עקרונות יסוד באבטחת מידע למנהלים

Fundamental principles in information security for managers

מחזור כ"ו – כיתת דליה (קבוצה א01) וכיתת דקל (קבוצה א02)
תקופה מס' 2 – דצמבר-פברואר 2021

שם הקורס: עקרונות יסוד באבטחת מידע למנהלים
Fundamental principles in information security for managers
מספר הקורס: 209.4441
שם המרצה: פרופ' שי גירון (החוג למתמטיקה)
מועד ההרצאה: יום שישי, 08-11 (קבוצה א') 11-14 (קבוצה ב')
תאריכים: 22.12.2020 – 19.02.2021
שעות הקבלה: יום חמישי 9:00-10:00 (בתיאום מראש עם המרצה)
התקשרות עם המרצה: ההתקשרות עם המרצה תתבצע רק דרך אתר הקורס במערכת מוודל (MOODLE),באמצעות משלוח הודעה אישית למרצה, או באמצעות כתיבה בפורום הקורס. הודעות ייבדקו וייענו בתדירות של פעמים בשבוע. במקרים יוצאי דופן, ניתן לפנות למרצה דרך מזכירות החוג.

רקע ורציונל

המשאב הטכנולוגי והמשאב האנושי הם משאבים מרכזיים בכל תאגיד. ככאלה, ניהול נכון של נקודת ההשקה ביניהם עשוי להוות מנוף לכח רב אך עלול גם לייצר חשיפות קריטיות. בעולמנו הטכנולוגי, כל מנהל, בכל תחום ובכל תאגיד, חייב להכיר את העקרונות הבסיסיים של ממשק אבטחת המידע עם הזכות לפרטיות, כשם שהוא יודע לעיין, ולו באופן שטחי במאזן רווח-הפסד. תפקידו של מנהל טוב שלוב בניהול מצוין שהוא עורך. הקורס בנושא אבטחת מידע למנהלים, יספק למנהל את הכלים הראשוניים לעשות זאת בהצלחה.

מטרות הקורס ותפוקות הלמידה

בקורס ילמדו התלמידים/ותאת העקרונות הבסיסיים של אבטחת מידע, אבטחה במרחב הסייבר, ושמירת פרטיות. לאחר סיום הקורס בהצלחה, יוכלו התלמידים / תלמידות:

- להסביר את העקרונות של אבטחת המידע, למנות את מושגי היסוד והאתגרים המרכזיים בעולם הסייבר, להסביר כיצד עובדות מספר התקפות ולתאר סוגים שונים של פגיעויות, להסביר כיצד פועלים מספר מנגנוני אבטחה בהתאם לעקרונות האבטחה ומהם יתרונותיהם/חסרונותיהם, להסביר ולנתח מספר עקרונות בנושאי פרטיות.
- להסביר כיצד ניתן ליישם מספר עקרונות אבטחה כדי לפתור בעיות ולנתח את נושא אבטחת המידע מנקודת מבטו של מנהל: הערכת סיכונים העומדים בפני מערכות (מחשב),יאור של עיקרי האיומים לארגון באירוע סייבר, תכנון עיקרי תפיסת אבטחה המתאימה לארגון.

תכני הקורס

הקורס ידון נושאים הבאים: מטרות אבטחת המידע (סודיות, שלמות, זמינות, פרטיות, אנונימיות, יושרה ואותנטיות, אימות, דין וחשבון, הרשאה, ביקורת, אבטחה), עקרונות התכנון הבסיסיים (למשל של Saltzer and Schroeder), מודלים בסיסיים (למשל בל-לפדולה, ביבהל קלארק ווילסון), בקרת כניסה ובקרת גישה, מדיניות אבטחה, היבטי האסדרה (רגולציה) בתחום, ואחריות מנהלים. יינתן גם רקע בסיסי התחום הקריפטוגרפיה ופרוטוקולים לאבטחת תקשורת (כגון TLS) ואבטחת מידע. יידונו מספר היבטים הקשורים לאבטחת מידע ברשת, פגיעות והתקפות (נגיפים, תולעים, התקפות מבוזרות למניעת שירות (DDOS), נוזקות, התקפות כופר), מנגנוני הגנה (חומות אש), לשמירה על פרויות ולזכויות יוצרים ברשת.

דגשים מתודולוגיים

הקורס מתבסס על למידה פעילה הכוללת הרצאות, קריאה וניתוח של חומרים, ניתוח אירועים, דיונים בכיתה ולמידה קולקטיבית מהצגת עבודות. נוכחות והשתתפות פעילה בהרצאות הן חשובות ביותר, ולכן מוגדרות כחובה.

שיטת ההוראה ודרישות סף

הקרס יינתן בצורה מקוונת. מתוך שמונה המפגשים יהיו (לפחות) שנים אשר יינתנו בצורה א-סינכרונית, כפעילויות בזמן הנתון לבחירת המשתתפים/ות (ולפי לוח הזמנים של הקורס). שאר המפגשים יהיו סינכרוניים, ויועברו דרך מערכת הזום (Zoom). במפגשים הסינכרוניים נדרשים המשתתפים/ות לפתוח מצלמות, כאשר אי פתיחת מצלמה תחשב כהיעדרות מהמפגש.

ההשתתפות בשיעורים (דרך הזום) מצריכה ומחייבת את המשתתפים/ות לריכוז ומחוייבות אישית (למשל, עבודה ממקום שקט ולא תוך כדי "עריכת קניות בסופר"). התלמידים/ות נדרשים לשתף פעולה ולתקשר עם עמיתיהם (וגם עם המרצה) באופן מנומס ומכבד, לא להפריע למהלך השיעורים, ולהופיע לשיעור בצורה מכבדת (אין צורך בחליפה ועניבה, אבל נא לא להתייצב בפיג'מה מול מצלמת הזום).

דרישות הסף כוללות: אוריינות מחשב ותושיה בסיסית (כולל שימוש בזום, מוודל), ויכולת בסיסית להפעיל מספר כלים (למשל סריקת מסמך והעלאתו (בזריזות) למערכת המוודל, באמצעות יישומון, או בדרך אחרת).

ציוד נדרש: מחשב נייד לעבודה (כזה שניתן להתקין עליו תכנות, ולחבר אליו החסן נייד (דיסקון USB), דיסקון (ריק), טלפון חכם. בקורס יינתנו מספר הדגמות שהמשתתפים/ות יידרשו להפעיל. ההדגמות יבוצעו על מערכת הפעלה Windows, ועל טלפון חכם עם מערכת iOS ("אייפון").

היקף העבודה הנדרשת

ההשתתפות בקורס (והצלחה בו) מחייבת עבודה שוטפת בהיקף של כ 1.5 שעות בין המפגשים לצורך הכנת עבודות בית, קריאה והכנה למפגש העוקב. חלק מהעבודות יהיו בקבוצות, לפי ההנחיות שיימסרו במהלך הלימודים. חלק מההערכה של התלמידים/ות בקורס ייתבסס על בדיקה של תוצאות ההכנה והעבודה השוטפת.

דרישות הקורס והרכב הציון

השתתפות פעילה ועניינית בכל ההרצאות/מפגשים, הכנה רצינית לקראת השיעורים, הגשת תרגילי הבית ותרגילי הכיתה, הגשת עבודה סופית (הגשה עד שבועיים מיום המפגש האחרון בקורס), מענה על המבדקים במהלך השיעורים.

בכל המטלות שיינתנו בקבוצות, ייקבעו הקבוצות על ידי המרצה (על פי הגרלה).

ההנחיות לעבודות מטלות השונות, צורת ההגשה, ומועדי ההגשה יינתנו במהלך השיעורים (ויפורסמו באתר הקורס).

התנאים הבאים הנם חובה ומהווים תנאי הכרחי לקבלת ציון בקורס: נוכחות מלאה בכל השיעורים, הגשת כל המטלות בזמן, וקבלת ציון עובר בהם. הגשות באיחור לא ייתקבלו, והציון עבורן יהיה אפס.

הרכב הציון

עבור התלמידים/ות שעמדו בתנאי הקורס, יחושב הציון הסופי בקורס על ידי שקלול של צבירת ניקוד המעקב (נוכחות פעילה, השתתפות, הצגת נושאים/עבודות), ציוני המבדקים (שיינתנו במהלך תקופת הלימוד), ציוני עבודות הבית, וציון העבודה המסכמת (בקבוצות). התמהיל המדוייק של הניקוד יפורסם באתר הקורס.

ספרות עזר:

David Salomon, "Foundations of Computer Security" (Springer)
Library index: QA76.9.A25 S266 (2006)

Ross Anderson, "Security Engineering," John Wiley & Sons,
ISBN 0-471-38922-6.
3rd Edition is available online at: https://www.cl.cam.ac.uk/~rja14/book.html

William Stallings, Lawrie Brown, "Computer Security: Principles and Practice". Pearson Publication.
Link to the author's web page (including student resources)
http://williamstallings.com/ComputerSecurity/

Charles Pfleeger, Shari Pfleeger, Jonathan Margulies, "Security in Computing 5th Edition", ISBN-13: 978-0134085043

הפניות לחומרים נוספים יינתנו באתר הקורס.