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

YBER.VET.EU

AMÉLIORER LA PRÉPARATION À LA CYBERSÉCURITÉ DU SECTEUR EUROPÉEN DE L'ENSEIGNEMENT ET DE LA FORMATION PROFESSIONNELS

MATÉRIEL DE FORMATION

SENSIBILISATION À LA CYBERSÉCURITÉ MATÉRIEL DE FORMATION POUR LE SECTEUR DE L'EFP

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

INTRO

De l'automne 2021, en lien avec le mois européen de la cybersécurité, au printemps 2022, les partenaires du projet CYBER.VET.EU ont organisé plusieurs GameJams dans les pays des partenaires. Les jeunes ont été impliqués en leur donnant l'opportunité d'être proches des sujets de cybersécurité et en leur fournissant de nouveaux outils.

L'objectif principal était de répondre au besoin de sensibilisation à la cybersécurité. Nous nous sommes tournés vers le processus de "gamification" afin d'obtenir une solution facile à adopter, rapide à mettre en œuvre, évolutive dans le temps et inclusive. Le processus de gamification, défini comme "l'application des mécanismes du jeu à des contextes non ludiques dans le but de susciter l'engagement et d'augmenter les niveaux de motivation", est un moyen éprouvé de maintenir les utilisateurs engagés dans des activités d'apprentissage, avec d'excellents résultats même sur une courte période grâce à l'exploitation du divertissement qui motive les participants à s'engager davantage avec le matériel et à pratiquer. En tant que tel, ce produit agira comme une combinaison de directives, de formation et de pratique, avec la caractéristique d'être facilement mis à jour lorsque du nouveau matériel doit être ajouté.

RÉSULTATS DES ACTIVITÉS / GAME JAMS

- Sensibilisation accrue à la sécurité numérique
- Sensibilisation accrue à la sécurité numérique au sein des communautés des participants (famille, amis, collègues)
- Réduction du taux de réussite des logiciels malveillants au sein des institutions
- Réduction du nombre de fuites de données
- Intérêt accru pour le secteur de la cybersécurité en tant qu'opportunité d'emploi.

AEII / INERCIA DIGITAL [ES]

ACTIVITES

Les activités les plus pertinentes menées par les partenaires espagnols AEII et Inercia Digital ont été les suivantes:

- Hackathon
- GameJams
- Journées d'information
- Conférence internationale
- Evénement de diffusion

RÉSULTATS

Les sessions GameJam en Espagne ont fourni des résultats utiles qui peuvent être consultés ici :https://www.youtube.com/watch?v=3QFI9iB0iJU&t=124s

SUR LE SCRATCH

https://scratch.mit.edu/projects/611211889/
Cybersécurité - Attaqué

https://scratch.mit.edu/projects/610354561/
en espagnol

https://scratch.mit.edu/projects/611201682/

https://scratch.mit.edu/projects/714361293/
en espagnol

https://scratch.mit.edu/projects/714362963/
en espagnol

https://scratch.mit.edu/projects/714362911/
sur le phishing - un remix

https://scratch.mit.edu/projects/606933322
sur le phishing - en anglais

AEII / INERCIA DIGITAL [ES]

GAME JAM

AEII / INERCIA DIGITAL [ES]

Hackathon

La cybersécurité dans l'éducation

Les partenaires espagnols AEII et Inercia Digital ont participé en ligne à un Hackathon du 20 au 22 octobre 2021, avec 47 participants, dont de nombreux experts en informatique. https://www.comprometidosporelfuturo.com/proyectos# soutenu par Boehringer Ingelheim en Espagne.

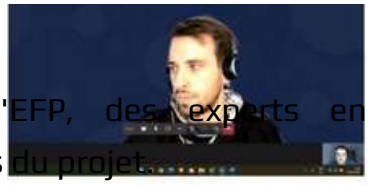
PROBLÈME À RÉSOUDRE

La cyberintimidation est l'un des principaux risques de l'internet pour les jeunes. Il est fréquent de trouver des messages au contenu offensant pour certaines personnes et que ceux-ci soient utilisés pour harceler et se moquer des victimes.

La cyberintimidation provoque souvent de graves perturbations chez les victimes, telles que le syndrome de stress post-traumatique, la dépression, les pensées et comportements suicidaires ou l'anxiété.

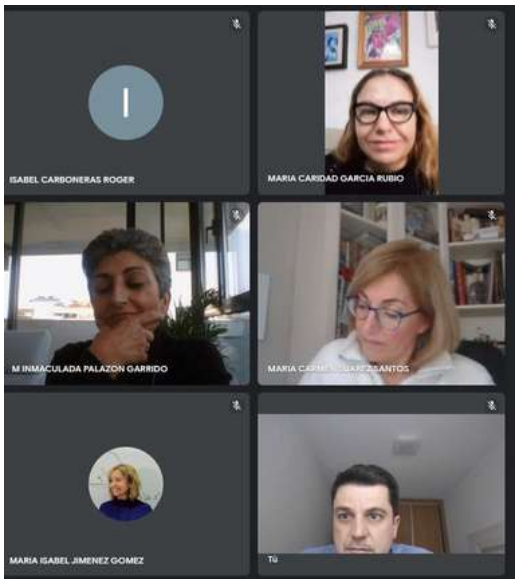
Ce défi consiste à étudier et à analyser les connaissances des jeunes en matière de sécurité, ainsi qu'à les sensibiliser aux risques qu'ils encourent dans leurs centres éducatifs et dans leur vie quotidienne.
Ce défi vise, par le biais de la gamification, à sensibiliser les élèves et les enseignants de la vie quotidienne aux questions liées à la sécurité dans l'utilisation des nouvelles technologies..

RÉSULTATS



- Jeu et animation liés à la cybersécurité dans l'enseignement
- Participation de l'administration publique, des écoles d'EFP, des experts en informatique, des enseignants, des étudiants et des partenaires du projet
- Création de courtes vidéos interactives

AEII / INERCIA DIGITAL [ES]



D'une manière générale, après avoir mené de nombreuses enquêtes, les connaissances en matière de cybersécurité des enseignants et des étudiants des centres de formation professionnelle sont encore faibles en Espagne. Pour cette raison, ce projet et d'autres similaires sont très pertinents en Espagne.

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

GAME JAM

L'ONG Nest Berlin, Extrafondente Open Source - EOS et IASIS ont organisé ensemble une session de GameJam en février 2022. La GameJam a débuté le samedi 12 et a duré 6 jours au total. Elle a vu les équipes nationales développer et travailler ensemble sur une ébauche de jeu (d'un jeu en ligne ou de plateau).

Un jury indépendant a été réuni et a été invité à évaluer le projet de jeu en suivant des directives communes et un modèle d'évaluation.

L'équipe gagnante a bénéficié d'un mentorat de 6 mois ainsi que de ressources techniques afin de poursuivre le développement de son idée de jeu.

A PROPOS DU JEU

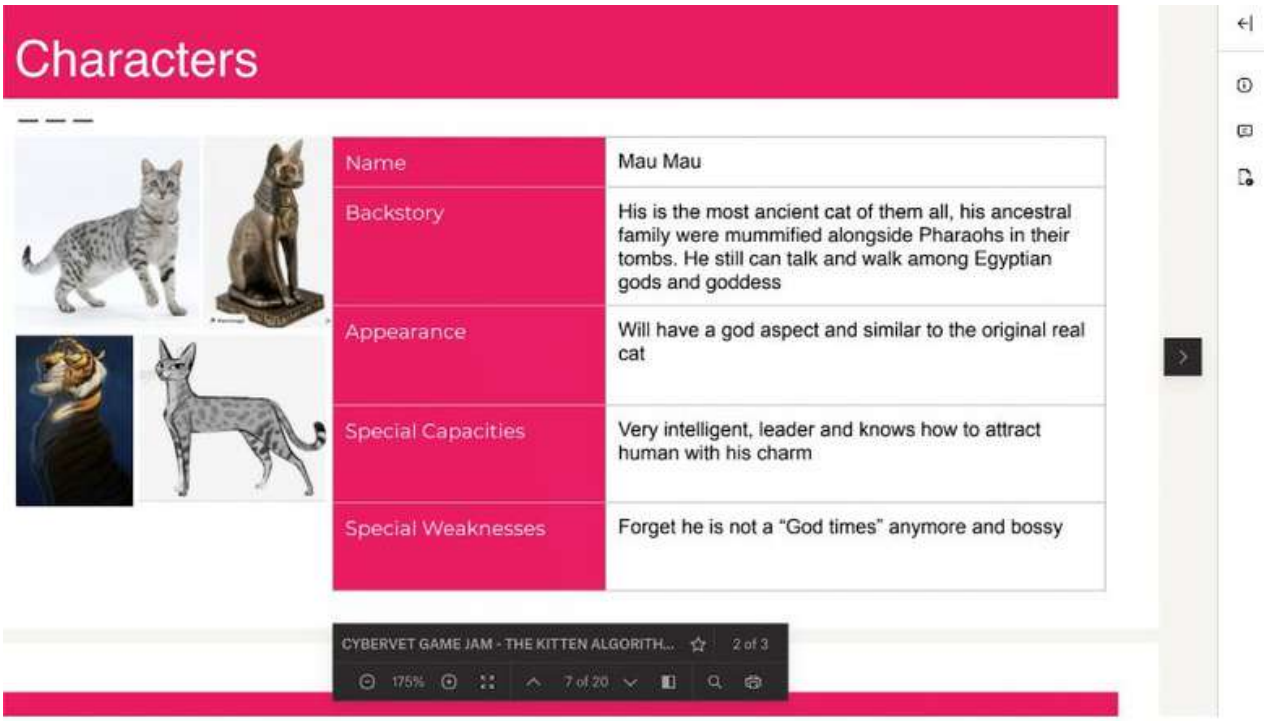
Il s'agit d'un jeu de société stratégique de 2 à 6 joueurs, qui se joue en 30 à 60 minutes. Dans ce jeu, vous devez tromper les humains pour les convaincre que vous êtes le meilleur chat et obtenir plus de prestige en obtenant le plus grand nombre possible de serviteurs des chats humains. Gardez l'œil ouvert, les autres chats patrons vont activement essayer de saboter votre chemin pour atteindre les humains et prendre la gloire pour eux-mêmes. Ne vous fiez pas à leurs jolis visages !

Vous perdez la partie si vous n'avez pas un nombre élevé d'humains comme serviteurs ou si le 10ème tour est terminé et qu'aucun des joueurs n'a au moins 4 humains sous son commandement.

La difficulté réside dans le fait qu'il y a 6 patrons qui essaient de tromper les humains pour qu'ils deviennent leurs serviteurs et qu'ils puissent les contrôler, mais tout le monde a le même objectif et certains pourraient même aider les humains à se libérer du contrôle du chat.

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

Mau Mau



LECSA (LV)

GAME JAM

Le partenaire LECSA de Lettonie a organisé un événement GameJam du 27 septembre au 1er octobre 2021. En raison des restrictions épidémiologiques et des différents lieux où se trouvaient les participants, l'événement a été organisé de manière hybride (sur place à l'école technique de Saldus et via la plateforme Zoom). Pendant l'événement, 6 équipes (4-5 personnes par équipe) ont été formées pour travailler sur le développement de prototypes de jeux. Pour obtenir des résultats tangibles, le concept de Game Jam prévoyait le développement de deux types de jeux : des jeux d'ordinateur et des jeux de société.

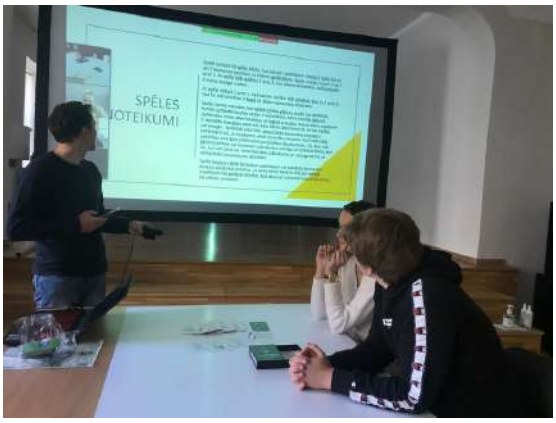
ACTIVITÉS

- Les mois d'août et septembre 2021 ont été consacrés à la planification et à l'organisation de l'événement (recherche d'experts en cybersécurité et en développement de jeux, diffusion d'informations aux participants potentiels, planification de l'agenda et définition des critères du jeu, etc.)
- Evénement multiplicateur - Actualité des cyberattaques (27.09.2021) : Introduction du projet CYBER.EU.VET et conférence sur les tendances en matière de cyberattaques avec M. Armins Palms, expert en cybersécurité du CERT.LV (institution de réponse aux incidents de sécurité informatique de la République de Lettonie).
- Nombre de participants : 26 personnes
- Lieu : École technique de Saldus (ville de Saldus) et plateforme ZOOM
- Annonce du Game Jame (27.09.2021) : définition et discussion sur les défis actuels de la cybersécurité (évaluation des besoins) ; formation des équipes, rencontre avec les mentors et discussion sur la suite du travail (atelier sur le moteur de jeu Unity), brainstorming sur l'idée et le concept du jeu.
- Activités de Game Jam en cours (28.09-30.09.2021) : les équipes ont travaillé sur le développement de prototypes, la consultation avec les mentors a été assurée, si nécessaire.
- Présentation de l'avancement (30.09.2021) : présentation des concepts de jeu et de l'avancement du travail pour recevoir les suggestions des mentors.
- Grande finale (01.10.2021) : quatre équipes ont présenté leurs résultats et les mentors ont fourni une évaluation. Une équipe, développant un jeu d'ordinateur, s'est retirée. Conclusion de l'événement et discussion informelle.
    - Nombre de participants : 30
    - Lieu : École technique de Saldus et plateforme ZOOM

LECSA (LV)

RÉSULTATS

1. prototype du jeu en ligne - Le Virus
2. Jeu de société - Cards About Security
3. Jeu de société - Cyberwar
4. Jeu de cartes compétitif - Cyber Mind



EXAMPLE Cyber Mind - Un jeu de cartes compétitif

Il s'agit d'un jeu de cartes éducatif avec des éléments de quiz. La tâche principale du jeu est d'enseigner les bases de la sécurité quotidienne sur Internet et ce à quoi les gens s'exposent en y faisant des bêtises. Il couvre des sujets tels que la sécurité sur Internet et la protection des données dans le contexte de l'utilisation des réseaux sociaux. À l'issue du jeu, les personnes (joueurs) devraient être capables de reconnaître les tentatives d'escroquerie dans la vie réelle.

Développé par l'équipe Veiksminieki (du letton : les gens qui réussissent), des étudiants de l'école technique de Saldus lors de la Game Jam en Lettonie (octobre 2021) :

Renars Ricards Hartmanis, Estere Ozoliņa, Sindija Diāna Valtere & autres.

Niveau : élémentaire (pour les débutants). Groupe cible : élèves, étudiants, enseignants et parents.

Le jeu contient : 50 cartes, 2 carnets de santé (pour compter la santé des joueurs), 2 dés et une carte de règle.

LECSA (LV)

GAME JAM

À PROPOS DE

Les tentatives de cyberattaques dans le monde augmentent chaque jour. Le gouvernement mondial a donc eu l'idée d'organiser un tournoi pour identifier les personnes qui présentent des cyberrisques et les contrer. Jeu éducatif permettant d'apprendre les principaux types de cyberattaques, les méthodes de prévention et d'élimination en se protégeant ou en protégeant son équipe et en contre-attaquant l'adversaire. Le but du jeu est d'éliminer toutes les vies de l'adversaire.

COMMENT JOUER/RÈGLES DU JEU

Nombre de joueurs : 2 ou 4 personnes (1 contre 1 ou 2 contre 2).
Chaque joueur ou équipe (à 2 contre 2) dispose de "100 vies" (Health=HP) au début du jeu.
Le décompte des points de vie se fait à l'aide de blocs-notes noirs ou d'autres notes disponibles. Désignez une personne distincte qui suivra et calculera la consommation d'énergie et de santé des joueurs, si possible. Sinon, les joueurs le font eux-mêmes.
Chaque joueur reçoit 5 cartes. Si le jeu se joue à 2 contre 2, les deux joueurs ont "une main commune" dans l'équipe ou 10 cartes ensemble.

Il existe trois types de cartes : Cartes d'attaque (rouge), Cartes de bouclier (jaune) et Cartes de vie ou de guérison (vertes).

Le jeu se joue en rounds. Le joueur/équipe qui obtient le plus grand nombre avec les dés commence la partie.

Chaque carte coûte de l'énergie. Au début de chaque tour, le joueur lance 2 dés pour définir une énergie qui est indiquée en haut de la carte (en bleu). Les cartes doivent être jouées de manière à ne pas dépasser le montant d'énergie obtenu.
Le joueur/équipe qui commence le tour peut attaquer (avec des cartes d'attaque), se protéger (cartes de bouclier) ou ajouter de la vie (cartes de guérison), tandis que les seconds peuvent uniquement utiliser les cartes d'attaque et de bouclier pour minimiser leur vulnérabilité en termes de vie.
Gardez à l'esprit que le nombre maximum de vies par joueur/équipe pendant le jeu peut être de 100 HP (par exemple, si la somme des vies et de l'énergie après le tour fait 110 HP au total, votre nombre de vies reste quand même de 100 HP).
Le jeu se termine dès qu'un joueur/équipe n'a plus de vies (0 vie).
Si le jeu n'a plus de cartes, vous devez à nouveau mélanger les cartes de la pile.

LECSA (LV)

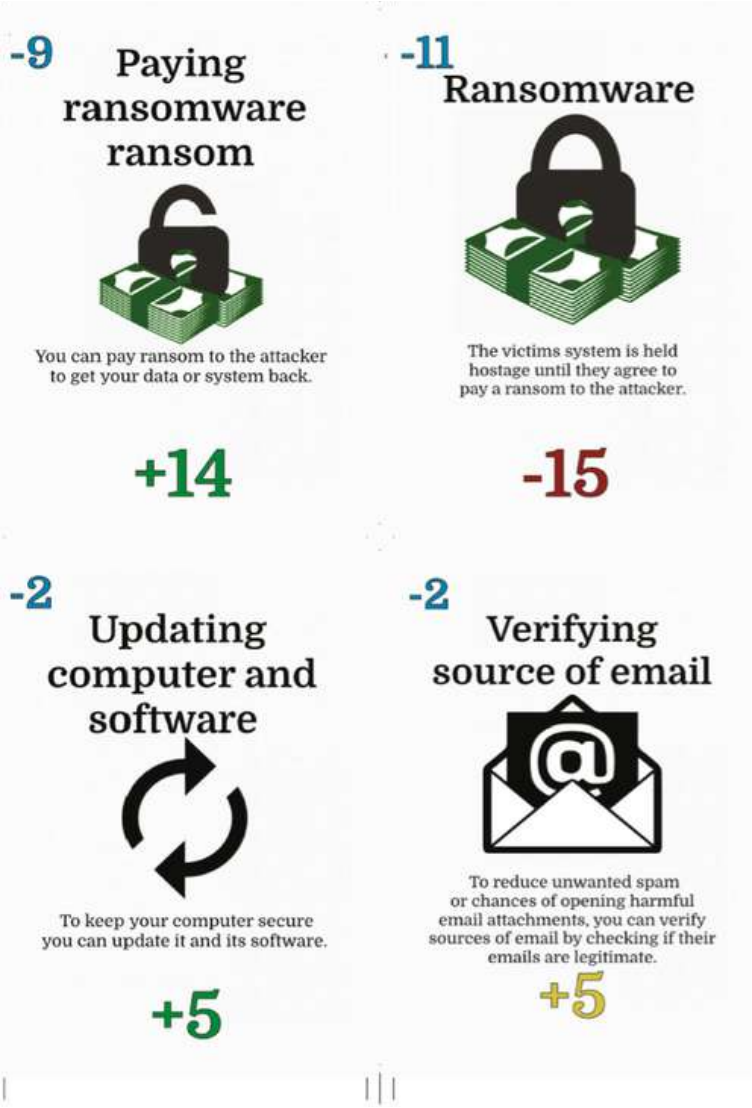
Exemples de cartes

En **bleu** – Energie

En **rouge** Cartes d'attaque

En **jaune** - Cartes de bouclier

En vert - Cartes de guérison



Exemple de calcul de la santé

EXEMPLE Cyberwar - Jeu de société

Développé par l'équipe Exodus (étudiants de l'école technique de Saldus), leader de l'équipe Valdemārs Šperbergs.

2-6 joueurs < - > Convient aux personnes âgées de 15 ans et plus.

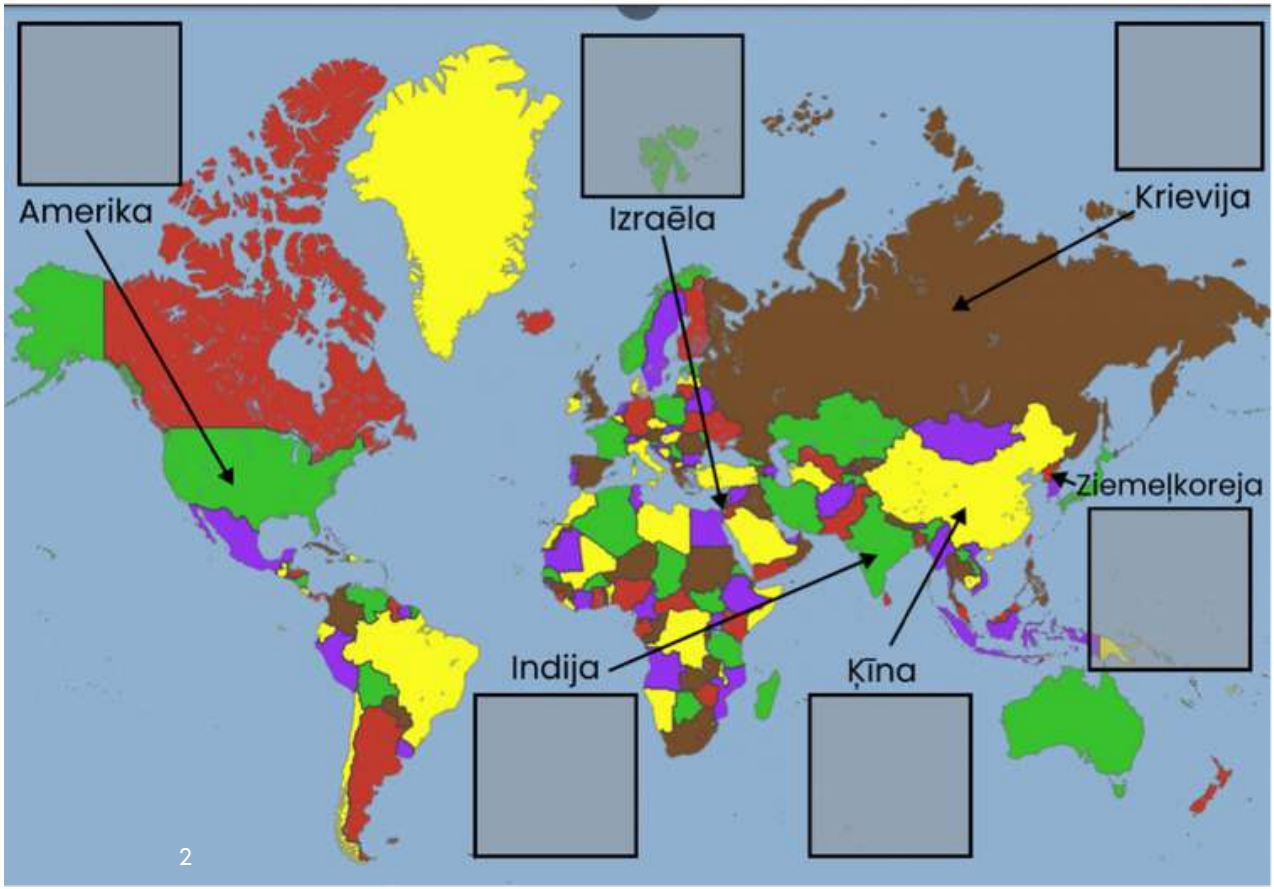
Un jeu de société qui met l'accent sur la tactique et l'aléatoire (le hasard).

Niveau : jeu éducatif pour ceux ayant une certaine compréhension sur la cybersécurité.

Le jeu contient : Une carte du monde, 2 dés, des serveurs, des cartes avec fonction "attaque", "défense" ou "réaction", une légende des vulnérabilités, un tableau avec les mouvements possibles pour chaque type de vulnérabilité.

À PROPOS DE

Le but du jeu est de protéger le pays représenté par le joueur et d'attaquer les autres pays pour gagner la cyber-guerre. Dans Cyberwar, chaque joueur doit choisir un pays à représenter. Chaque joueur dispose d'un serveur avec 3 vulnérabilités. Le but du joueur est de pirater les serveurs des autres pays en exploitant deux des trois vulnérabilités ou de corriger deux des trois vulnérabilités sur son propre serveur.



LECSA (LV)

COMMENT JOUER

Les joueurs choisissent le pays à représenter et placent un objet serveur à l'endroit désigné sur la carte. Chaque pays a ses propres bonus.

Chaque joueur tire au hasard (prend) 3 vulnérabilités - une de chaque niveau de difficulté, et les place face cachée à leur emplacement respectif sur leur champ serveur. Les vulnérabilités ne sont pas connues des joueurs.

Les vulnérabilités ont 3 niveaux de difficulté. Le niveau de difficulté détermine également le nombre de chiffres nécessaires pour exploiter une vulnérabilité (voir "Attaques"), ainsi que le nombre de coups nécessaires pour corriger la vulnérabilité (voir "Défense").

Le jeu se déroule en tours, les actions (mouvements) suivantes peuvent être effectuées - **Scanning, Attaque et Défense**. Les joueurs déterminent la séquence des joueurs en lançant deux dés.

Début

Chaque joueur reçoit 4 cartes au début de chaque tour. A la fin du tour, il est possible - de garder 2 cartes ou de les échanger contre des cartes existantes.

Le 1er tour est un tour de balayage où aucune carte d'attaque ou de défense n'est autorisée. Lors des tours suivants, les joueurs peuvent choisir de scanner ou d'attaquer ou d'essayer de réparer leurs vulnérabilités (voir Défense). Le jeu se poursuit tour après tour jusqu'à ce qu'une condition de victoire soit atteinte.

Numérisation

- L'attaquant choisit un pays pour scanner sa vulnérabilité (par exemple, "Je scanne un Russe de 2ème niveau de vulnérabilité").
- Le joueur effectue le scan - lance deux dés, applique les bonus de son pays représenté, compare avec le niveau de difficulté de la vulnérabilité + les bonus du pays de la victime.

Si l'attaquant obtient un nombre égal ou supérieur au niveau de difficulté de la vulnérabilité de la victime, il peut regarder la vulnérabilité scannée.

- Les bonus des pays ne sont pas ajoutés lorsque l'on se scanne soi-même.

Niveaux de difficulté

1er - le joueur doit obtenir au moins le numéro 4 (hors bonus du pays).

2ème - le joueur doit obtenir au moins le numéro 8 (sans les bonus du pays)

3ème - le joueur doit obtenir au moins le numéro 11 (sans les bonus du pays).

ATTAQUE

Le joueur nomme la cible de l'attaque (par exemple, "J'attaque une vulnérabilité russe de niveau 2") et révèle la carte d'attaque à tous les joueurs, en la plaçant à côté de la vulnérabilité.

Le joueur lance le dé pour voir si l'attaque fonctionne en comparant le résultat du dé à la difficulté de la vulnérabilité + les bonus (si le résultat du dé + les bonus correspondent ou dépassent la difficulté, l'attaque réussit).

Les attaques peuvent être repoussées en utilisant la carte de réaction prévue pour cette attaque. Chaque attaque a son propre type de réaction qui peut être jouée et son propre type de vulnérabilité pour laquelle elle fonctionne.

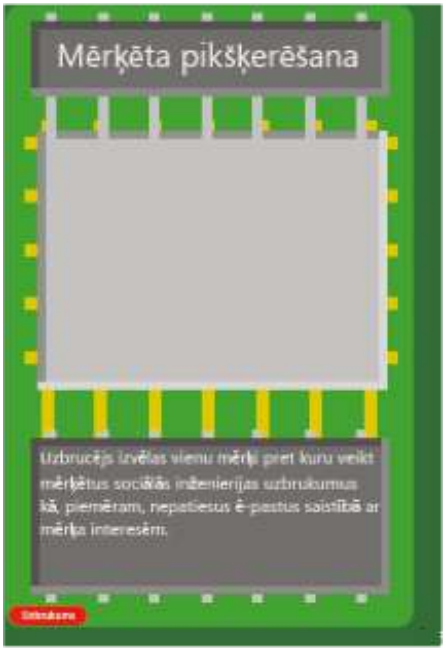
- Si l'attaque échoue ou est bloquée par une carte Réaction - les cartes Attaque et Réaction jouées restent sur la table jusqu'à la fin du prochain tour et empêchent les autres joueurs d'attaquer avec la même attaque pour la même vulnérabilité. Après le déplacement, les deux cartes retournent sur la pile.

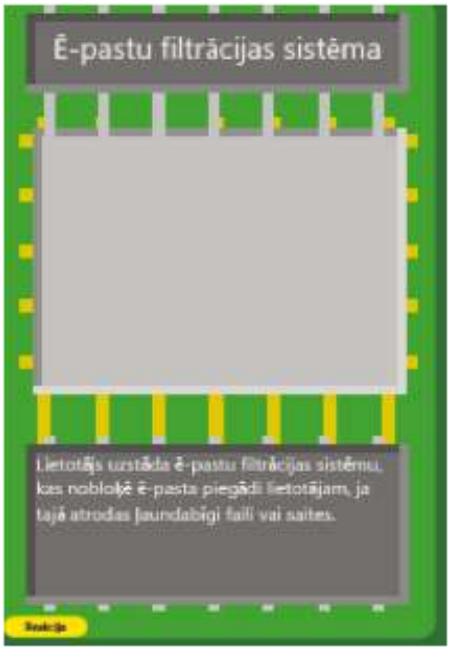
Niveaux de difficulté

1er - le joueur doit obtenir au moins le numéro 4 (hors bonus du pays).

2ème - le joueur doit obtenir au moins le numéro 8 (sans les bonus du pays)

3ème - le joueur doit obtenir au moins 11 (sans les bonus du pays).





LECSA (LV)

Défense

- Défense - choisir la bonne méthode contre une vulnérabilité particulière. Les cartes Réaction arrêtent (annulent) l'attaque entrante (et toutes les autres attaques visant la même vulnérabilité) pendant 1 tour.
- Pour annuler une attaque entrante, le joueur place une carte Réaction correspondant au type d'attaque (voir tableau des vulnérabilités) sur la carte d'attaque dès que l'attaque est jouée.
- Pour commencer à réparer une blessure, le joueur place une carte Défense à côté de la blessure à réparer.
- Les autres joueurs peuvent attaquer cette blessure pendant qu'elle est en défense (avant que le tour de défense ne soit terminé).
- Lorsque le joueur tente de réparer une blessure sur son serveur avec une carte Défense, celle-ci ne peut pas attaquer, mais peut essayer d'empêcher les attaques avec des cartes Réaction. Pour une réparation complète, il faut |niveau de difficulté + 1| tour. Les actions de balayage sont autorisées pendant la période de réparation.

Si la méthode de défense n'est pas correcte, le joueur saute 3 tours et ne peut pas utiliser de cartes de défense pendant cette période (les réactions et les actions de balayage sont autorisées).

Primes des pays

- USA : +2 en numérisation
- Russie : +2 pour les attaques
- Chine : +2 pour la défense contre les attaques
- Corée du Nord : +2 pour la défense contre les balayages
- Inde : +1 à toutes les attaques, -1 contre les attaques
- Israël : +3 dans toutes les attaques, -3 contre les attaques

Vulnérabilités par niveaux

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; Code injection using Polyglot	Introductory synthesis	Introduction of the symbol blacklist

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

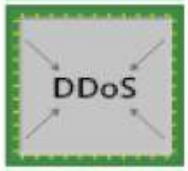
Rūtera panelis ar noklusējuma lietotājvārdu un paroli

XSS ievainojums ar filtru

SQL injekcija ar filtru

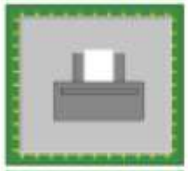
Nepilnīgi nokonfigurēts ugunsmūris

WiFi tīkls ar WEP drošību



Pakalpojuma atteices kļūda

Ievainojama OpenSSL programma

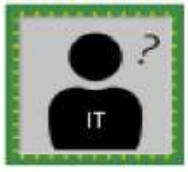


Ievainojama Print Spooler programma

Bufera pārpildes ievainojums

Vājš jaucējvērtības algoritms

Aizņemts priekšnieks



Slinks IT speciālists

LECSA (LV)

GAME JAM

LECSA (LV)

CONSEILS ET EXPÉRIENCES DU GAMEJAM EN LETTONIE

- Au cours de l'événement de deux jours, il n'est pas possible de développer un véritable jeu vidéo, mais plutôt un premier prototype, qui pourra ou non être développé en fonction de la motivation des participants.
- Des prix ou d'autres types d'avantages peuvent contribuer à impliquer davantage de participants et à garantir de meilleurs résultats (plus tangibles) à la fin (dans notre cas, des pizzas et des boissons ont été offertes à la fin de l'événement, ainsi qu'un soutien supplémentaire de la part des mentors (par exemple pour placer des jeux sur la plate-forme)).
- Les mentors sur les questions de développement de jeux et de cybersécurité jouent un rôle important dans la Game Jam en consultant et en aidant les participants.
- Planification à l'avance - il s'agit d'un événement assez complexe qui nécessite une planification minutieuse.
- Les organisateurs doivent tenir compte du fait que certaines équipes peuvent être exclues de la compétition (en raison du temps limité).

Veuillez consulter les posts FB avec les résultats de l'événement.:https://www.facebook.com/cybereuvetproject.eu/posts/138127645211214 https://www.facebook.com/saldustehnikums/posts/1780232175520378

L'événement a été organisé par LECSA en coopération avec la Commission européenne. Latvijas Universitāte | Ekonomikas un kultūras augstskola / EKA University of Applied Sciences | McĀbols | cert.lv | Coldwild Games | Saldus tehnikums!

MEATH PARTNERSHIP (IE)

ACTIVITÉS

- Réunion d'information sur l'évaluation des besoins avec les étudiants (formation au codage dans un établissement local d'enseignement pour adultes)
- GameJam de 2 jours (session d'information en ligne le 1er jour ; 2ème jour consacré au Game Jam)
- Événement multiplicateur - Matinée de sensibilisation à la cybersécurité

DESCRIPTION & RÉSULTATS

1) Réunion d'information sur l'évaluation des besoins avec les étudiants
(formation au codage dans un établissement local d'enseignement pour adultes)

Date : Octobre 2021

DESCRIPTION

Afin de diffuser le projet et d'identifier les principaux thèmes de la Game Jam, l'équipe de Meath Partnership a organisé une session d'information avec les étudiants d'une classe locale de formation au codage. Le partage d'informations sur la cybersécurité et la discussion sur les menaces les plus récentes ont été suivis d'une session de brainstorming où les étudiants ont été divisés en deux groupes afin de discuter des questions permettant d'identifier les sujets les plus intéressants à explorer pendant le Gamejam. Des informations supplémentaires sur le Gamejam et le projet CYBER.EU.VET ont également été partagées avec les participants ce jour-là.

EXEMPLE D'ÉVALUATION

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)

RÉSULTATS

Grâce à cette activité, l'équipe de Meath Partnership a pu mieux comprendre les connaissances générales des élèves en matière de cybersécurité et de cybermenaces. Elle a également recueilli des informations qui ont été intégrées dans le processus de planification et de mise en œuvre du GameJam.

L'ÉVALUATION EN ACTION

2) Gamejam de 2 jours

(session d'information en ligne le 1er jour ; 2ème jour dédié au Game Jam)

DESCRIPTION

La première journée a été consacrée à l'accueil des participants, à la présentation du projet CYBER.EU.VET et à l'ouverture de la Game Jam, ainsi qu'au partage d'informations sur les deux sujets identifiés lors de la réunion d'évaluation des besoins. Les participants ont eu la possibilité de travailler individuellement ou en équipe. Ils ont également eu la possibilité de poser des questions ou d'obtenir des précisions sur les procédures liées au développement des jeux le deuxième jour.

Le deuxième jour était consacré au développement des jeux. Des membres de notre équipe et un expert en support informatique étaient disponibles via Zoom pour aider les participants pendant toute la durée de la Game Jam, de 9h à 21h.
Les participants ont été invités à télécharger leurs jeux sur la plateforme Itchio sous un profil créé dans le cadre de cet événement : CYBER.EU.VET : Cybersecurity Game Jam - itch.io

RÉSULTATS

Après que les participants ont partagé leurs ébauches de jeux avec l'équipe, un participant a décidé d'aller de l'avant et de télécharger le jeu pour une évaluation plus approfondie. Les autres participants ont décidé de ne pas soumettre leurs ébauches car elles n'en étaient qu'à leurs débuts.

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

Jeu interactif en ligne sur la cybersécurité :
https://itch.io/jam/cybereuvet-cybersecurity-gamejam

MEATH PARTNERSHIP (IE)

3) Événement multiplicateur - Matinée de sensibilisation à la cybersécurité

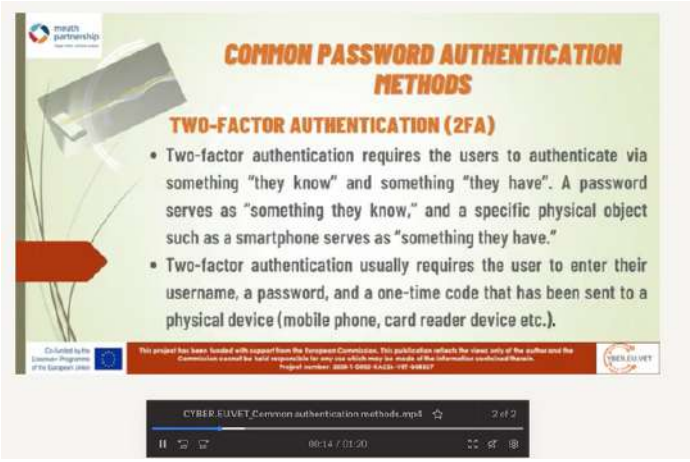
Date: Novèmbre 2021

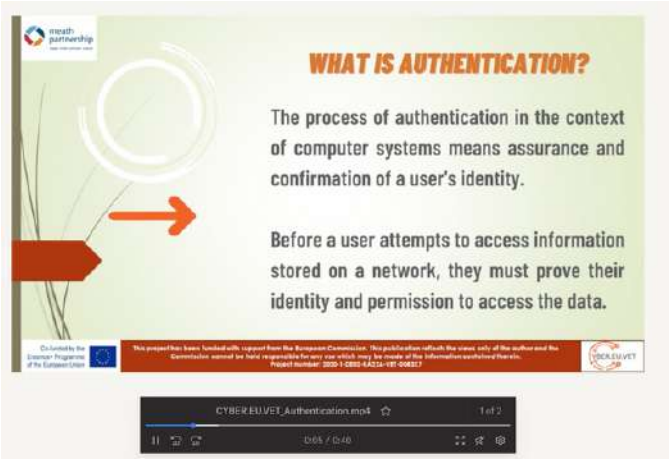
DESCRIPTION

L'événement multiplicateur a été organisé en ligne via Zoom afin de faire connaître le projet et ses activités. L'événement a été largement diffusé auprès d'une grande variété de parties prenantes intéressées ou impliquées dans la cybersécurité. L'événement a commencé par une présentation et une vue d'ensemble du projet et de la Game Jam, suivie d'une présentation et d'une discussion sur la cybersécurité et le partage d'informations pratiques sur la façon de rester en ligne (les cybermenaces actuelles et la façon d'éliminer les attaques possibles étaient possibles).

RÉSULTATS

L'événement multiplicateur a contribué à faire connaître le projet et a également permis de présenter à un public plus large les étapes franchies depuis le début du projet. Ce fut également une excellente occasion de partager des informations et des conseils pratiques en matière de cybersécurité avec les participants à l'événement.





COFAC / UNIVERSIDADE LUSÓFONA (PT)

GAME JAM

ACTIVITÉS

1) Cyber & Ethical Hacking post-graduation pour les futurs professionnels et les enseignants du marché Oct 2021 - Fév 2022 (en partenariat avec un cabinet de conseil local nommé Cybersec)

2) 2 Sessions GameJam organisées en janvier 2022 dans les écoles d'EFP :

Escola de Comércio de Lisboa - https://escolacomerciolisboa.pt

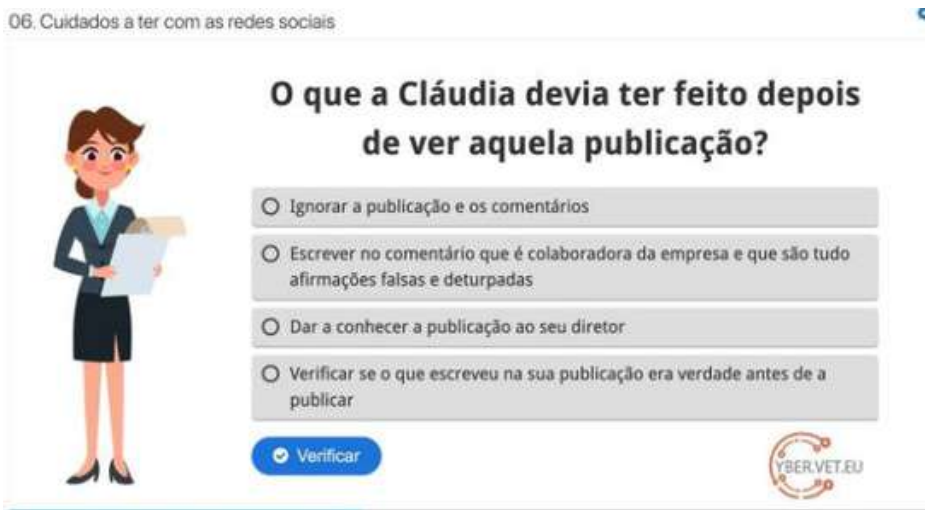
Escola Profissional Almirante Reis - https://www.epar.pt

3**)** cyberformation de trois demi-journées pour les élèves de l'enseignement secondaire en mars 2022 à l'Université Lusofona dans le cadre de l'événement Tecweb. - https://tecweb.ulusofona.pt

RÉSULTATS

Preuve du rapport de diffusion où l'on peut voir les différents tests qui ont été réalisés pendant une année civile (avril 2021 à avril 2022). Dans ce rapport, nous pouvons voir des captures d'écran de publications sur les réseaux sociaux, des affiches de différents événements, des questionnaires sur la sensibilisation à la cybersécurité (disponibles en portugais à l'adresse suivante https://docs.google.com/forms/d/e/1FAIpQLSeXACV_oeplRpTfbaC1NFKED76kRSYD6cT8cFMKjc7ohGMHZw/viewform).

DAu cours des Cyberjams, il a également été créé, sur la base des enquêtes de sensibilisation à la cybersécurité, une série de mini-jeux interactifs et conviviaux portant sur des situations simples.



TANDEM PLUS NETWORK – MEMBER IASIS [GR]

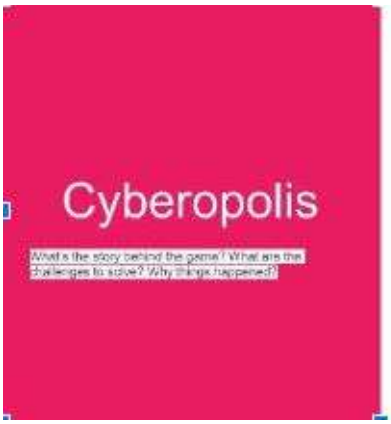
GAME JAM

Outil de conception de jeux (IASIS) - Cyberopolis

Ce jeu est un jeu de société destiné aux personnes intéressées par la cybersécurité, avec un maximum de 2-4 joueurs, et ses principaux aspects sont la confidentialité et l'intégrité des données; tandis que les sujets qu'il traite sont les logiciels malveillants, le phishing, les attaques basées sur le Web, les attaques d'applications Web, le spam, le vol d'identité, les DDoS et l'homme au milieu...

Voir l'image de ''Cyberopolis'' pour mieux comprendre les étapes à suivre pendant le jeu et les défis à résoudre.

Captures d'écran du jeu lors de la session GameJam où l'on peut constater le succès du jeu et le grand intérêt manifesté par les participants.



RÉSEAU TANDEM PLUS – MEMBRE IASIS [GR]

VIDEO - Prévention de la cyberintimidation

Cette vidéo développée par le partenaire grec rapproche les visiteurs des différentes manières de prévenir et de combattre la cyberintimidation.

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.

Design
NGO Nest Berlin e.V.
Berlin, 2022

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