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

MELHORAR A PREPARAÇÃO PARA A CIBERSEGURANÇA DO SETOR EUROPEU DO ENSINO E FORMAÇÃO PROFISSIONAL

MATERIAIS DE FORMAÇÃO

MATERIAL DE FORMAÇÃO DE SENSIBILIZAÇÃO PARA A CIBERSEGURANÇA PARA O SETOR DO EFP

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

INTRODUÇÃO

Desde o outono de 2021, relacionado com o Mês Europeu da Cibersegurança, até à primavera de 2022, os parceiros do projeto CYBER.VET.EU organizaram várias Game Jams nos países parceiros. Envolveram-se jovens que tiveram a oportunidade de estarem próximos dos temas de cibersegurança e de novas ferramentas.

O principal objetivo aqui foi resolver a necessidade de aumentar a sensibilização para a cibersegurança. Recorremos ao processo de "gamificação" com vista a obter uma solução fácil de adotar, rápida de implementar, escalável no tempo e inclusiva. O processo de gamificação, definido como "a aplicação de mecânicas de jogos a contextos não relacionados com jogos com o objetivo de induzir o envolvimento e aumentar os níveis de motivação", é uma forma comprovada de manter os utilizadores envolvidos em atividades de aprendizagem, com ótimos resultados mesmo num período curto de tempo graças ao aproveitamento do entretenimento que motiva os participantes a envolverem-se mais com o material e a praticarem. Como tal, este produto funcionará como uma combinação de diretrizes, formação e prática, com a característica de ser facilmente atualizável quando se adiciona novo material.

RESULTADOS DAS ATIVIDADES / GAME JAMS

- Maior consciência sobre segurança digital
- Maior consciência sobre segurança digital entre as comunidades dos participantes (família, amigos, colegas).
- Redução da taxa de sucesso de malware no seio das instituições Redução de eventos de fuga de dados
- Maior interesse pelo setor da cibersegurança como oportunidade de emprego.

ATIVIDADES

As atividades mais relevantes realizadas pelos parceiros espanhóis AEII e Inercia Digital:

Hackathon

GameJams

Dias de informações

Conferência internacional

Evento de disseminação

RESULTADOS

As sessões de Game Jam em Espanha proporcionaram alguns resultados úteis que podem ser vistos aqui:

https://scratch.mit.edu/projects/611211889/

https://scratch.mit.edu/projects/611201682/ https://www.youtube.com/watch?v=3QFI9iB0iJU&t=124s

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 ...

AEII / INERCIA DIGITAL [ES]

Hackathon

Cybersecurity in Education

Os parceiros espanhóis AEII e Inercia Digital participaram online num Hackathon entre 20 e 22 de outubro de 2021, com 47 participantes, muitos deles especialistas em TI. https://www.comprometidosporelfuturo.com/proyectos# apoiado pela Boehringer Ingelheim em Espanha.

PROBLEMA PARA RESOLVER

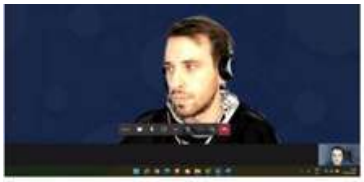
O ciberbullying é um dos principais riscos da Internet para os jovens. É comum encontrar publicações com conteúdos ofensivos para algumas pessoas e que são utilizadas com o intuito de assediar e gozar com as vítimas.

O ciberbullying provoca frequentemente perturbações graves nas vítimas, tais como perturbação de stress pós-traumático, depressão, pensamentos e comportamentos suicidas ou ansiedade.

Este desafio consiste em estudar e analisar o que os jovens sabem sobre segurança, assim como sensibilizá-los para os riscos que correm nos seus centros educativos e na vida quotidiana.
Este desafio procura, através da gamificação, a maior consciência de alunos e professores no dia a dia sobre questões relacionadas com a segurança na utilização de novas tecnologias.

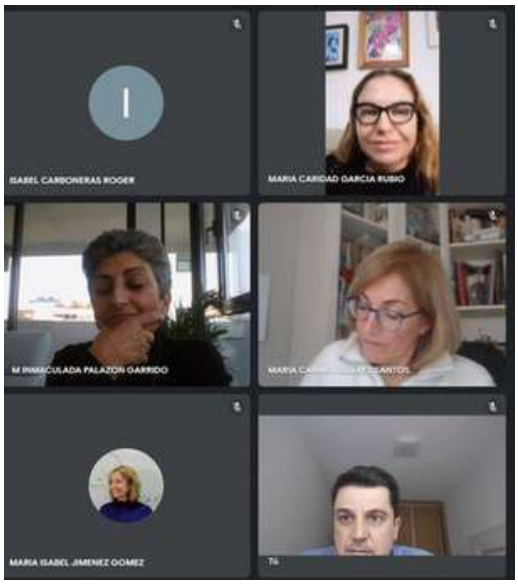
RESULTADOS

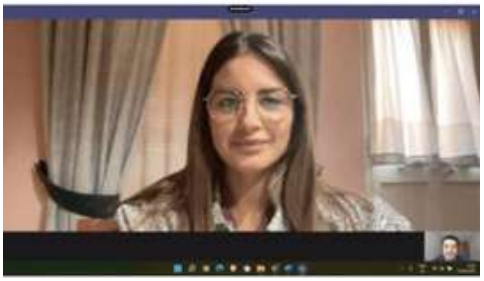
Jogo e animação ligados à cibersegurança na educação



Envolvimento da administração pública, escolas do EFP, especialistas de TI, professores, parceiro do projeto
Criação de pequenos vídeos

AEII / INERCIA DIGITAL [ES]





Em geral, após a realização de inúmeras pesquisas, o conhecimento de cibersegurança por parte de professores e alunos em centros de EFP ainda é reduzido em Espanha. Por este motivo, este projeto e outros idênticos são muito relevantes em Espanha.

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

GAME JAM

A NGO Nest Berlin, Extrafondente Open Source - EOS e IASIS realizaram uma sessão de Game Jam em fevereiro de 2022. A Game Jam teve início no sábado, dia 12, e durou 6 dias no total. As seleções nacionais desenvolveram e trabalharam em conjunto num rascunho de jogo (de um jogo online ou de tabuleiro).

Reuniu-se um júri independente a quem foi pedido que avaliasse o rascunho do jogo seguindo diretrizes comuns e um modelo de avaliação.

A equipa vencedora recebeu uma mentoria de 6 meses e recursos técnicos para desenvolver ainda mais a ideia do jogo.

SOBRE O JOGO

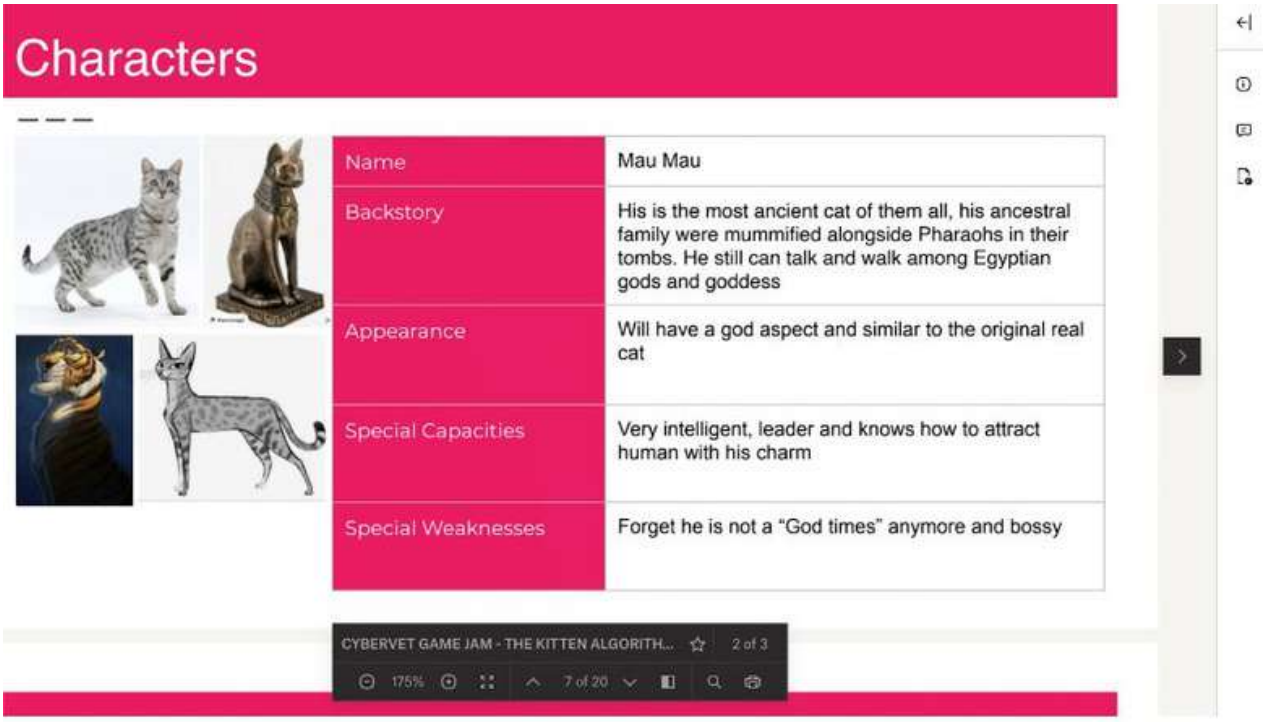
É um jogo de tabuleiro estratégico para 2 a 6 jogadores, que demora cerca de 30 a 60 minutos a ser jogado. Neste jogo, o jogador engana os humanos para os convencer de que é o melhor gato e ganha mais prestígio ao conseguir o maior número possível de servos de gatos humanos. Preste atenção, os outros gatos chefes tentarão ativamente sabotar o seu caminho para chegar aos humanos e ficarem eles com os louros. Não confie nas suas carinhas fofas!

O jogador perde o jogo se não tiver um número elevado de humanos como seus servos o se a 10ª rodada terminar e nenhum dos jogadores tiver, pelo menos, 4 humanos sob as suas ordens.

A dificuldade é que são 6 Chefes a tentarem enganar os humanos para serem seus servos e assim os chefes podem controlá-los, mas todos têm o mesmo objetivo e alguns podem até estar a ajudar os humanos a libertarem-se do controlo do gato.

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

Mau Mau



GAME JAM

O parceiro LECSA da Letónia organizou um evento Game Jam entre 27 de setembro e 1 de outubro de 2021. Devido às restrições epidemiológicas e diferentes localizações dos participantes, o evento foi organizado como um evento do tipo híbrido (presencial na Escola Técnica Saldus e via plataforma Zoom). Durante o evento, formaram-se 6 equipas (4-5 pessoas por equipa) para trabalharem no desenvolvimento de protótipos de jogos. Para alcançar alguns resultados tangíveis, o conceito Game Jam previu o desenvolvimento de dois tipos de jogos - jogos de computador e jogos de tabuleiro.

ATIVIDADES

Agosto - Setembro de 2021 foi dedicado ao planeamento e organização do evento (procura de especialistas em cibersegurança e desenvolvimento de jogos, distribuição de informações a potenciais participantes, planeamento da agenda e definição de critérios para o jogo, etc.)

Evento Multiplicador – Realidades nos Ciberataques (27.09.2021):
Introdução do projeto CYBER.EU.VET e palestra sobre as tendências nos ciberataques com Armins Palms, especialista em cibersegurança do CERT.LV (Instituto de Resposta a Incidentes de Segurança de TI da República da Letónia)
Número de participantes: 26 pessoas
Local: Escola Técnica de Saldus (cidade de Saldus) e plataforma ZOOM

Anúncio do Game Jam (27.09.2021): definição e discussão sobre os desafios reais em cibersegurança (avaliação de necessidades); formação de equipas, reunião com mentores e discussão sobre trabalhos futuros (workshop sobre o motor de jogo Unity), brainstorming sobre a ideia e o conceito do jogo.

Atividades de Game Jam em curso (28.09-30.09.2021): as equipas trabalharam no desenvolvimento de protótipos, sendo assegurada a consulta a mentores, se necessário

Apresentação do progresso (30.09.2021): apresentação sobre os conceitos do jogo e o progresso do trabalho para receber sugestões dos mentores.

Grande final (01.10.2021): quatro equipas apresentaram os seus resultados e os mentores avaliaram. Uma equipa, a desenvolver um jogo de computador, desistiu.
Conclusão do evento e discussão informal.
Número de participantes:
Local: Escola Técnica de Saldus e plataforma ZOOM

LECSA (LV)

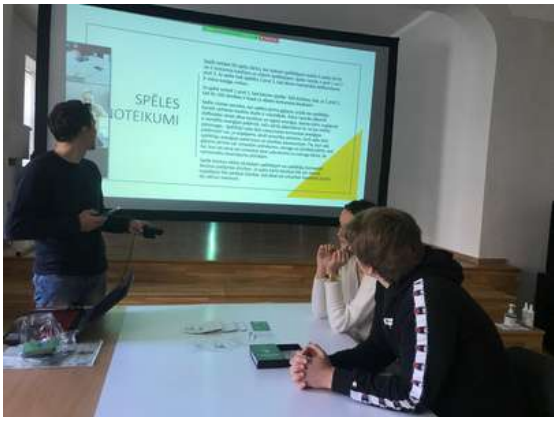
RESULTADOS

1.1. Protótipo de jogo online - The Virus

2. Jogo de tabuleiro - Cartas sobre segurança

3. Jogo de tabuleiro - Cyberwar

4.Jogo de cartas competitivo - Cyber Mind



EXEMPLO Cyber Mind - Um jogo de cartas competitivo

Este é um jogo de cartas educativo com elementos de questionário. A principal tarefa do jogo é ensinar os fundamentos da segurança quotidiana na Internet e aquilo que as pessoas se expõem quando fazem coisas tolas na Internet. Abrange tópicos como segurança na Internet e proteção de dados no contexto da utilização de redes sociais. No resultado do jogo, as pessoas (jogadores) devem ser capazes de reconhecer tentativas de fraude na vida real.

Desenvolvido pela equipa Veiksminieki (em letão: Pessoas de sucesso), alunos da Escola Técnica de Saldus durante o Game Jam na Letónia (outubro de 2021): Renars Ricards Hartmanis, Estere Ozoliņa, Sindija Diana Valtere e outros.

Nível: básico (para iniciantes). Grupo-alvo - alunos, estudantes, professores e pais

O jogo contém: 50 cartas, 2 blocos de saúde (para contar a saúde dos jogadores), 2 dados e carta de regras.

LECSA (LV)

GAME JAM

SOBRE

As tentativas de ciberataques em todo o mundo aumentam a cada dia que passa, como tal, o governo mundial teve a ideia de organizar um torneio para identificar pessoas que estão a trazer ciber-riscos e contra-atacá-las.

Jogo educativo que ajuda a aprender sobre os principais tipos de ciberataques, métodos de prevenção e eliminação, protegendo-se a si ou à sua equipa e contra-atacando o adversário. O objetivo do jogo é tirar todas as vidas do(s) adversário(s).

COMO JOGAR - JOGOS + REGRAS

Número de jogadores: 2 ou 4 pessoas (1 contra 1 ou 2 contra 2).

Cada jogador ou equipa (quando 2 contra 2) tem "100 vidas" (Saúde=HP) no início do jogo. A contagem da saúde é feita recorrendo a blocos de anotações pretos ou outras notas disponíveis.

Nomear uma pessoa para acompanhar e calcular o consumo de energia e saúde dos jogadores, se possível. Caso contrário, os jogadores fazem isso sozinhos.

Cada jogador recebe 5 cartas. Se o jogo for jogado 2 contra 2, ambos os jogadores terão "uma mão comum" na equipa ou 10 cartas juntas.

Existem três tipos de cartas: Cartas de ataque (vermelhas), Cartas de escudo (amarelas) e Cartas de Vida ou de Cura (verdes).

O jogo é jogado em rodadas. O jogador/equipa que obtiver o maior número no dado inicia o jogo.

Cada carta custa energia. No início de cada rodada, o jogador lança 2 dados para definir uma Energia que está indicada no topo da carta (a azul). As cartas têm de ser jogadas para que não exceda a sua quantidade de energia lançada.

O jogador/equipa que inicia a rodada pode atacar (com Cartas de Ataque), proteger-se (Cartas de Escudo) ou adicionar vida (Cartas de Cura), e os segundos só podem usar cartas de Ataque e Escudo para minimizar a sua vulnerabilidade de vida.

Lembre-se de que o número máximo de vidas por jogador/equipa durante o jogo pode ser de 100 HP (por exemplo, se a soma de vidas e energia após a rodada totalizar 110 HP, o seu número de vidas permanece – 100 HP).

O jogo termina assim que um jogador/equipa ficar sem todas as vidas (0 vidas).

Se o jogo ficar sem cartas, terá de baralhar as cartas da pilha novamente.

LECSA (LV)

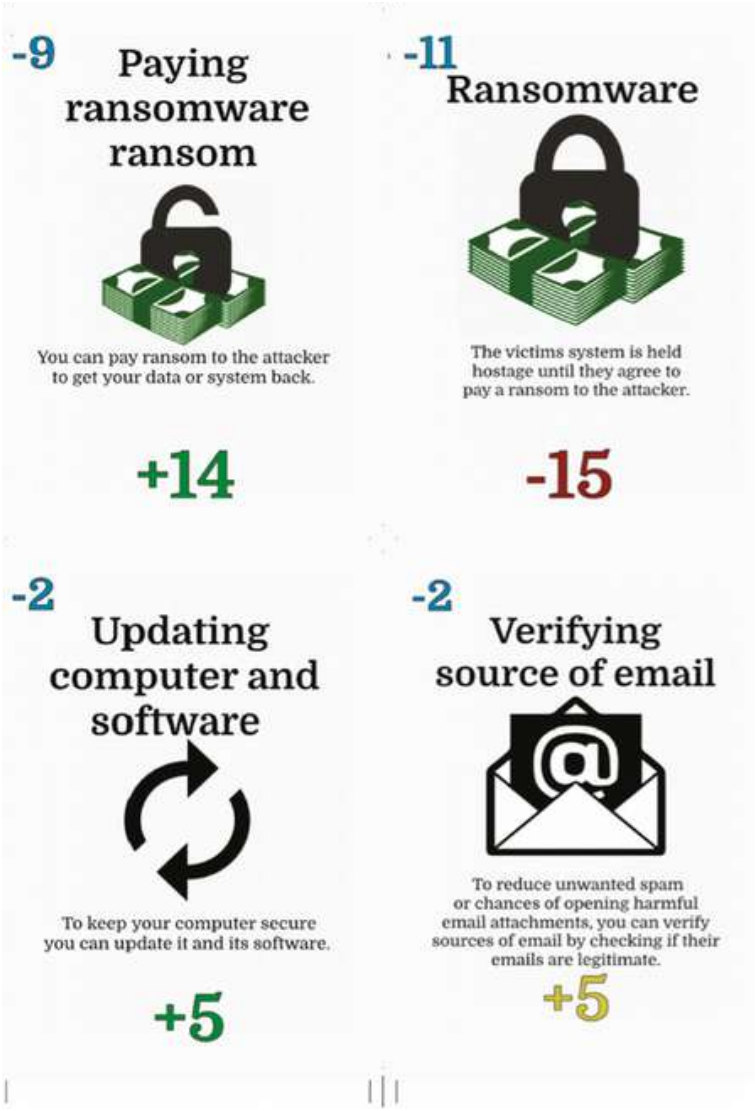
Exemplos de cartas

A **azul** – Energia

A **vermelho** - Cartas de ataque

A **amarelo** - Cartas de escudo

A **verde** - Cartas de cura



Exemplo para cálculo de saúde

EXEMPLO Cyberwar - Jogo de tabuleiro

Desenvolvido pela equipa Exodus (alunos da Escola Técnica de Saldus), líder da equipa Valdemārs Šperbergs.

2-6 jogadores< – > Adequado para maiores de 15

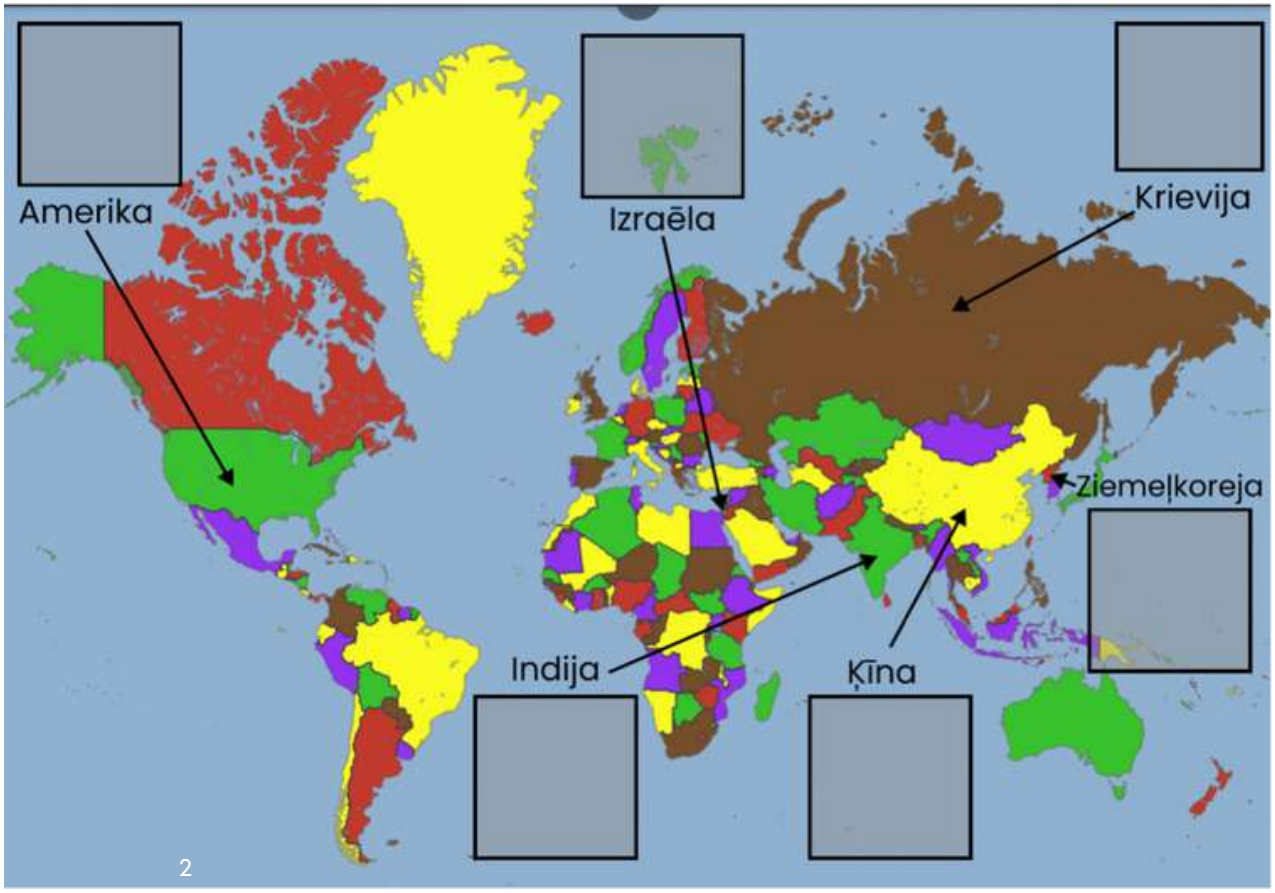
Um jogo de tabuleiro com uma forte ênfase em táticas e aleatoriedade (acaso).

Nível: jogo educativo para quem tem algum conhecimento sobre cibersegurança.

O jogo contém: Mapa-mundo, 2 dados, servidores, cartas com função "ataque", "defesa" ou "reação", legenda de vulnerabilidades.

SOBRE

O objetivo do jogo é proteger o país representado pelo jogador e atacar outros países para vencer a ciberguerra. No Cyberwar, cada jogador deve escolher um país para representar. Cada jogador tem um servidor com 3 vulnerabilidades. O objetivo do jogador é hackear servidores de outros países explorando duas das três vulnerabilidades ou corrigir duas das três vulnerabilidades no seu próprio servidor.



LECSA (LV)

COMO JOGAR

Os jogadores escolhem o país para representarem e colocam um objeto do servidor no local designado no mapa. Cada país tem os seus próprios bónus.

Cada jogador sorteia (pega) aleatoriamente 3 vulnerabilidades – uma de cada nível de dificuldade – e coloca-as viradas para baixo nos seus respetivos locais nos seus campos de servidor. As vulnerabilidades não são conhecidas pelos jogadores.

As vulnerabilidades têm 3 níveis de dificuldade. O nível de dificuldade também determina o número necessário para explorar uma vulnerabilidade (ver "Ataques"), assim como determina quantos movimentos serão necessários para corrigir a vulnerabilidade (ver "Defesa").

O jogo ocorre nas rodadas, as seguintes ações (movimentos) podem ser executadas – **Scanear, Ataque** e **Defesa**. Os jogadores determinam a sequência de jogadores lançando dois dados.

COMEÇAR

Cada jogador recebe 4 cartas no início de cada rodada. No fim da rodada, é possível manter 2 cartas ou trocá-las por outras já existentes.

A 1ª rodada é uma Rodada de Varredura na qual não é permitida nenhuma carta de Ataque ou Defesa. Nas rodadas posteriores, os jogadores podem optar por Scanear ou Atacar ou tentar reparar as suas vulnerabilidades (ver Defesa) O jogo continua rodada a rodada até que se alcance a vitória.

Scanear

O atacante escolhe um país para scanear a sua vulnerabilidade (por exemplo, "estou a scanear um segundo nível de vulnerabilidade russo").

Jogador scaneia – lança dois dados, aplicando o bónus do seu país representado, compara com o nível de dificuldade de vulnerabilidade + bónus do país da vítima.

Se o atacante tirar um número igual ou superior ao nível de dificuldade de vulnerabilidade da vítima, o atacante pode olhar para a vulnerabilidade scaneada.

Os bónus de país não são adicionados quando é o próprio a scanear.

Níveis de dificuldade

1º – o jogador deve tirar, pelo menos, o número 4 (excluindo os bónus do país)

2nd – player must roll at least 8 (excluding bonuses of the country)

3rd – player must roll at least 11 (excluding bonuses of the country).

ATAQUE

O jogador indica o alvo do ataque (por exemplo, "Eu ataco uma vulnerabilidade russa de nível 2") e revela a carta de ataque a todos os jogadores, colocando-a ao lado da vulnerabilidade.

O jogador lança o dado para ver se o ataque funciona comparando o número que tira com a dificuldade de vulnerabilidade + bónus (se o número tirado + bónus corresponder ou exceder a dificuldade, o ataque é bem-sucedido).

Os ataques podem ser forçados a recuar usando a Carta de Reação concebida para esse ataque. Cada ataque tem o seu próprio tipo de reação que pode ser jogado e o próprio tipo de vulnerabilidade para o qual funciona.

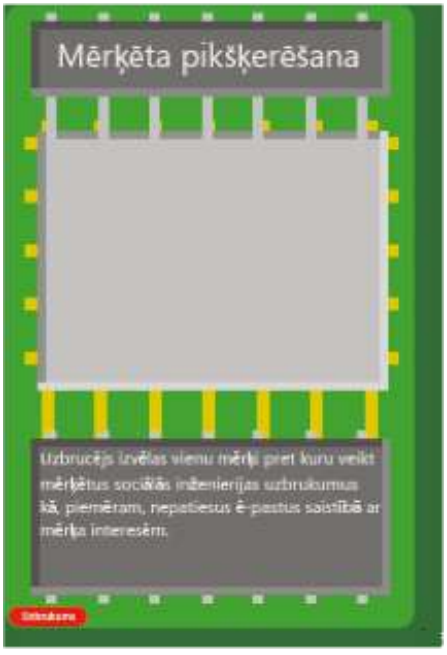
Se o ataque falhar ou for bloqueado por uma Carta de Reação - as cartas de Ataque e Reação jogadas permanecem na mesa até ao fim da próxima rodada e impedem o ataque por outros jogadores com o mesmo ataque pela mesma vulnerabilidade. Após a jogada, ambas as cartas voltam para o monte.

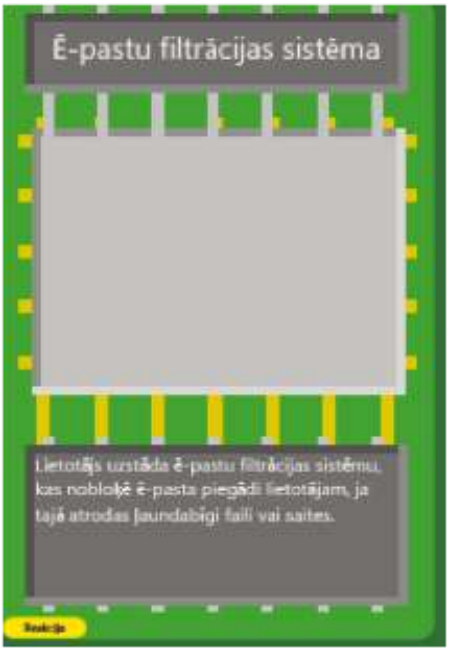
Níveis de dificuldade

1º – o jogador deve tirar, pelo menos, o número 4 (excluindo os bónus do país)

2º – o jogador deve tirar, pelo menos, 8 (excluindo os bónus do país)

3º – o jogador deve tirar, pelo menos, 11 (excluindo os bónus do país).





Defesa

Defesa – escolher o método certo contra uma vulnerabilidade específica. As Cartas de Reação param (cancelam) o ataque recebido (e todos os outros ataques direcionados à mesma vulnerabilidade) por 1 volta.

Para cancelar um ataque recebido, o jogador coloca uma Carta de Reação correspondente ao tipo de ataque (ver a tabela de vulnerabilidades) na carta de ataque
assim que o ataque é realizado.

Para começar a reparar um ferimento, o jogador coloca uma Carta de Defesa ao lado do ferimento a ser reparado.

Outros jogadores podem atacar este ferimento enquanto estiver na defesa (antes de a volta Defesa terminar). Quando o jogador tenta reparar um ferimento no seu servidor com uma Carta de Defesa, ele não pode atacar, mas pode tentar impedir ataques com Cartas de Reação. Para uma reparação completa, é necessário |nível de dificuldade + 1|
volta. A ação de scanear é permitida durante o período de reparação.

Se o método de defesa não for correto, o jogador salta 3 voltas e não pode usar cartas de defesa durante esse período (reações e ações de scanear são permitidas).

Bónus dos países

EUA: +2 scaneamento

Rússia: +2 para ataques

China: +2 para defesa contra ataques

Coreia do Norte: +2 para defesa contra scaneamento

Índia: +1 in all attacks, -1 against attacks

Israel: +3 em todos os ataques, -3 contra ataques

Vulnerabilities by levels

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

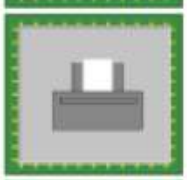
SQL injekcija ar filtru

Nepilnīgi nokonfigurēts ugunsmūris

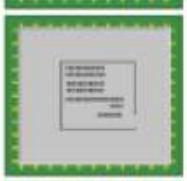
WiFi tīkls ar WEP drošību

Pakalpojuma atteices kļūda

Ievainojama OpenSSL programma



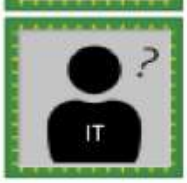
Ievainojama Print Spooler programma



Bufera pārpildes ievainojums

Vājš jaucējvērtības algoritms

Aizņemts priekšnieks



Slinks IT speciālists

LECSA (LV)

GAME JAM

DICAS E EXPERIÊNCIAS DA GAME JAM NA LETÓNIA

Durante o evento de 2 dias não é possível desenvolver um jogo de computador real, mas sim o primeiro protótipo, que poderá ou não ser desenvolvido dependendo da motivação dos participantes.

Prémios ou outros tipos de benefícios podem ajudar a envolver mais participantes e garantir melhores resultados (mais tangíveis) no fim (no nosso caso, pizza e bebidas foram fornecidas no fim do evento, apoio adicional dos mentores (por exemplo, colocando jogos na plataforma)).

Os mentores no desenvolvimento de jogos e questões de cibersegurança desempenham um papel importante na Game Jam, ao aconselhar e ajudar os participantes.

Planear com antecedência – pois este é um evento bastante complexo e requer um planeamento cuidadoso. Os organizadores devem ter em conta que algumas equipas podem ficar fora da competição (devido ao tempo limitado).

Por favor, ver as publicações do FB com os resultados do evento:
https://www.facebook.com/cybereuvetproject.eu/posts/138127645211214
https://www.facebook.com/saldustehnikums/posts/1780232175520378

O evento foi organizado pela LECSA em colaboração com Latvijas Universitāte | Ekonomikas un kultūras augstskola / EKA University of Applied Sciences | McĀbols | cert.lv | Coldwild Games | Saldus tehnikums!

MEATH PARTNERSHIP (IE)

ATIVIDADES

Reunião de informação de avaliação de necessidades com os alunos (formação de codificação numa instituição local de ensino de adultos)

Game Jam de 2 dias (sessão de informação online no 1º dia; 2º dia dedicado à Game Jam)

Evento Multiplicador – Manhã de Sensibilização para a Cibersegurança

DESCRIÇÃO E RESULTADOS

1) 1) Reunião de informação de avaliação de necessidades com os alunos
(Formação de codificação numa instituição local de ensino de adultos) Data: Outubro 2021

DESCRIÇÃO

Com o objetivo de disseminar o projeto e identificar os principais temas para a Game Jam, a equipa da Meath Partnership organizou uma sessão de informação com os alunos de uma turma de formação de Codificação local. A partilha de informações sobre Cibersegurança e discussão sobre as ameaças mais recentes foi seguida de uma sessão de brainstorming em grupo na qual os alunos foram divididos em dois grupos com vista a discutirem questões que levassem à identificação dos temas mais interessantes a explorar durante a Game Jam. Mais informações sobre a Game Jam e o projeto CYBER.EU.VET também foram partilhadas com os participantes do dia.

EXEMPLO PARA AVALIAÇÃO


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)

RESULTADOS

Como resultado desta atividade, a equipe da Meath Partnership obteve uma maior compreensão do conhecimento geral dos alunos em relação à cibersegurança e ciberameaças, assim como informações recolhidas que foram posteriormente incluídas no processo de planeamento e implementação da Game Jam.

AVALIAÇÃO EM AÇÃO

MEATH PARTNERSHIP (IE)

GAME JAM

2) Game jam de dois dias
(sessão de informação online no 1º dia; 2º Dia dedicado à Game Jam)

DESCRIÇÃO

O DIA 1 foi dedicado às boas-vindas aos participantes e apresentação do projeto CYBER.EU.VET e à abertura da Game Jam, assim como à partilha de informações sobre os 2 temas identificados durante a reunião de avaliação de necessidades. Aos participantes foram oferecidas opções para trabalharem individualmente ou como parte de uma equipa. Também tiveram a oportunidade de tirar dúvidas ou ouvir mais esclarecimentos sobre os procedimentos
relacionados com o desenvolvimento dos jogos no dia 2.

O DIA 2 foi dedicado ao desenvolvimento dos jogos e os membros da nossa equipa e um especialista em suporte de TI estiveram disponíveis via Zoom para apoiar os participantes durante toda a duração da Game Jam entre as
9h e as 21h.
Os participantes foram convidados a fazerem o upload dos seus jogos na plataforma Itchio através de um perfil criado para efeitos deste evento: CYBER.EU.VET : Cybersecurity Game Jam - itch.io

RESULTADOS

Depois de os participantes partilharam os seus rascunhos de jogos com a equipa, um participante decidiu avançar e fazer o upload do jogo para uma avaliação mais aprofundada. Os restantes participantes decidiram não submeter os seus rascunhos, pois estavam em fases muito iniciais.

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

Online interactive cybersecurity game:
https://itch.io/jam/cybereuvet-cybersecurity-gamejam

MEATH PARTNERSHIP (IE)

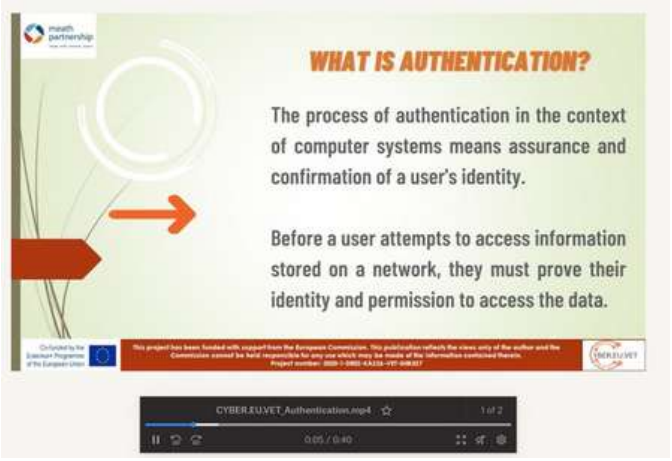
3) Evento Multiplicador – Manhã de Sensibilização para a Cibersegurança
Data: Novembro 2021

DESCRIÇÃO

O Evento Multiplicador foi realizado online Via Zoom com o objetivo de divulgar o projeto e as suas atividades. O evento foi amplamente divulgado entre as mais diversas partes interessadas ou envolvidas em Cibersegurança. O evento começou com uma apresentação e visão geral do projeto e do Game Jam, seguindo-se uma apresentação e discussão sobre Cibersegurança e partilha de informações práticas sobre como se manter online (foram possíveis as atuais ciberameaças e como eliminar possíveis ataques).

RESULTADOS

O Evento Multiplicador contribuiu para a divulgação do projeto e também criou a oportunidade de apresentar as concretizações alcançadas desde o início do projeto a um público mais alargado. Foi também uma grande oportunidade de partilhar informações práticas e conselhos relacionados com a cibersegurança com os participantes no evento.



COFAC / UNIVERSIDADE LUSÓFONA (PT)

GAME JAM

ATIVIDADES

1) Pós-graduação em Cyber & Ethical Hacking para futuros profissionais e professores no mercado Out 2021 – Fev 2022 (em parceria com uma consultora local chamada Cybersec Cybersec)

2) 2 sessões de Game Jam realizadas em janeiro de 2022 em escolas do EFP: Escola de Comércio de Lisboa :

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

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

3**)** Uma ciberformação de três dias e meio para alunos do ensino secundário em março de 2022 na Universidade Lusófona como parte do evento Tecweb - https://tecweb.ulusofona.pt

RESULTADOS

Evidência de relatório de divulgação onde se podem ver os diferentes testes que foram realizados durante um ano civil (abril de 2021 a abril de 2022). Neste relatório, podemos ver screenshots de publicações nas redes sociais, cartazes de diferentes eventos, questionários de sensibilização para a cibersegurança (disponíveis em português em https://docs.google.com/forms/d/e/1FAIpQLSeXACV_oeplRpTfbaC1NFKED76kRSYD6cT8cFMKjc7ohGMHZw/viewform)

DDurante os Cyberjams, também se criou, com base nos inquéritos de sensibilização para a cibersegurança, um conjunto de minijogos interativos/simples para o utilizador sobre situações simples realizadas.

TANDEM PLUS NETWORK – MEMBER IASIS [GR]

GAME JAM

Ferramenta de desenho de jogos (IASIS) - Cyberopolis

Este jogo é um jogo de tabuleiro destinado a pessoas interessadas em cibersegurança, com um máximo de 2 a 4 jogadores, e os seus principais aspetos são a confidencialidade e a integridade dos dados... e os tópicos abordados são o malware, phishing, ataques baseados na web, ataques de aplicações da web, spam, roubo de identidade, DDoS e Man in the middle...

Ver a imagem de ''Cyberopolis'' para compreender melhor os passos a seguir durante o jogo e quais os desafios a serem resolvidos...

Screenshots do jogo durante a sessão de Game Jam onde podemos ver o sucesso do jogo e o grande interesse demonstrado pelos participantes.

TANDEM PLUS NETWORK – MEMBER IASIS [GR]

VÍDEO - Preventing Cyberbullying

Este vídeo desenvolvido pelo parceiro grego aproxima os visitantes de diferentes formas de prevenir e combater o ciberbullying.

YBER.EU.VET

Funded by the European Union

AVISO LEGAL

Desenho
NGO Nest Berlin e.V.
Berlim, 2022

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