VARNOST ORGANIZACIJ

UČNI NAČRT PREDMETA/COURSE SYLLABUS

Predmet:	Varnost organizacij
Course title:	Organisation Security
Članica nosilka/UL Member:	UL FRI

Študijski programi in stopnja	Študijska smer	Letnik	Semestri	Izbirnost
Računalništvo in informatika, prva stopnja, visokošolski strokovni (v postopku)	Ni členitve (študijski program)		1. semester	izbirni

Univerzitetna koda predmeta/University course code:	0643424
Koda učne enote na članici/UL Member course code:	63773

Predavanja /Lectures	Seminar /Seminar	Vaje /Tutorials	Klinične vaje /Clinical tutorials	Druge oblike študija /Other forms of study	Samostojno delo /Individual student work	ECTS
45	30				105	6

Nosilec predmeta/Lecturer:	David Modic
Vrsta predmeta/Course type:	izbirni-strokovni/elective-vocational

Jeziki/Languages:	Predavanja/Lectures:	Angleščina, Slovenščina
	Vaje/Tutorial:	Angleščina, Slovenščina

Pogoji za vključitev v delo oz. za opravljanje študijskih obveznosti:	Prerequisites:
Vpis v letnik.	Enrollment in the study year.

Vsebina:	Content (Syllabus outline):

Vsebina predavanj:
Predmet se osredoča na praktične vidike informacijske varnosti v gospodarstvu, od malih do srednjih in večjih podjetij. Vse krovne vsebine navedene v tem učnem načrtu so del ACM CyberSecurity kurikula iz leta 2017 (sekcije 4.7 Organisational Security, ss.59-77) .
• Organizacijske strukture
  • Vloge varnostnega osebja in hierarhija odločanja s praktičnimi primeri,
  • Potek dela pri odzivanju na incidente.
• Upravljanje s tveganji v praksi
  • Praktični primeri vodenja incidentov
  • prepoznavanje in modeliranje groženj
  • Manjšanje tveganj v praksi.
	Module contents:
	The course adressess practical aspects of information security in the private sector, spanning from SME to large enterprises. All main topics listed in this syllabus are part of the 2017 ACM CyberSecurity curriculum (Knoweldge Area 4.7 Organisational Security, pp.59-77).
	• Organisational structures
	  • Security roles in a Company and hierarchy of response, with practical examples
	  • Incident response workflow
	• Risk Management
	  • Practical examples of workflow.
	  • threat identification and threat modelling
	  • Mitigation in practice

• Praktični postopki (povratna zanka, komuniciranje, srebrne ekipe, VOC). • Varnostno upravljanje in politika • Standardi (npr. ISO 27001) in varnostne smernice. • Struktura in težave povezane z varnostnimi politikami (nepoznavanje, neinformiranost, neživljenskost) • Zasebnost • Praktična uporabnost, zahteve podjetij proti zasebnim; • Zasebnost v praksi (npr. pri razvoju programske opreme). • Etika varnosti v praksi. • Analitična orodja in analitika • Orodja, pregled in osnove uporabe v praksi. • Običajne zbirke in načini zbiranja (IDS, SOC, netflow logs ...). • Zbiranje, analiza in razširjanje varnostnih obveščevalnih podatkov • Pasti zbiranja obveščevalnih podatkov • Pregled nekaterih orodij za zbiranje obveščevalnih podatkov (Shodan, Google, Spiderfoot, Maltego ...) • Varnost zaposlenih v praksi • Varnostno ozaveščanje, usposabljanje in izobraževanje • Fizično varovanje (stroji, pisarne, brskanje po smeteh itd.)	• Practical application (feedback loops, communication, silver teaming, SOC). • Security Governance & Policy • Standards (e.g. ISO 27001) and policy structure • Pitfalls of Security Policy (ignorance, lack of information, questionable usefulness). • Privacy • Practical uses, business considerations vs. personal ones. • Practical application (e.g. in software development). • INFOSEC and ethics • Analytical Tools and analysis • Tools (Overview and practical use (basics). • What data is expected and how is it gathered (IDS, SOC, netflow logs...). • Security intelligence collection, analysis, and dissemination of security information • Pitfalls of intelligence gathering • Overview of some intelligence gathering tools (Shodan, Google, Spiderfoot, Maltego...) • Personnel Security • Security awareness, training and education • Physical security (machines, offices, dumpster diving, etc)

Temeljna literatura in viri/Readings:

Anderson, R. (1994). Liability and computer security: Nine principles. In D. Gollmann (Ed.), Computer Security — ESORICS 94 (Vol. 875, pp. 231-245): Springer Berlin Heidelberg.

Anderson, R. (2021). Security Engineering: A Guide to Building Dependable Distributed Systems (3rd ed.). Indianapolis: John Wiley and Sons. ISBN: 978-1119642787**.**

Anderson, R., Barton, C., Böhme, R., Clayton, R., van Eeten, M., Levi, M., . . . Savage, S. (2012). Measuring the Cost of Cybercrime. Paper presented at the 11th Annual Workshop on the Economics of Information Security WEIS 2012, Berlin, Germany.

Banoth, R., Gugulothu, N., & Godishala, A. K. (2023). A comprehensive guide to information security management and audit, CRC Press, Boca Raton:USA. ISBN: 9781003322191

HM Government. (2013). Emergency Response and Recovery: Non statutory guidance accompanying the Civil Contingencies Act 2004. London, UK: UK Government Retrieved from https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/253488/Emergency_Response_and_Recovery_5th_edition_October_2013.pdf.

International Organization for Standardization. (2013). Information technology — Security techniques — Information security management systems — Requirements (ISO / IEC 27001) (pp. 30). Geneva, Switzerland: ISO copyright office.

Matherly, J. (2016). The Complete Guide to Shodan: Collect. Analyze. Visualize. Make Internet Intelligence Work For You: Amazon.

Cilji in kompetence:	**Objectives and competences:**
Cilji predmeta so: • Študente v grobem seznaniti s standardi, organigrami, storitvami in vpetostjo varnostne infrastrukture v podjetjih. • Omogočiti študentom zmožnost sodelovanja pri procesih identifikacije tveganj, njihovega	The goals and core skills of the module are to: • familiarize students with Standards, organizational charts, services and integration of the security infrastructure in Businesses.

omejevanja, prepoznavanja groženj, ter militve tveganj. • Študentom nuditi potrebna predznanja, da bodo lahko pričeli s samostojnim delom v podjetjih ter pri tem upoštevali varnostne politike in principe gradnje varnosti od temeljev naprej. • Nuditi okvirno razumevanje pravnih, etičnih in strateških smernic, ki so nujne za ohranjanje varnosti podjetij	• Empower students with the ability to participate in the processes of identifying and limiting risks, identifying threats, and risk mitigation. • To provide students with the necessary background knowledge enabling them to start working independently in SME's, taking into account security policy and principles of architecting security from the ground up. • Provide basic understanding of the legal, ethical and strategic frameworks necessary to maintain Companies secure.

Predvideni študijski rezultati:	**Intended learning outcomes:**
Po uspešno zaključenem predmetu bodo študenti zmožni: • Prepoznavati svojo vlogo v podjetju in samostojno poskrbeti, da jo izpolnjujejo varno, v okvirih zakonov, etike in smernic podjetja. • Razumeti proces ocenjevanja in omejevanja tveganj, ter pri njem sodelovati v okviru svoje vloge v podjetju. • V grobem razumeti in slediti etičnim in internim smernicam, ter varnostni politiki podjetja. • Bolje prepoznavati posebnosti varovanja zasebnosti in bolje skrbi zanjo. • Izpeljati osnovno analizo podatkov in zbirati informacije potrebne za krizni odziv in večanje varnosti podjetij. • Prepoznavati široko paleto tveganj, ki so jim podjetja izpostavljena (od globalnih, infrastrukturnih, do lokalnih in človeških vektorjev napada).	The goals and core skills of the module are to: • familiarize students with Standards, organizational charts, services and integration of the security infrastructure in Businesses. • Empower students with the ability to participate in the processes of identifying and limiting risks, identifying threats, and risk mitigation. • To provide students with the necessary background knowledge enabling them to start working independently in SME's, taking into account security policy and principles of architecting security from the ground up. • Provide basic understanding of the legal, ethical and strategic frameworks necessary to maintain Companies secure. • Recognize their role in a Business, and with less oversight ensure that their tasks are completed securely, within the judicial framework, Ethics and Company policies. • Understand the process of risk assessment and limitation. They will be able to participate in these processes within their Company role. • Roughly understand and adhere to Ethical and internal guidelines, as well as the Company's security policy. • Better recognize the peculiarities of privacy protection and take better care of it. • Perform basic data analysis and collect information necessary for crisis response and Company security hardening. • Recognize the wide range of risks that companies are exposed to (from global, infrastructural, to local, and human attack vectors).

Metode poučevanja in učenja:	**Learning and teaching methods:**
Predavanja, praktične vaje in demonstracije, projektni način dela pri seminarjih in vajah.	Lectures, lab work, home assignments, project work.

Načini ocenjevanja:	**Delež/Weight**	**Assessment:**
Način (pisni izpit, ustno izpraševanje, naloge, projekt)		Type (examination, oral, coursework,project)

Sprotno preverjanje (domače naloge, projektno delo)	50,00 %	Continuous (home assignments, project work)
Končno preverjanje (pisni izpit)	25,00 %	Final (written exam)
Končno preverjanje (ustni izpit)	25,00 %	Final (oral exam)
Ocene: 6-10 pozitivno, 5 negativno (v skladu s Statutom UL).		Scale: 6-10 pass, 5 and below fail (According to the rules and ordnances of the University of Ljubljana).

Reference nosilca/Lecturer's references:

Modic, D. (2022). Do Not Distract Me While I Am Winning This Auction: The Psychology of Auction Fraud. In Y. Hanoch & S. Wood (Eds.), A Fresh Look at Fraud: Theoretical and Applied Perspectives (1 ed., pp. 240). London, UK: Routledge.

Modic, D., & Ciglarič, M. (2020). Ali sploh znamo pravilno komunicirati? Glas Gospodarstva, 5, 22-23.

Modic, D., Mittig, K., & Ciglarič, M. (2019). Behind The Mask: Classification Of Unauthorized Intruders Into Computer Systems [under review]. Human Computer Interaction, 31.

Modic, David, Anderson, Ross in Palomäki, Jussi. (2018). We Will Make You Like Our Research: The Development of a Susceptibility-to-Persuasion Scale. *PLOS ONE, 13*(3), e0194119. doi: 10.1371/journal.pone.0194119

Modic, David in Anderson, Ross. (2015). It's All over but the Crying: The Emotional and Financial Impact of Internet Fraud. *IEEE Security & Privacy, 13*(5), 99-103. doi: 10.1109/MSP.2015.107

Modic, David in Anderson, Ross. (2014). Reading This May Harm Your Computer: The Psychology of Malware Warnings. *Computers in Human Behavior, 41*, 71-79. doi: 10.1016/j.chb.2014.09.014