikas un kultūras augstskola / EKA University of Applied Sciences | McĀbols | cert.lv | Coldwild Games | Saldus tehnikums durchgeführt.

MEATH PARTNERSHIP (IE)

AKTIVITÄTEN

- Informationstreffen zur Bedarfsermittlung mit Studenten (Codierungstraining in einer lokalen Einrichtung der Erwachsenenbildung)
- 2-tägiger GameJam (Online-Informationssession am 1. Tag; Tag 2 ist dem Game Jam gewidmet)
- Multiplikator-Veranstaltung - Cybersecurity Awareness Morning

BESCHREIBUNG & ERGEBNISSE

1) Informationstreffen zur Bedarfsermittlung mit Studenten (Codierungstraining in einer lokalen Einrichtung der Erwachsenenbildung)

BESCHREIBUNG

Um das Projekt bekannt zu machen und die Hauptthemen für den Game Jam zu bestimmen, veranstaltete das Team von Meath Partnership eine Informationsveranstaltung mit den Schülern eines lokalen Programmierkurses. Nach dem Austausch von Informationen über Cybersicherheit und der Diskussion über die jüngsten Bedrohungen folgte ein Gruppen-Brainstorming, bei dem die SchülerInnen in zwei Gruppen aufgeteilt wurden, um Fragen zu diskutieren, die zur Ermittlung der interessantesten Themen führten, die während des Gamejams weiter erforscht werden sollten.
Weitere Informationen über den Gamejam und das CYBER.EU.VET-Projekt wurden den Teilnehmern an diesem Tag ebenfalls mitgeteilt.

BEISPIEL FÜR EINSCHÄTZUNG UND BEDARFSANALYSE


YBER.VET.EU

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

Needs assessment meeting guidelines

1. What do you know about cybersecurity?
2. Why do I need to be worried about it?
3. What are the biggest cybersecurity concerns/threats right now?
4. Do you know how to recognise those threats?
5. What is a cyber attack?
6. Can you give us an example of a cyber attack?
7. Can you give us, at least, 3 possible solutions to it?

MEATH PARTNERSHIP (IE)

ERGEBNISSE

Als Ergebnis dieser Aktivität gewann das Team von Meath Partnership ein besseres Verständnis für das allgemeine Wissen der SchülerInnen in Bezug auf Cybersicherheit und Cyberbedrohungen und sammelte Informationen, die in den Planungs- und Umsetzungsprozess des GameJams einflossen.

Schüler bei der Selbsteinschätzung und Beantwortung der Fragen

MEATH PARTNERSHIP (IE)

GAME JAM

2) 2-tägiger Gamejam
(Online-Informationssession am 1. Tag; Tag 2 ist dem Game Jam gewidmet)

BESCHREIBUNG

TAG 1 war der Begrüßung der Teilnehmer, der Vorstellung des CYBER.EU.VET-Projekts und der Eröffnung des Game Jams gewidmet sowie dem Informationsaustausch über die beiden Themen, die während der Bedarfsermittlung ermittelt wurden. Den Teilnehmern wurde die Möglichkeit geboten, einzeln oder in einem Team zu arbeiten. Sie hatten auch die Möglichkeit, Fragen zu stellen oder weitere Erläuterungen zu den Verfahren zu erhalten. im Zusammenhang mit der Entwicklung der Spiele an Tag 2.

TAG 2 war der Entwicklung der Spiele gewidmet. Mitglieder unseres Teams und ein IT-Support-Experte standen den Teilnehmern während der gesamten Dauer des Game Jams über Zoom zur Verfügung, von 9 Uhr bis 21 Uhr.
Die TeilnehmerInnen wurden eingeladen, ihre Spiele auf die Itchio-Plattform unter einem eigens für diese Veranstaltung erstellten Profil hochzuladen: CYBER.EU.VET : Cybersecurity Game Jam - itch.io

ERGEBNISSE

Nachdem die Teilnehmer ihre Spielentwürfe dem Team vorgestellt hatten, beschloss ein Teilnehmer, das Spiel zur weiteren Bewertung hochzuladen. Die übrigen Teilnehmer beschlossen, ihre Entwürfe nicht einzureichen, da sie sich noch in einem sehr frühen Stadium befanden.

Click or not click

Online interactive cybersecurity game

A short narrative driven game on raising awareness for cyber security threats. The game prompts players to make the right decision and avoid losing your security level.

Link: https://itch.io/jam/cybereuvet-cybersecurity-gamejam

Interaktives Online-Spiel zur Cybersicherheit:
https://itch.io/jam/cybereuvet-cybersecurity-gamejam

MEATH PARTNERSHIP (IE)

3) Multiplikator-Veranstaltung - Cybersecurity Awareness Morning

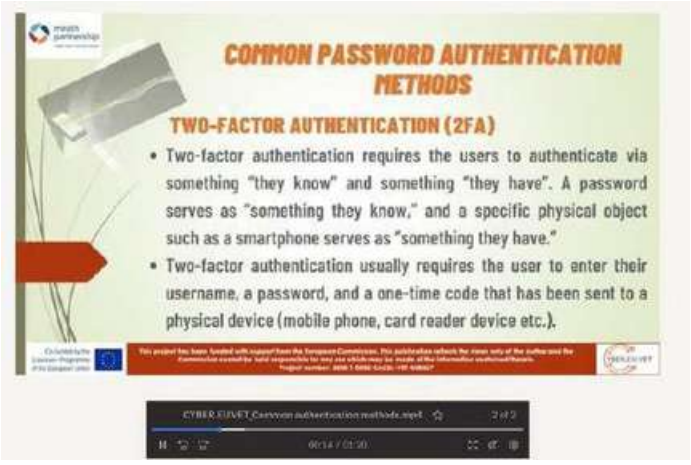
Datum: November 2021

BESCHREIBUNG

Die Multiplikatorenveranstaltung wurde online über Zoom abgehalten, um das Projekt und seine Aktivitäten bekannt zu machen. Die Veranstaltung wurde unter einer Vielzahl von Akteuren, die an Cybersicherheit interessiert oder beteiligt sind, weit verbreitet. Die Veranstaltung begann mit einer Präsentation und einem Überblick über das Projekt und den Game Jam, gefolgt von einer Präsentation und Diskussion über Cybersicherheit und dem Austausch praktischer Informationen darüber, wie man online bleiben kann (die aktuellen Cyber-Bedrohungen und wie man mögliche Angriffe verhindern kann).

ERGEBNISSE

Die Multiplikatorenveranstaltung trug dazu bei, den Bekanntheitsgrad des Projekts zu erhöhen, und bot außerdem die Möglichkeit, die seit Projektbeginn erreichten Meilensteine einem breiteren Publikum vorzustellen. Es war auch eine gute Gelegenheit, praktische Informationen und Ratschläge zur Cybersicherheit mit den Teilnehmern der Veranstaltung zu teilen.



COFAC / UNIVERSIDADE LUSÓFONA (PT)

GAME JAM

AKTIVITÄTEN

1) Cyber & Ethical Hacking Post-Graduierung für zukünftige Fachleute und Marktlehrer (Okt. 2021 - Feb. 2022 (in Partnerschaft mit einer lokalen Beratungsfirma namens Cybersec)

2) 2 GameJam-Sessions, die im Januar 2022 an berufsbildenden Schulen durchgeführt wurden: Escola de Comércio de Lisboa - https://escolacomerciolisboa.pt
Escola Profissional Almirante Reis - https://www.epar.pt

3) Ein dreieinhalbtägiges Cybertraining für Gymnasiasten im März 2022 an der Universität Lusofona als Teil der Tecweb-Veranstaltung - https://tecweb.ulusofona.pt

ERGEBNISSE

Verbreitungsbericht, in dem Sie die verschiedenen Tests sehen können, die während eines Kalenderjahres (April 2021 bis April 2022) durchgeführt wurden. In diesem Bericht sind Screenshots von Veröffentlichungen in sozialen Netzwerken, Plakate von verschiedenen Veranstaltungen und Fragebögen zum Bewusstsein für Cybersicherheit zu sehen (in portugiesischer Sprache verfügbar unter
https://docs.google.com/forms/d/e/1FAIpQLSeXACV_oeplRpTfbaC1NFKED76kRSYD6cT8cFMKjc7ohGMHZw/viewform).
Während des Cyberjams wurde auf der Grundlage der Umfragen zum Bewusstsein für Cybersicherheit auch eine Reihe von benutzerfreundlichen/interaktiven Minispielen zu einfachen Situationen durchgeführt.

TANDEM PLUS NETZWERK [FR] - MIT IASIS [GR]

GAME JAM

Spielentwicklung Cyberopolis (IASIS)

Dieses Spiel ist ein Brettspiel, das sich an Personen richtet, die sich für Cybersicherheit interessieren, mit maximal 2-4 Spielern, und dessen Hauptaspekte Datenvertraulichkeit und Datenintegrität sind... während die Themen, mit denen es sich beschäftigt, Malware, Phishing, webbasierte Angriffe, Angriffe auf Webanwendungen, Spam, Identitätsdiebstahl, DDoS und Man in the middle sind...

Sehen Sie sich das Bild von ''Cyberopolis'' an, um besser zu verstehen, welche Schritte während des Spiels zu befolgen sind und welche Aufgaben zu lösen sind...

Screenshots des Spiels während der GameJam-Sitzung, auf denen wir den Erfolg des Spiels und das große Interesse der TeilnehmerInnen sehen können.

TANDEM PLUS NETZWERK [FR] - MIT IASIS [GR]

VIDEO - Vorbeugung von Cybermobbing

Dieses vom griechischen Partner entwickelte Video bringt den Besuchern verschiedene Möglichkeiten zur Prävention und Bekämpfung von Cybermobbing näher.

YBER.EU.VET

Funded by the European Union

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.

Gestaltung
NGO Nest Berlin e.V.
Berlin, 2022

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