

בית הספר למוסמכים במינהל עסקים ע"ש ליאון רקנאטי

1242.3282.01 – אבטחת סייבר למנהלים

Cybersecurity for Managers

(ללא דרישות קדם)

סמסטר א' – תשפ"ב – מחצית ראשונה

קבוצה	יום בשבוע	שעה	תאריך בחינה	מרצה	דואר אלקטרוני	טלפון
01	א'	18:45-21:30	בהתאם ללוח הבחינות	ד"ר יעקב מנדל	jacob4x4@gmail.com	054-4547369

שעת קבלה – בתיאום מראש

עוזר הוראה: ד"ר רפי הוד rhod@tau.ac.il

היקף הלימודים

היקף הי"ס לקורס: 1

ECTS = 4 ECTS י"ס – (European Credit Transfer and Accumulation System), ערך הניקוד של הקורס במוסדות להשכלה גבוהה בעולם שהינם חלק מ"תהליך בולוניה".

תיאור הקורס

מטרת הקורס לפרוס את העולם הטכנולוגי של הסייבר על מרכיביו השונים. נקודות החוזק ונקודות התורפה, מטרות האבטחה בסייבר, מבנה מחשבים ורשתות תקשורת, מגבלותיהם ופגיעותם. הקורס סוקר היבטים טכנולוגיים בהתפתחותה ומודל פעולתה של רשת האינטרנט, פרוטוקולים, רשת ה-WEB והסכנות שבה, מחשוב ענן והאתגרי הסייבר הכרוכים בו, יסודות וכלים קריפטוגרפיים, תקיפות נפוצות, תשתיות תקיפה ומערכות הגנה.

במהלך הקורס הסטודנטים ילמדו והתנסו עם ארועים מורכבים, הבנת הכלים והטכנולוגיות להתמודדות עם השאלות העסקיות והאתגרים הניהוליים בעידן הדיגיטלי. הקורס עוסק בלימוד וניתוח תוך התמקדות בניהול טכנולוגיות בסביבה דינאמית. במהלך הקורס נסקור בעיות ואתגרים עסקיים וניהוליים מתחומים שונים, מהתעשייה והאקדמיה ונדון בדרכים להתמודדות באתגרי הסייבר של האירגונים.

הקורס מיועד לסטודנטים מתחומים שאינם טכנולוגיים, עם זאת הוא טכנולוגי במהותו. בקורס נסקור את ההיבטים הטכנולוגיים של עולם הסייבר ומרכיביו השונים. חוזק וחולשה עיקריים, יעדי אבטחת סייבר, כלי קריפטוגרפיה בסיסיים, מבנה מחשבים ורשתות תקשורת, כמו גם מגבלותיהם ופגיעותיהם.

הקורס מבוסס על מספר מרכיבים :

- **הרצאות ודיונים בכיתה** – במהלך ההרצאות יילמדו נושאי הקורס המפורטים מטה. מצגות הקורס יפורסמו באתר הקורס (<http://moodle.tau.ac.il>) / השקפים שיוצגו באתר אינם כוללים את כל החומר שיוצג וידון בכיתה.
- **קריאה משלימה וניתוח מאמרים** – במהלך הסמסטר יפורסמו באתר מאמרים רלוונטיים אשר יהוו בסיס לדיון בכיתה. יש לקרוא את המאמרים לפני מועד השיעור.
- **הרצאות אורח** – הקורס ילווה בהרצאות של מרצים מובילים מהתעשייה והאקדמיה שיסקרו נושאים מגוונים בתחום הסייבר.
- **מבחן מסכם**

עם סיום הקורס בהצלחה יוכל הסטודנט/ית:

1. לתאר את מושגי היסוד והאתגרים המרכזיים בעולם הסייבר
2. להבין מאפיינים טכנולוגיים של עולם הסייבר והקשר בינם לבין מערכות הניהול של האירגון
3. להסביר את מנגנוני ההגנה המקובלים כיום ואת יתרונותיהם/חסרונותיהם
4. לנתח ולתכנן מערכת הגנה לאירגון בראי איומי הסייבר
5. שיטות ועקרונות לבניית מערכת הגנה ארגונית
6. הבנת הקשר בין מערכות/טכנולוגיות ההגנה להיבטי הניהול של הארגון

ציון הקורס:

הציון ישוקלל על בסיס השתתפות פעילה בשיעורים*, הגשת תרגילים/עבודות ומבחן מסכם, עפ"י המפתח הבא:

מטלה	משקל	תאריך
תרגיל 1	10%	יפורסם בתחילת הסמסטר
תרגיל 2	10%	יפורסם בתחילת הסמסטר
מבחן מסכם**	80%	בהתאם ללוח הבחינות של הפקולטה

* תלמיד, הנעדר משיעור המחייב השתתפות פעילה או שלא השתתף באורח פעיל, רשאי המורה להודיע למזכירות כי יש למחוק את שמו מרשימת המשתתפים. (התלמיד יחויב בתשלום בגין קורס זה)

** מועד הבחינה יפורסם באתר הפקולטה - לוח בחינות.

1. נוכחות בשיעורים
2. השתתפות פעילה בשיעורים
3. הגשת תרגילים
4. מבחן מסכם על החומר הנלמד

כל אי עמידה במי ממשלות הקורס מחייבת הודעה מראש (במייל) למרצה או לעוזר ההוראה

מדיניות שמירה על טווח ציונים

החל משנה"ל תשס"ט מונהגת בפקולטה מדיניות שמירה על טווח ציונים בקורסי התואר השני. עקרונות השיטה חלים על כל קורסי התואר השני, ומדיניות השמירה על טווח הציונים תיושם לגבי הציון הסופי בקורס זה. מידע נוסף בנושא זה מתפרסם בהרחבה באתר הפקולטה.

<https://coller.tau.ac.il/MBA-students/programs/2018-19/MBA/regulations/exams>

הערכת הקורס ע"י הסטודנטים

בסיומו של הקורס הסטודנטים ישתתפו בסקר הוראה על מנת להסיק מסקנות לטובת צרכי הסטודנטים והאוניברסיטה.

אתר הקורס

אתר הקורס יהווה המקום המרכזי בו ימסרו הודעות לסטודנטים, לפיכך מומלץ להתעדכן בו מדי שבוע, לפני השיעור, ובכלל – גם בתום הסמסטר. (לצורך תיאום עינייני הבחינה/פרוייקט הסיום למשל). שקפי הקורס העיקריים יהיו באתר הקורס. לתשומת לבכם - בכיתה ידונו גם נושאים (ובפרט דוגמאות) שאינם מופיעים בשקפים או מופיעים בכותרת בלבד. כל אלו הינם חלק בלתי נפרד מחומר הקורס.

נושאי הקורס ***

*** התכנית הינה בסיס לשינויים. רשימת הנושאים אינה לפי סדר ההרצאות בפועל. קיימת אפשרות שבמהלך הסמסטר יתווספו נושאים עדכניים נוספים ו/ או הרצאות אורח. בהתאם לצורך - יתכן שתנתן הרצאת השלמה/נוספת אחת באחד מימי השישי במהלך הסמסטר. בהרצאות המיועדות להרצאות אורח, דיון, מצגות סטודנטים, ובחינה בע"פ יש חובת נוכחות. מידע לגבי מועדי הרצאות אלו יפורסם בתחילת הסמסטר.

נושאי הלימוד וחובות הקריאה:

פירוט חובות הקורס	נושא	#
קריאה מס' 1	סקירה כללית של הקורס והקדמה, מה השתנה בעולם אבטחת המידע ובמרחב כלכלת הסייבר, סקירת נושאי הקורס, מהי לוחמת סייבר, סיכונים, סוגי תוקפים, מטרת האבטחה (Security Objectives)	1
קריאה מס' 1	טכנולוגיות הזדהות, פרוטוקולי הגנה, תיעול (Tunneling),	2
קריאה מס' 2	SSL/TLS, IPSEC, חומת אש,	3
קריאה מס' 2	אנטי-וירוס, מלכודת דבש, IDS	4
קריאה מס' 3	היבטי הסייבר במחשוב ענן (cloud) וההבדלים בהיבטי הסייבר בין מחשוב ענן לבין פלטפורמות אחרות. רגולצית אבטחה (CCPA, GDPR, NYDFS, HIPAA, NIST, SIG) בהתהוות.	5
קריאה מס' 3	(המשך) רגולצית אבטחה (CCPA, GDPR, NYDFS, HIPAA, NIST, SIG) בהתהוות. המשך נושא הרגולציה והשפעתה על הנהלת האירגון ואופן פעילותה העיסוקית.	6
הגשת תרגיל מס' 1	הרצאת אורח - הקורס ילווה בהרצאות של מרצים מובילים מהתעשייה והאקדמיה שייסקרו נושאים מגוונים בתחום הסייבר. כגון: הצגה וניתוח של אירוע/י סייבר או/ו טכנולוגיות/מחקרים מתקדמים.	7
קריאה מס' 4	קריפטוגרפיה – היסטוריה, טכניקות בסיסיות (פונקציות חד-כיוונית, הצפנה, שלמות הודעה), Block cipher לעומת Stream cipher, הצפנה סימטרית, הצפנה א-סימטרית	8
קריאה מס' 4	(המשך) קריפטוגרפיה – חתימה אלקטרונית, ניהול מפתחות, החלפת מפתחות, אמון, היררכיית רשויות, תעודות (certificate authorities hierarchy), תקינה והשפעתה על חלקי האירגון השונים (ניהול, פיתוח ומחקר, כספים, תפעול וכו')	9
קריאה מס' 5	תקיפות נפוצות, איש באמצע (MiM- Man in the Middle), הפרעה לשירות (DOS) + הפרעות מבוזרות (DDOS), Hijack, Phishing, Ransomware	10
קריאה מס' 7	ניתוח אירוע: התמודדות הנהלת האירגון מול מתקפת כופרה	11
קריאה מס' 7	(המשך) ניתוח אירוע: התמודדות הנהלת האירגון מול מתקפת כופרה	12
הגשת תרגיל מס' 2	ראיות (Forensic), טכניקות התחמקות (Covering), Proxy, Intermediaries, Steganography	13
	תשתיות תקיפה (Botnet, Fast-flux), תקיפות בערוץ צדדי (side channel, Key loggers)	14

מאמרים - חובה

1. EU Cybersecurity Act, European Parliament, 2019
2. Insider Threat Report, Verizon, 2019
3. Cybersecurity Impact on Insurance Business and Operations, Thomas Hartl, Kevin Olberding, David Schraub, 2017
4. The Hackable City, Michiel de Lange, Martijn de Waal, (2019) Springer
5. Mitigating Security Risks Through Attack Strategies Exploration; Braham Lotfi Mediouni, Ayoub Nouri, Marius Bozga, Axel Legay, and Saddek Bensalem, 2018
6. Guidelines on assessing DSP (digital service providers) and OES (operators of essential services) compliance to the NISD security requirements, ENISA, 2018
7. תפיסה לאומית בסייבר להיערכות ולניהול מצבי משבר, 2018.

מאמרים - רשות

8. New Horizons for a Data-Driven Economy, A Roadmap for Usage and Exploitation of Big Data in Europe, José María Cavanillas, Edward Curry, Wolfgang Wahlster, 2016
9. Cost of community violence to hospitals and health systems; Jill Van Den Bos, Nick Creten, Stoddard Davenport, Mason Roberts, 2017
10. Cybersecurity Investments Decision Support Under Economic Aspects, Stefan Beissel, 2016

ספרים (רשות)

11. Gray Hat Hacking, the Ethical Hacker's Handbook, Allen Harper, Shon Harris, Jonathan Ness, Chris Eagle, Gideon Lenkey, and Terron Williams, 2011.
12. Cybersecurity, Managing Systems, Conducting Testing, and Investigating Intrusions, Thomas J. Mowbray, PhD, 2014.
13. Penetration testing, Georgia Weidman. 2014

**** יתכנו עדכונים ותוספות לרשימה. הרשימה המלאה תפורסם בתחילת הסמסטר.