TREĆA NACIONALNA KONFERENCIJA NKS-a

KIBERNETIČKA SIGURNOST

ČOVJEK U SREDIŠTU

NKS NACIONALNO KOORDINACIJSKO SREDIŠTE

CARNET

CADMUS

Cultivating Cybersecurity Defence Expertise with Mindful Readiness and Skills

IQ DEFENCE

Humans as intelligent shield against cyber threats

Tomislav Dominković
Sveučilište Algebra Bernays

ALGEBRA

Osnovne informacije

- **Program financiranja**: Digital Europe
- **Trajanje**: 36 mjeseci (3 godine)

	CADMUS	IQ DEFENCE
Vremenski okvir	12/2024-11/2027	1/2026-12/2028
Vrijednost projekta	~6,3 mil EUR	~4,1 mil EUR
Članovi konzorcija	7	2

Co-funded by the European Union

CADMUS project has received funding from the DIGITAL-2023-SKILLS-05-CYBERACADEMY under Grant Agreement No. 101190006.
The Digital Europe Programme funds IQ Defence (Grant Agreement No. 101249724) under the call DIGITAL-ECCC-2024-DEPLOY-CYBER-07.

ECCC EUROPEAN CYBERSECURITY COMPETENCE CENTRE

IQ DEFENCE project funded under Grant Agreement No. 101249724 is supported by the European Cybersecurity Industrial, Technology and Research Competence Centre (ECCC)

O projektu IQ DEFENCE

- **Cilj**: podržati ključne i važne organizacije, uključujući mala i srednja poduzeća i javna tijela, kao i kreatore politika i tijela za nadzor tržišta iz država članica EU-a, u značajnom unapređenju pripravnosti za kibernetičku sigurnost, usklađenosti s regulativom (NIS2, CRA) i operativne otpornosti..
- **Ciljane skupine:**
  - Ključni i važni subjekti (u okviru NIS2 direktive)
  - Mala i srednja poduzeća i sudionici opskrbnog lanca
  - Javna tijela i tijela za nadzor tržišta
  - CSIRTs and stručnjaci za odgovor na incidente
  - Obrazovne institucije i tijela nadležna za kvalifikacije
  - Građani koji žele unaprijediti svijest o kibernetičkoj sigurnosti

Rezultati

1. Informativni materijali o zahtjevima NIS2 i CRA regulative te najboljim praksama provedbe (brošure, smjernice, plakati, studije slučaja, online edukacije) - BESPLATNO
2. E-tečajevi o NIS2 i CRA regulativi (na 24 EU jezika) - BESPLATNO
3. 12+ novih standarda zanimanja i kvalifikacija usklađenih s ECSF-om (razvila ENISA)
4. Video kampanje za podizanje svijesti - BESPLATNO
   a) Podizanje svijesti o najčešćim kibernetičkim prijetnjama (10 videa)
   b) Promicanje karijera u području kibernetičke sigurnosti (12 videa)
5. Edukacija i certificiranje predavača o NIS2 i CRA regulativi
6. Konferencije na temu kibernetičke sigurnosti - BESPLATNO
7. Kibernetičke vježbe temeljene na scenarijima sa sudjelovanjem stručnjaka iz različitih zemalja
8. Online koordinacijski sastanci te seminari i radionice uživo za razmjenu znanja i iskustava u procesima prenošenja i provedbe NIS2 i CRA regulative na razini EU-a

Ideje za brošure i smjernice (6)

1. **NIS2 u praksi: Na koga se odnosi i što se mijenja?**
   - Uvodni materijali koji objašnjavaju područje primjene, obveznike i ključne organizacijske promjene.
2. **NIS2 odgovornosti: Što menadžment mora znati?**
   - Fokus na upravljanju, odgovornosti menadžmenta, internim odgovornostima i ulozi vodstva u usklađenosti sa zahtjevima kibernetičke sigurnosti.
3. **Upravljanje rizicima prema NIS2: od usklađenosti do stvarne otpornosti**
   - Objašnjava pristup temeljen na rizicima, procjenu rizika, određivanje prioriteta i upravljanje kibernetičkim rizicima.
4. **Izvještavanje o incidentima prema NIS2: što učiniti kada nešto pođe po zlu**
   - Obuhvaća prepoznavanje incidenata, eskalaciju, odgovor na incidente, dokumentiranje i obveze izvještavanja.
5. **NIS2 i sigurnost opskrbnog lanca: najslabija karika vaše organizacije može biti vanjska**
   - Fokusira se na ovisnosti o trećim stranama, rizike povezane s dobavljačima, sigurnosne zahtjeve u nabavi i vanjsku izloženost.
6. **NIS2 spremnost: 10 praktičnih koraka za početak provedbe**
   - Pruža jednostavan i praktičan plan za organizacije koje započinju proces usklađivanja s NIS2 direktivom.

Ideje za seriju videa o podizanju svijesti o kibernetičkoj sigurnosti (10)

1. **Hitna poruka: opasan klik –** budite oprezni s phishingom i zlonamjernim poveznicama.
2. **Jedna lozinka, mnogo problema –** slabe lozinke i upotrebljavanje istih lozinki.
3. **Ljubazni pozivatelj –** socijalni inženjering putem telefona.
4. **Predobro da bi bilo istinito** – lažne internetske trgovine i prevare pri plaćanju.
5. **Besplatan Wi-Fi, skriveni rizik** – nesigurno korištenje javnih ili nezaštićenih Wi-Fi mreža.
6. **Jedan klik do potpune blokade** – neoprezno preuzimanje datoteka ili otvaranje privitaka može pokrenuti ransomware napad.
7. **Dijeljenje previše informacija** – prekomjerno dijeljenje sadržaja na društvenim mrežama.
8. **Ukradeno bez dodirivanja novčanika** – krađa identiteta i zlouporaba osobnih podataka.
9. **Pametan uređaj, nesigurna postavka** – nesigurno korištenje pametnih kućnih uređaja.
10. **Poruka od prijatelja** – lažne poruke poslane od poznatih kontakata.
11. **Ažuriraj kasnije, požali ranije** – rizici ignoriranja ažuriranja softvera i aplikacija
12. **USB iznenađenje** – rizici korištenja nepoznatih prijenosnih medija.
13. **Ekran u javnosti, podaci u javnosti** – škicanje preko ramena i neoprezno ponašanje u javnim prostorima.

Ideje za online edukacije (6)

NIS2

1. Upravljanje, odgovornost i upravljanje imovinom
2. Procjena i upravljanje kibernetičkim rizicima
3. Upravljanje incidentima i izvještavanje o njima
4. Sigurnost opskrbnog lanca i upravljanje rizicima povezanima s trećim stranama

CRA

1. CRA osnove: regulatorni zahtjevi za proizvode s digitalnim elementima.
2. Siguran životni ciklus proizvoda i upravljanje ranjivostima u skladu s CRA regulativom.

IQ DEFENCE kontakti i informiranje

CADMUS

Katalog treninga planiran za razvoj

Security Awareness

- Course Description

  E-tečaj za samostalno učenje koji uvodi temeljna načela kibernetičke higijene i sigurnog digitalnog ponašanja. Polaznici uče kako prepoznati online prijetnje, zaštititi račune, izbjeći phishing, koristiti sigurne lozinke, primijeniti višestruku autentifikaciju (MFA) i sigurno rukovati podacima u svakodnevnim aktivnostima.

- Ciljevi učenja
  - Objasniti važnost kibernetičke higijene u svakodnevnim digitalnim aktivnostima.
  - Prepoznati uobičajene kibernetičke prijetnje i nesigurna ponašanja.
  - Primijeniti snažne prakse zaštite lozinki, višestruke autentifikacije i računa.
  - Prepoznati pokušaje krađe identiteta (phishing), socijalnog inženjeringa i online prijevara.
  - Usvojiti načela sigurnog pregledavanja i sigurnog rukovanja podacima.
  - Prepoznati kibernetičke prijetnje i reagirati na odgovarajući način.

Cyber Range vježbe (samostalno)

- Network and OS Security Hardening
  - Basics of Security Hardening of Networking Devices
  - Advanced Layer 2 Switching and Security Strategies
  - Advanced Layer 3 Security Hardening and Traffic Control
  - Firewall Configuration and Security Management
  - Linux OS Security Hardening and Compliance Validation
  - Windows OS Security Hardening and Active Directory Defence
  - Android Device Security and Hardening
- Business Continuity & Disaster Recovery
  - Business Continuity Planning and Resilience Simulation
  - Disaster Recovery Operations and Technical Restoration

Cyber Range vježbe (samostalno)

- Secure Coding
  - Secure Coding C/C++
  - Secure Coding .Net/C#
  - Secure Coding Java
  - Secure Coding Python
  - Secure Coding Mobile
- Penetration Testing
  - Network Penetration Testing
  - WEB Application Penetration Testing
  - Operating Systems Penetration Testing
  - Mobile/OT Penetration Testing

Cyber Range vježbe (samostalno)

- Incident Responce
- Digital Forensics Investigation and Evidence Handling
- Advanced Digital Forensics and Incident Response

- Denial of Service (DoS)
- Post-Quantum_Cryptography

Malware Analysis and Reverse Engineering

- Online self-paced courses
  - Introduction to malware detection
  - Malware analysis, detection and threat intelligence
  - Reverse Engineering
  - Introduction to Purple Team Operations

  - OT/ ICS Security
  - HW Hacking

Serious Games and TTX

- Serious Games:
  - Defend the Hospital (feb-27)
  - Cyber Crisis Leadership Challenge (jan-27)
  - Post-Quantum Cryptography Transition Knowledge (jun-26)
- TTX:
  - Incident Response – Cross-Functional Crisis (jun-26)
  - Public Sector Ransomware Crisis (mar-26)
  - Critical Infrastructure Incident Response (feb-27)
  - Cybersecurity Crisis Management for Public Authorities (jun-26)
  - Asset & Risk Management – Organisational Exposure Assessment (dec-26)
  - Cyber Security Audit Simulation & Compliance Review (jul-26)
  - Implementing Cryptography Correctly (feb-27)

SG scenariji repliciraju realne organizacijske krize koje zahtijevaju od sudionika da procijene nadolazeće informacije, uravnoteže tehnička i poslovna ograničenja, upravljaju dionicima i jasno komuniciraju rizike.

TTX nadopunjuju SG igre pružanjem strukturiranih simulacija vođenih raspravom koje se usredotočuju na usklađenost, koordinaciju, upravljanje, operativnu strategiju i odgovor na krize na organizacijskoj i među-agencijskoj razini.

CADMUS kontakti i informiranje

Mikrokvalifikacije uz HZZ vaučer

- Sigurnost informacijskih sustava (CompTIA Security+)
- Strategije i prakse kibernetičke sigurnosti (CISO)
- Primjena SOC-a u prevenciji i analizi kibernetičkih napada
- Digitalna forenzika
- Primjenjivanje tehnika etičkog hakiranja (EC-Council C|EH)
- Implementiranje sigurnosti u oblaku (Microsoft Azure)

Hvala na pažnji.