אבטחת סייבר למנהלים – 1242.3282.01

Cybersecurity for Managers

(ללא דרישות קדם)

סמסטר א' – תשפ"ג – מחצית ראשונה

חדר	יום בשבוע	שעה	תאריך בחינה	מרצה	דואר אלקטרוני	טלפון
105	א'	18:45-21:30	עבודה מסכמת	מר אודי דואניס	udidoenyas@gmail.com	052-9530093

שעת קבלה – בתיאום מראש

עוזר הוראה: **ד"ר רפי הוד (PhD, MBA)** rhod@tau.ac.il

היקף הלימודים

היקף הי"ס לקורס : 1

ECTS 4 = 1 י"ס –(European Credit Transfer and Accumulation System) ECTS), 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 ואתגרי הסייבר הכרוכים בו, יסודות וכלים קריפטוגרפים. כמו כן נסקור מי השחקנים בשוק, סוגי תקיפות נפוצות והמוטיבציות מאחוריהן, תשתיות תקיפה ומערכות הגנה.

במהלך הקורס הסטודנטים ילמדו על ארועים מורכבים, הבנת הכלים וניהול הטכנולוגיות להתמודדות עם השאלות העסקיות, האתיות והאתגרים הניהולים בעידן הדיגיטלי בסביבה דינאמית. במהלך הקורס נסקור בעיות ואתגרים עסקיים, אתיים וניהוליים הנובעים מהתחום, ונדון בדרכים להתמודדות באתגרי הסייבר הבינ"ל בכלל ושל האירגונים בפרט מהתעשייה והאקדמיה.

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

מבנה הקורס

הקורס מבוסס על מספר מרכיבים :

- **הרצאות ודיונים בכיתה** – במהלך ההרצאות יילמדו נושאי הקורס המפורטים מטה. מצגות הקורס יפורסמו באתר הקורס במודל. יש לשים לב שלעיתים השקפים 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.
- **הרצאת אורח** – במידת האפשר, תתקיים הרצאה אורח מהתעשיה/ אקדמיה שיסקור נושאים מגוונים בתחום.
- **מצגת אמצע ובוחן ביניים**.

תפוקות למידה

עם סיום הקורס בהצלחה יוכל הסטודנט/ית:

1. לתאר את מושגי היסוד, האתגרים והבוחות המרכזיים בעולם הסייבר
2. להבין מאפיינים טכנולוגיים של עולם הסייבר והקשר בינם לבין מערכות הניהול של הארגון
3. להסביר את מנגנוני ההגנה המקובלים כיום ואת יתרונותיהם/חסרונותיהם לארגון בראי איומיי הסייבר
4. הבנת הקשר בין מערכות/טכנולוגיות ההגנה להיבטי הניהול של הארגון

פירוט המטלות בקורס

1. נוכחות והשתתפות פעילה בשיעורים
2. בוחן ביניים על החומר הנלמד
3. הגשת והצגת מטלה מסכמת

כל אי עמידה במי ממטלות 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/2022-23/MBA/regulations/exams

הערכת הסטודנט בקורס והרכב הציון

<u>ציון הקורס</u>:

הציון ישוקלל על בסיס השתתפות פעילה בשיעורים*, הצגת והגשת מטלות ובוחן אמצע, עפ"י המפתח הבא:

מטלה	משקל	אישי / קבוצתי	תאריך
בחירת נושא למטלת מסכמת**	5%	קבוצתי	עד תחילת השיעור השני
בוחן ביניים	20%	אישי	שבוע 6
הצגת טיוטת מטלה מסכמת	25%	קבוצתי	שיעורים מס' 7 + 6
הגשת מטלה מסכמת	50%	קבוצתי	שבועיים לאחר מועד השיעור האחרון

* 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)

** המטלה המסכמת תעשה בצוותים של 2-4 סטודנטים. הנחיות מפורטות יפורסמו בתחילת הקורס.

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 - בביתה ידונו גם נושאים (ובפרט דוגמאות) שאינם מופיעים בשקפים או מופיעים בכותרת בלבד. כל אלו הינם חלק בלתי נפרד מחומר הקורס.

כל התקשורת בנושאי הקורס תעשה דרך תיבת מסרים אישית שתפתח עבור זה במודל.

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.

<u>פירוט נושאי הלימוד* וחובות הקריאה:</u>**

#	נושא	פירוט חובות הקורס
1	סקירה כללית של הקורס והקדמה, מה השתנה בעולם אבטחת המידע ובמרחב כלכלת הסייבר, מהי לוחמת סייבר, סיכונים, סוגי תוקפים, מטרות האבטחה (Security Objectives), מונחים ודוגמאות רלוונטיות – מבוא חלק א'. סקירת משימת הקורס עם דוגמאות.	קריאה מס' 1
2	מבוא חלק ב' – פוטנציאל סייבר לטובה ולרעה ברמת הארגון, לאומית ובינ"ל; השלמת מונחים בסיסיים. קריפטוגרפיה – טכניקות בסיסיות (פונקציות חד-כיווניות, הצפנה, שלמות הודעה) , ניהול והחלפת מפתחות, Block cipher לעומת Stream cipher, הצפנה סימטרית, הצפנה א-סימטרית, חתימה אלקטרונית, אמון, היררכיית רשויות, תעודות (certificate authorities hierarchy).	קבוצה לניתוח ארוע קריאה מס' 2
3	יסודות טכניים רלוונטיים. טכנולוגיות הזדהות, פרוטוקולי תקשורת והגנה, מרכיבי מערכת מיחשוב. תיעול (Tunneling) ,SSL/TLS, IPSEC , חומת אש, אנטי-ירוס, מלכודת דבש, IDS. היבטי הסייבר במחשוב ענן (cloud) וההבדלים לעומת פלטפורמות אחרות. סוגי תקיפות ושיטות תקיפה ידועות.	קריאה מס' 3
4	תקיפות נפוצות, MiM- Man in the Middle, הפרעה לשירות (DOS) + הפרעות מבוזרות (DDOS), Hijack, Phishing, Ransmware ועוד. רגולציות וסטנדרטים של אבטחה (CCPA, GDPR, NYDFS, HIPAA, NIST, SIG). המשך נושא הרגולציה והשפעתה על הנהלת האירגון ואופן פעילותה העיסקית. תקינה והשפעתה על חלקי האירגון השונים (ניהול, פיתוח ומחקר, כספים, תפעול וכו')	קריאה מס' 4
5	דילמות אתיקה ומוסר בתחומי הסייבר השונים. הרצאת אורח (TBD) על נושאים מגוונים בתחום הסייבר, כגון: הצגה וניתוח של אירוע/י סייבר, IR או/ו טכנולוגיות/מחקרים מתקדמים.	קריאה מס' 5
6	מצגות ניתוחי אירועי סייבר בארגונים בשנתיים האחרונות. ניתוח אירוע: התמודדות הנהלת האירגון מול מתקפות	הצגת ניתוח ארוע בוחן בכיתה קריאה מס' 6
7	קונספטים וטכניקות בהגנת סייבר. ראיות (Forensic), טכניקות התחמקות (Covering, Proxy, Intermediaries, Steganography) תשתיות תקיפה (Botnet, Fast–flux), תקיפות בערוץ צדדי (side channel, Key loggers)	הצגת ניתוח ארוע (המשך) קריאה מס' 7
&	הגשת מטלה מסכמת - אין שיעור -	הגשה עד 18/12/22

*** שינויים יתכנו

ספרי לימוד ורשימת קריאה ****

מאמרים - לקריאה

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, Jose´ Mar´ıa 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. https://www.idi.org.il/media/16859/what-is-cyber-security-part-one-cyberspace-cyber-attacks-and-cyber-protection.pdf
12. Gray Hat Hacking, the Ethical Hacker's Handbook, Allen Harper, Shon Harris, Jonathan Ness, Chris Eagle, Gideon Lenkey, and Terron Williams, 2011.
13. Cybersecurity, Managing Systems, Conducting Testing, and Investigating Intrusions, Thomas J. Mowbray, PhD, 2014.
14. Penetration testing, Georgia Weidman. 2014

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