הקריה האקדמית אונו
Ono Academic College

הפקולטה מנהל עסקים
לימודים לתואר בוגר
שנת הלימודים תשפ"ב

שם הקורס: מבוא להגנת סייבר
סוג הקורס: בחירה
דרישות קדם:
מרצה: עמיחי ניסימוב
סמסטר: 1
נקודות זכות: 3

מטרות הקורס:

עולם הסייבר מתפתח בהתמדה והופך למימד פעילות אנושית נרחבת- פעילות כלכלית, צבירת ידע, חברתית, ציבורית וגם פשיעה ולחימה מתרחשות בו באופן שוטף. הדבר מציב אתגרי הגנה רבים לגופים ולארגונים כלכליים ושאינם.

הקורס יציג את מגוון האיומים מולם מתמודדים המתגוננים, את הדילמות שבין התגוננות להכלה בארגונים ובמדינות, את השיקולים השונים העומדים בפניהם ואת משפחות כלי ההגנה בסייבר, תפקידם במערך ההגנה הארגוני ובחינת הכדאיות של שילובם בארגון.

הקורס יסקור מגוון נושאים ובכללם הבנת מניעי התוקפים, סוגי תקיפות מובילות כגון PHISHING, Man in the middle ועוד ואת מגוון משפחות כלי ההגנה בארגון- מערכות SIEM, יכולות הגנת עמדות קצה, הגנת מובייל, הגנת מסדי נתונים ופרטיות (והתקינה המקובלת בעולם), יכולות איסוף ברשת, ניתוח מידע מודיעין תומך להגנת סייבר ומערכות תגובה וניהול אירועי סייבר. לצד זאת, ילמדו השיקולים בהגנה על ארגון ותהליך בניית תפישת ההגנה הכולל סקרי סיכונים ובדיקות חדירות. כלים אלו יסייעו בהחלטות כגון: בחינת התמהיל הנכון להשקעה בהגנת סייבר בארגון לעומת מכלול סיכוני הסייבר ויכולות הארגון וכמובן שבהתאם לאסטרטגיית מערכות מידע ולצרכי הארגון.

הקורס יעניק לסטודנטים הכרות עם עולם האתגר שבהגנה על הארגון לצד מודלים להגנה על ארגונים ורשתות וכלים אנליטיים להערכת טיבן של קבלת החלטות בעולם הסייבר, הערכת קבלת ייעוציים טכנולוגיים-עסקיים, הערכת עוצמות הטכנולוגיות הקיימות בענף והאיומים האסטרטגיים, בדיקת עלות-תועלת של מיזמי הגנה חדשים ותהליכי ניהול וגידור הסיכונים בהגנת הסייבר.

בנוסף, בחלק נרחב הקורס יכללו גם סיפורי אירועי אבטחה מובילים בעולם לצד יכולות קריאה, ניתוח והבנה ראשוניות של מקורות מידע בעולם הסייבר והמלצות ליישומם של לקחים מובילים בארגונים.

שיטת הלימוד:

הקורס ייערך באופן מקוון (בזום), לחלק מהשיעורים תידרש קריאת קדם.

בנוסף, הסטודנטים יבצעו ניתוחי מקרה בקבוצות בשיעור וכמטלת אמצע בעזרת הכלים האנליטיים שנלמדים בקורס.

הגישה הפדגוגית היא שקיימת גם למידה בצורה וירטואלית דרך החומרים הרבים שעולים לאתר הקורס.

דרישות הקורס:

מטלת אמצע קורס ועבודת גמר, נדרש לעבור הן את המטלה והם את עבודת הגמר בציון גבוהה מ-60.

שקלול הציון:

30% מטלת אמצע קורס – מצגת של עבודת הגמר בפני הכיתה

70% עבודת גמר – הגשה עבודת הגמר

נושאים:

הרצאות 1 – 2: הקורס נפתח בהכרות כללית עם עולם האינטרנט ודרך פעולתו כמבוא להבנת עולם הסייבר. נלמד את מודל 7 השכבות, ובצורה בסיסית מספר פרוטוקולי תקשורת מרכזיים (HTTP DNS וכו').

הרצאות 3 – 5: הסייבר כמרחב פעולה אנושי ובהבנת מניעי התוקפים השונים ומגוון האיומים על ארגונים, על הפרט ועל מדינות. נעסוק בקצרה בשיטות התקיפה הנפוצות על אנשים פרטיים ארגונים ומדינות, תוך למידה מארועים שהתרחשו במציאות. בחלק זה תיושם הקניית ידע במושגים כלליים בעולם הסייבר

הרצאות 6 – 7: בחלק זה בקורס, יוצגו תפיסות הגנה מובילות ומשפחות כלי ההגנה להגנה היקפית על ארגונים ורשתות, יתרונותיהם לארגון לצד עלויותיהם התפעוליות והאחרות לארגונים. ייוחד פרק לכל אחת ממשפחות ההגנה הבאות- SIEM, End Point, Data and Privacy Protection, intelligence and research assets, mobile protection, cloud protection, incident response tools, DLP. בסופו של פרק זה ינתחו הסטודנטים ארוע תקיפה אמיתי ויציעו פתרונות הגנה שהיו יכולים ליצר מענה אפקטיבי עבור המגן.

הרצאות 7 – 12: בחלק המסיים בקורס יוצגו השיקולים בהגנת הארגון ובשימוש בכלי ההגנה שנלמדו, וכן הכרות בסיסית עם דרישות הרגולציה להגנה בסייבר (תקנים ישראליים כגון 361 ותקינה בין לאומית כגון GDPR ו-PCI).
יוצגו מודלים להערכת סיכוני סייבר בארגון ושיטות לבדיקות חדירות, לצד שיקולים מובילים בניהול סיכוני ההגנה בסייבר בארגונים.
בעבודה המסכמת, יתבקשו הסטודנטים לנתח ארוע הגנה בארגון, תוך שימוש במודלים ובהכרותם עם כלי ההגנה הקיימים ולהציע, בהתאם לשיטות ניהול הסיכון שנלמדו את פתרון ההגנה האופטימלי לארגון.

רשימת קריאה:

ספר הקורס:

Principles of Information Security, Michael E. Whitman and Herbert J. Mattord

Fifth Edition

תורת ההגנה של מערך הסייבר הלאומי