מנהל מדע וטכנולוגיה
תחום טכנולוגיה - מגמת תקשוב

מקצוע התמחות - מגמת תקשוב
תכנית לימודים מיישם סייבר
Ver 2.1

רציונל התכנית

<u>מבוא לתכנית הלימודים</u>

במסגרת המאמץ לקידום ההגנה הלאומית במרחב הסייבר הוסדרו מקצועות הגנת הסייבר בישראל.
מיישם הגנת סייבר – אדם בעל ידע תיאורטי בסיסי ויכולת יישומית (Hands-On) האחראי על יישום הגנת הסייבר בארגון.
מטרת יחידה זו הינה להקנות ידע למיישם ב: הבנת תחום הסייבר, תפישות סייבר, ידע בחוקים ובתקנות הרלוונטיות, סביבות טכנולוגיות, מוצרי אבטחת מידע, תהליכי אבטחה שגרתיים, תהליך טיפול באירוע ואתיקה מקצועית.

ממטרת על זו נגזרים היעדים הבאים:

- להכיר את השפה והטרמינולוגיה בתחום הסייבר
- להכיר את תקני אבטחת המידע וניהול הסיכונים
- להכיר גישות ושיטות הגנה ואבטחה בתקשורת
- להכיר היבטי אבטחת מידע
- להכיר שיטות הצפנה ואימות
- להכיר את נושא דלף המידע
- להכיר שיטות ניהול, רישום וטיפול באירועי אבטחת מידע
- להכיר את נושא מחשוב הענן
- להכיר שיטות שינוע מידע
- להכיר את נושא ההמשכיות העסקית
- להכיר את החוק והאתיקה בתחום

מיעדים אילו נגזרה פריסת התכנים באופן הבא:

פרק	נושא	ע	מ
1	מבוא לאבטחת מידע והגנת הסייבר		
2	תקני אבטחת מידע וניהול סיכונים		
3	הגנת גישה בתקשורת ואינטרנט		
4	בידול והפרדת רשתות תקשורת		
5	היבטי אבטחת מידע בציודי תקשורת (הקשחה) ואבטחת מידע		
6	הצפנה ואימות		
7	בקרת גישה		
8	היבטי אבטחת מידע במערכות הפעלה והקשחות שרתים		
9	היבטי אבטחת מידע במסדי נתונים		
10	תוכנות זדוניות וזיהוי אנומליות		
11	דלף מידע		
12	ניהול ורישום אירועי אבטחת מידע (Audit)		
13	טיפול באירועי אבטחת מידע		
14	מחשוב ענן, שירותי אירוח, וירטואליזיה		
15	שינוע מידע מ/אל הארגון		
16	המשכיות עסקית (BCP/DRP)		
17	אבטחה אפליקטיבית		
18	מתודולוגית ביצוע ניסיונות חוסן (תשתית ואפליקציה)		
19	חוק ואתיקה		
20	אבטחה פיסית		
21	התנסות מעשית התומכת את הידע התאורטי		

פרק 1 – מבוא לאבטחת מידע והגנת הסייבר

<u>מטרות כלליות</u>

- התלמיד יכיר מונחי יסוד באבטחת מידע
- התלמיד יכיר מושגי יסוד בתחום הסייבר
- התלמיד יכיר את מורכבות תחום אבטחת המידע והסייבר

<u>סטנדרט ביצוע</u>

- התלמיד יתאר אונטולוגיה של אבטחת מידע וסייבר.
- התלמיד יתאר סוגי יריבים והמוטיבציה לתקיפה
- התלמיד יסביר סוגי תקיפות
- התלמיד יסביר סוגי פגיעות
- התמיד יתאר דרכי התמודדות ארגונית
- התלמיד יתאר את המרכיב האנושי בארגון
- התלמיד יסביר מדיניות ונהלים של אבטחת מידע
- התלמיד יסביר אבטחת מידע בפרויקט

<u>מוקדי תוכן ומושגים עיקריים</u>

נושא	פירוט
אונטולוגיה של אבטחת מידע וסייבר	מונחים, איומים, קשרים בין המונחים השונים, תפישת NIST, תפיסת האיכות quality assurance, ואונטולוגיות אחרות. המונח dependability.
סוגי יריבים והמוטיבציה לתקיפה	
סוגי תקיפות	תקיפת מחשב מרחוק, מתוך הארגון, חדירה פיזית למתחמי מחשב, Social Engineering, תקיפות משולבות, שימוש במייל, הפניה לאתרים נושאי תוכנה זדונית.
סוגי פגיעות במערכות /במידע	פגיעות בהיבטי זמינות, אמינות, שלמות וסודיות השלכות ומשמעויות הפגיעה - כלכליות ,מוניטין ,משמעויות מעבר לרמת הארגון.
דרכי התמודדות ארגוניות	מינוי בעלי תפקידים, הגדרת מדיניות ונהלים, הגדרת נכסי מידע ומערכות חיוניות, ניהול סיכונים, אבטחה פיזית
המרכיב האנושי ומהימנות עובדים	מודעות, הטמעה בתרבות הארגונית, דיווחים ובקרות, גופים לאומיים העוסקים בתחום בישראל
מדיניות ונהלים של אבטחת מידע	
אבטחת מידע בפרויקט	הטמעת היבטי אבטחת מידע במחזור החיים לפיתוח תוכנה, לרבות השלבים של

	הפצה ליצור וניהול שינויים

<u>הזדמנויות למידה</u>

- סרטונים
- הדגמה של סוגי תקיפות

- Dos Santos Moreira, Edson, Luciana Andréia Fondazzi Martimiano, Antonio José dos Santos Brandão, and Mauro César Bernardes. "Ontologies for information security management and governance." Information Management & Computer Security 16, no. 2 (2008): 150-165.
- Computer security principles and practice. William Stalling and Lawrie Brown. Third edition. ISBN: 978-1-292-06617-2. (Use the relevant sections from the book).
- Official (ISC)2® Guide to the CISSP® CBK®, Fourth Edition. Edited by Adam Gordon. (Use the relevant sections from the book).
- Simplicable Business Guide blog. "The Big List of Information Security Threats."
- http://simplicable.com/arch/new/the-big-list-of-information-security-threats. Avizienis, J.-C. Laprie, B. Randell, and C. Landwehr. Basic concepts and taxonomy of dependable and secure computing. IEEE Transactions on Dependable and Secure Computing, 1(1):11{33, January-March 2004.

<u>דרכי הערכה</u>

- התלמיד יבנה מצגות / ייצור סרטונים המסבירים מושגים מהפרק הנלמד
- מבחן עיוני / מעשי

פרק 2 – תקני אבטחת מידע וניהול סיכונים

<u>מטרות כלליות</u>

- התלמיד יכיר תקני אבטחה וה-Best practices, המקובלים בתחום אבטחת המידע והסייבר
- התלמיד יכיר את יסודות סקר סיכונים

<u>סטנדרט ביצוע</u>

- התלמיד יתאר את תקני האבטחה המקובלים בתחום אבטחת המידע והסייבר.
- התלמיד יסביר את יסודות סקר הסיכונים
- התלמיד יסביר כיצד מתבצע סקר סיכונים
- התלמיד יסביר את מטרותיו של סקר סיכונים
- התמיד יתאר פעילויות להקטנת סיכון
- התלמיד יסביר מושגים של סיכון
- התלמיד יסביר מהו סיכון שיורי

<u>מוקדי תוכן ומושגים עיקריים</u>

נושא	פירוט
הסטנדרטים המקובלים של ISO27K, סטנדרטים של סקרי סיכונים	מה הסיבה והיתרון המתקבל מקיומם, כיצד הם משפרים את ההגנה על הארגון, מהם חסרונותיהם, וההבדלים בין הסטנדרטים
מתודולוגיות לביצוע סקרי סיכונים	
השלבים השונים של סקר סיכונים	
היעדים של סקרי סיכונים	
סוגי סקרים	כמותי איכותי משולב
נשוא הסקרים	אפליקציות, תשתיות, למערכות האבטחה, שילוב סקרים

<u>הזדמנויות למידה</u>

- סרטונים
- מכון התקנים

- http://www.isaca.org/journal/archives/2010/volume-1/pages/performing-a-security-risk-assessment1.aspx. .
- http://searchsecurity.techtarget.com/magazineContent/Information-security-risk-assessment-frameworks..

- ENISA, "Risk Assessment and Risk Management Methods: Information Packages
- for Small and Medium Sized Enterprises (SMEs)". Available online,
- https://www.enisa.europa.eu/publications/information-packages-for-small-and-medium-sized-enterprises-smes/at_download/fullReport.
- OWASP, https://www.owasp.org/index.php/OWASP_Risk_Rating_Methodology. NIST, "Managing Information Security Risk, Organization, Mission, and information System View". NIST Special Publication 800-39. Available online. http://csrc.nist.gov/publications/nistpubs/800-39/SP800-39-final.pdf. NIST, "Guide for Conducting Risk assessments". NIST Special Publication 800-30. Available online.
- http://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-30r1.pdf. ISO 31000:2009, Risk Management—Principles and Guidelines. Geneva: International Standards Organization, Available online from ISO.
- ISO 31010:2009, Risk Management—Risk Assessment techniques. Geneva: International Standards Organization, Available online from ISO.
- ISO/IEC 27K, Information security standards. Available online from ISO.
- Arnason, Sigurjon Thor, and Keith D. Willett. How to achieve 27001 certifications: an example of applied compliance management. CRC Press, 2007.
- Von Solms, Rossouw. "Information security management: why standards are important." Information Management & Computer Security 7, no. 1 (1999): 50-58.

<u>דרכי הערכה</u>

- התלמיד יבנה מצגות / ייצור סרטונים המסבירים מושגים מהפרק הנלמד
- תרגילי תרחיש
- מבחן עיוני

פרק 3 – הגנת גישה בתקשורת ואינטרנט

<u>מטרות כלליות</u>

- התלמיד יכיר מנגנוני ההגנה
- התלמיד יכיר היבטי אבטחה בעת קישור הארגון לאינטרנט
- התלמיד יכיר מנגנוני אבטחה ופרוטוקולים אפליקטיביים של השכבות הגבוהות במודל OSI

<u>סטנדרט ביצוע</u>

- התלמיד יתאר את מנגנוני ההגנה המתאימים לכל דרך גישה למשאבי הארגון
- התלמיד יתאר היבטי אבטחת מידע וחולשות מרכזיות ואת הבעייתיות שבקישור הרשת הארגונית כולה/ או חלקה לאינטרנט
- התלמיד יתאר את סוגי הפרוטוקולים השונים המשמשים לקישור אפליקטיבי (תפקידם, היבטי אבטחת מידע וחולשות מרכזיות, מי מפעיל איזה פרוטוקול)

<u>מוקדי תוכן ומושגים עיקריים</u>

נושא	פירוט
מוצרי אבטחה והגנה ל- WAN/LAN, Wireless ו- Bluetooth	
גישה מרחוק למשאבי הארגון וההגנה על דרכי גישה אלו	
טיפול בגישה באמצעות מחשבים/ מכשירים ניידים דוגמת טלפונים חכמים, iPad	
הגדרת VLAN	
היבטי אבטחת המידע/ רשתות /ארגון בעת קישור הרשת הארגונית לאינטרנט	
בנית DMZ	
פרוטוקולים אפליקטיביים	HTML5, HTML3, WebRTC
שימושים והיבטי אבטחה	אין חובה לדעת את נבכי הפרוטוקול כפי המופיע ב- RFC.

השלמה לבידול בן רשתות	נושאי ה- Web Filtering, וה- WAF (web application firewall)

<u>הזדמנויות למידה</u>

- סרטונים

- Andrés, Steven, Brian Kenyon, and Erik Pack Birkholz. Security Sage's guide to hardening the network infrastructure. Syngress, 2004. <<Good also for network design>>
- Computer security principles and practice. William Stalling and Lawrie Brown. Third edition. ISBN: 978-1-292-06617-2. (Use the relevant sections from the book).
- Official (ISC)2® Guide to the CISSP® CBK®, Fourth Edition. Edited by Adam Gordon. (Use the relevant sections from the book).
- Official (ISC)2® Guide to the ISSAP® CBK®, Fourth Edition. Edited by Adam Gordon. (Use the relevant sections from the book).
- Meghanathan, Natarajan. "A Tutorial on Network Security: Attacks and Controls." arXiv preprint arXiv:1412.6017 (2014).

<u>דרכי הערכה</u>

- התלמיד יבנה מצגות / ייצור סרטונים המסבירים מושגים מהפרק הנלמד
- מבחן עיוני / מעשי

פרק 4 – בידול והפרדת רשתות תקשורת

<u>מטרות כלליות</u>

- התלמיד יכיר מנגנונים ומוצרים שעניינם הפרדת רשתות

<u>סטנדרט ביצוע</u>

- התלמיד יתאר מנגנוני בידול בהתאם לסוג הרשת
- התלמיד יסביר יתרונות וחסרונות של מנגנוני בידול
- התלמיד יתאר היבטי אבטחת מידע וחולשות מרכזיות
- התלמיד יסביר כיצד להקשיח את רשת התקשורת מפני מתקפות מבחוץ

<u>מוקדי תוכן ומושגים עיקריים</u>

נושא	פירוט
יסודות תאורטיים של בידול והפרדה	
כיצד מבטיחים שיחד עם ההפרדה יהיה ניתן לאפשר לעובדים לממש את תפקידם	
מוצרים ומנגנונים המשמשים להפרדה ובידול בין סביבות – רשתות תקשורת	
ניטור המידע העובר בין הרשתות	Firewall, מחשבי Proxy, Mail relay, Content filtering, מוצרי Air Gap
הקשחת רשת התקשורת הארגונית	

<u>הזדמנויות למידה</u>

- סרטונים

- Andrés, Steven, Brian Kenyon, and Erik Pack Birkholz. Security Sage's guide to hardening the network infrastructure. Syngress, 2004. Computer security principles and practice. William Stalling and Lawrie Brown. Third edition. ISBN: 978-1-292-06617-2. (Use the relevant sections from the book).
- Mustafa, Hafiz Attaul, Muhammad Imran, Muhammad Shakir, Ali Imran, and Rahim Tafazolli. "Separation Framework: An Enabler for Cooperative and D2D Communication for Future 5G Networks."

- Official (ISC)2® Guide to the CISSP® CBK®, Fourth Edition. Edited by Adam Gordon. (Use the relevant sections from the book).

<u>דרכי הערכה</u>

- התלמיד יבנה מצגות / ייצור סרטונים המסבירים מושגים מהפרק הנלמד
- תרגילי תרחיש
- מבחן עיוני / מעשי

פרק 5 – היבטי אבטחת מידע בציודי תקשורת (הקשחה) ואבטחת מידע

<u>מטרות כלליות</u>

- התלמיד יכיר את נושא הקשחת ציוד התקשורת, נתבים, בסביבות התקשורת השונות

<u>סטנדרט ביצוע</u>

- התלמיד יסביר מדוע נידרש לבצע הקשחת נתבים
- התלמיד יתאר את עקרונות תהליך ההקשחה
- התלמיד יבצע הקשחה תלוית ציוד תקשורת

<u>מוקדי תוכן ומושגים עיקריים</u>

נושא	פירוט
עקרונות תהליך ההקשחה	
הקשחה תלוית ציוד תקשורת	לדוגמא נתב של CISCO לעומת נתב של חברה אחרת
עדכון תוכנה, firmware, לציוד התקשורת	
בדיקת קשיחות לציוד	
מוצרים תומכים בהקשחה	
תאום עם מוצרי אבטחה לדיווח על אנומליות	

<u>הזדמנויות למידה</u>

- סרטונים

- William Stalling and Lawrie Brown. "Computer security principles and practice." Third edition. ISBN: 978-1-292-06617-2. (Use the relevant sections from the book).
- https://www.techopedia.com/definition/24833/hardening (Accessed 12.06.2016)
- Lück, Ingo, and Heiko Krumm. "Model-based security service configuration." PhD diss., PhD thesis, University of Dortmund, Germany, 2006. Available online.

- http://webhost.laas.fr/TSF/cabernet/cabernet/workshops/plenary/5th-plenary-papers/UniversityofDortmund.pdf.
- Sharma, Sakshi, Gurleen Singh, and Prabhdeep Singh. "Security Enhancing of a LAN Network Using Hardening Technique." International Journal of Innovative Technology and Exploring Engineering 2, no. 3 (2013): 174-181.
- Akin, T. (2002). Hardening cisco routers. O'Reilly Media Inc, Sebastopol, USA, p. 2. ISBN: 0-596-00166-5.
- Cisco, "Cisco Guide to Harden Cisco IOS Devices", Jun 02, 2016, available online
- http://www.cisco.com/c/en/us/support/docs/ip/access-lists/13608-21.html
- See also: https://www.techopedia.com/definition/24833/hardening.

<u>דרכי הערכה</u>

- התלמיד יבנה מצגות / ייצור סרטונים המסבירים מושגים מהפרק הנלמד
- מבחן עיוני / מעשי

פרק 6 – הצפנה ואימות

<u>מטרות כלליות</u>

- התלמיד יכיר פרוטוקולי התקשורת המשמשים לאימות
- התלמיד יכיר והיבטי אבטחה של כל פרוטוקול

<u>סטנדרט ביצוע</u>

- התלמיד יתאר את פרוטוקולי התקשורת המשמשים לאימות
- התלמיד יסביר את הביטי אבטחת המידע וחולשות מרכזיות של הפרוטוקולים הנ"ל
- התלמיד יתאר מי מפעיל כל פרוטוקול
- התלמיד יתאר את הקשרים בין הפרוטוקולים לציוד התקשורת
- התלמיד יתאר את השכבות בהן הפרוטוקולים עובדים

<u>מוקדי תוכן ומושגים עיקריים</u>

נושא	פירוט
הצפנה סימטרית	DES 3DES, א-סימטרית, דפי הלמן, RSA
אימות משתמשים	דפי הלמן
יסודות	Certificate Authority, לאימות קצוות תקשורת, זיהוי משתמשים (הנושא של זיהוי ציוד ילמד בנפרד).
פרוטוקולי תקשורת התומכים בנושא של הצפנה ואימות	IPSEC, SSL, HTTPS, SSH.

<u>הזדמנויות למידה</u>

- סרטונים

- William Stalling and Lawrie Brown. "Computer security principles and practice." Third edition. ISBN: 978-1-292-06617-2. (Use the relevant sections from the book).
- Schneier, Bruce, "Applied Cryptography: Protocols, Algorithm, and Source Code in C", Wiley, John & Sons, Inc., XP002138607; ISBN 0471117099, (Oct. 1995), Second Edition.

<u>דרכי הערכה</u>

- התלמיד יבנה מצגות / ייצור סרטונים המסבירים מושגים מהפרק הנלמד
- מבחן עיוני / מעשי

פרק 7 – בקרת גישה

<u>מטרות כלליות</u>

- התלמיד יכיר את הנושאים של בקרת גישה של משתמשים, תוכנות לרכיבים, מידע במערכות המחשב הארגוניות ורכיבים שונים ברשת הארגונית. מוצרים שונים בתחום
- התלמיד יכיר את התחום של מערכות ארגוניות לזיהוי ואימות משתמשים וחומרה

<u>סטנדרט ביצוע</u>

- התלמיד יתאר את המנגנונים הקיימים במערכת הפעלה לזיהוי ואימות משתמשים
- התלמיד יסביר את תהליך קישור רכיב חומרה למשתמש ספציפי
- התלמיד יתאר התמודדות עם תקלות בקרת גישה
- התלמיד יסביר את גישת BYOD
- התלמיד יתאר את ניהול האפליקציות
- התלמיד יתאר פעולות למניעת התחברות של ציוד בלתי מורשה
- התלמיד יתאר מוצרים וטכנולוגיות בתחום בקרת הגישה

<u>מוקדי תוכן ומושגים עיקריים</u>

נושא	פירוט
זיהוי ואימות משתמשים תאוריה	חזרה קצרה על המנגנונים הקיימים במערכת ההפעלה לזיהוי ואימות משתמשים
המושג של authentication Multifactor	
תוכנה/ חומרה נוספת לזיהוי ואימות משתמשים	Tokens, Smart cards, Biometric device
תהליכי קישור רכיב החומרה למשתמש ספציפי	טיפול בחריגים – אובדן, משתמש חדש במערכת, משתמש העוזב את הארגון. התפיסה של שימוש ביותר מרכיב אחד לזיהוי משתמש לדוגמא שימוש במוצר ביומטרי לזיהוי המשתמש + סיסמא
הגדרה ושימוש במערכות Identity management	כלל ארגוניות לזיהוי ואימות משתמשים והרשאותיהם במערכות השונות,Credentials התממשקות עם DNS לניהול משתמשים התראה על אירועים
זיהוי גישה של מכשירים ניידים מותרים (גישת	

(BYOD	
ניהול האפליקציות והגישה אליהן	מוצרי MAM (Mobile application management)
פעולות למניעת התחברות של ציוד בלתי מורשה	דוגמת מחשב נייד לרשת הארגונית.
מוצרים וטכנולוגיות בתחום	שימוש ב- certificate אירגוני לזיהוי ציוד תקשורת.

<u>הזדמנויות למידה</u>

- סרטונים

- Official (ISC)2® Guide to the CISSP® CBK®, Fourth Edition. Edited by Adam Gordon. (Use the relevant sections from the book).
- William Stalling and Lawrie Brown. "Computer security principles and practice." Third edition. ISBN: 978-1-292-06617-2. (Use the relevant sections from the book).
- Dhamija, Rachna, and Lisa Dusseault. "The seven flaws of identity management: Usability and security challenges." Security & Privacy, IEEE 6, no. 2 (2008): 24-29.
- SANS, "Identity Management". Available online. https://www.sans.org/reading-room/whitepapers/authentication/identity-management-1076. SANS, "An Introduction to Identity Management.". Available online. https://www.sans.org/reading-room/whitepapers/authentication/introduction-identity-management-852.
- INFOSEC INSTITUTE, "Chapter 11 – Identity management and Access controls.". Available online. http://resources.infosecinstitute.com/identity-management/. Ernst & Young. "Identity and Access Management – Beyond Compliance.". Available online. http://www.ey.com/Publication/vwLUAssets/Identity_and_access_management_-_Beyond_compliance/$FILE/Identity_and_access_management_Beyond_compliance_AU1638.pdf.
- Graba et al. "Bring your own device organizational information security and privacy".
- http://www.arpnjournals.com/jeas/research_papers/rp_2015/jeas_0215_1591.pdf

- Ernst & Young. "Bring Your Own Device Security and Risk Considerations for Your Mobile Device Program.". http://www.ey.com/Publication/vwLUAssets/EY_-_Bring_your_own_device:_mobile_security_and_risk/$FILE/Bring_your_own_device.pdf.

<u>דרכי הערכה</u>

- התלמיד יבנה מצגות / ייצור סרטונים המסבירים מושגים מהפרק הנלמד
- מבחן עיוני / מעשי

פרק 8 – היבטי אבטחת מידע במערכות הפעלה והקשחות שרתים

<u>מטרות כלליות</u>

- התלמיד יכיר היבטי אבטחת המידע במערכות ההפעלה השונות
- התלמיד יכיר העקרונות של הקשחת השרתים והשירותים השונים המטופלים במסגרת תהליכי ההקשחה

<u>סטנדרט ביצוע</u>

- התלמיד יתאר את ההיבטים המרכזיים של אבטחת מידע בכל מערכת הפעלה
- התלמיד יתאר את החולשות המרכזיות הקימות במערכות ההפעלה
- התלמיד יתאר מתקפות ידועות על מערכות הפעלה
- התלמיד יתאר תהליכי הקשחה
- התלמיד יתאר את התהליכים השונים והשירותים הניתנים ע"י מחשב מוקשח
- התלמיד יסביר כיצד על אף ההקשחה לאפשר שירותים שונים ע"ג מחשב מוקשח.

נושא	פירוט
מימוש אבטחת מידע	במסגרת שרותי מערכות ההפעלה הבאות: Unix, Win, Android, VM.
יסודות תהליכי זיהוי ואימות משתמשים קרברוס	הרשאות ל- Object ו- Subject, קבצים, קבוצות משתמשים. הנושא דנן ילמד לעומק בקורס שענינו אימות וזיהוי
לוגים של מערכת הפעלה התומכים באבטחת המידע	
חלק תאורטי של מדוע נידרש לבצע הקשחת שרתים	עקרונות תהליך ההקשחה
הקשחה תלוית סביבות ושירותים	
פעולות בסיסיות בסביבת מערכות ההפעלה השונות Unix, Win, VM.	
עדכון תוכנה חומרה	

לשרתים מוקשחים	
בדיקת קשיחות לשרת	
מוצרים תומכים בהקשחה	
תאום עם מוצרי אבטחה לדיווח על אנומליות	

<u>הזדמנויות למידה</u>

- סרטונים

- Lück, Ingo, and Heiko Krumm. "Model-based security service configuration." PhD diss., PhD thesis, University of Dortmund, Germany, 2006. (URL: http://webhost.laas.fr/TSF/cabernet/cabernet/workshops/plenary/5th-plenary-papers/UniversityofDortmund.pdf)
- Andrés, Steven, Brian Kenyon, and Erik Pack Birkholz. Security Sage's guide to hardening the network infrastructure. Syngress, 2004. <<Good also for network design>>
- William Stalling and Lawrie Brown. "Computer security principles and practice." Third edition. ISBN: 978-1-292-06617-2. (Use the relevant sections from the book).
- NIST, " NIST SP 800-123 Guide to General Server Security."
- http://csrc.nist.gov/publications/nistpubs/800-123/SP800-123.pdf.

<u>דרכי הערכה</u>

- התלמיד יבנה מצגות / ייצור סרטונים המסבירים מושגים מהפרק הנלמד
- מבחן עיוני / מעשי

פרק 9 – היבטי אבטחת מידע במסדי נתונים

<u>מטרות כלליות</u>

- התלמיד יכיר את היבטי אבטחת המידע – גישת משתמשים, הגנה על מידע נייח, במערכות מסדי נתונים וב- Storage systems. חולשות ואופני הגנה

<u>סטנדרט ביצוע</u>

- התלמיד יסביר את יסודות מסדי הנתונים
- התלמיד יתאר היבטי אבטחת מידע במדי נתונים (חולשות מרכזיות הקימות במערכת, אופני ההגנה, ומוצרים משלימים, ומתקפות ידועות)

<u>מוקדי תוכן ומושגים עיקריים</u>

נושא	פירוט
יסודות מסדי נתונים	SQL, Relational DB, MongoDB, ארכיטקטורה
היבטי אבטחת מידע במערכות הנ"ל	הגנת גישה, הגבלת מידע לצפייה/ עדכון פעולות תוכנה נדרשות (לדוגמא: בדיקת אורכי שדות קלט) חולשות ידועות, ומתקפות ידועות
תמיכת מערכת ההפעלה בשמירה על מסדי הנתונים	
תמיכת תוכנת מסד הנתונים בנושאי אבטחה	
Referential integrity	
מוצרים משלימים שמעבר לאשר ניתן ע"י מ"ה	
מערכות Storage systems ואבטחת המידע בהם	

<u>הזדמנויות למידה</u>

- סרטונים

- William Stalling and Lawrie Brown. "Computer security principles and practice." Third edition. ISBN: 978-1-292-06617-2. (Use the relevant sections from the book).
- Imperva. "Top ten Database Security Threats.", Available online. http://www.imperva.com/docs/wp_topten_database_threats.pdf. Last accessed 16.06.2016.
- Sandhu, Ravi S., and Sushil Jajodia. "Data and database security and controls." Handbook of information security management, Auerbach Publishers (1993): 1-37.
- Basharat, Iqra, Farooque Azam, and Abdul Wahab Muzaffar. "Database security and encryption: A survey study." International Journal of Computer Applications 47, no. 12 (2012).
- Official (ISC)2® Guide to the CISSP® CBK®, Fourth Edition. Edited by Adam Gordon. (Use the relevant sections from the book).
- Riedel, Erik, Mahesh Kallahalla, and Ram Swaminathan. "A Framework for Evaluating Storage System Security." In FAST, vol. 2, pp. 15-30. 2002. Available Online. https://www.usenix.org/legacy/events/fast02/full_papers/riedel/riedel_html/. Last accessed 17.06.2016
- UC Berkely, "Database Hardening Best Practices". Available online. https://security.berkeley.edu/resources/best-practices-how-articles/database-hardening-best-practices..

<u>דרכי הערכה</u>

- התלמיד יבנה מצגות / ייצור סרטונים המסבירים מושגים מהפרק הנלמד
- מבחן עיוני / מעשי

פרק 10 – תוכנות זדוניות וזיהוי אנומליות

<u>מטרות כלליות</u>

- התלמיד יכיר את נושא התוכנות הזדוניות דוגמת: וירוס מחשב, רוגלות. הסוגים השונים, דרכי הפצה, אופני התמודדות, מניעה ומוצרי הגנה מפני תוכנה זדונית.
- התלמיד יכיר כיצד מזהים קיום של תוכנה זדונית, שימוש במנגנונים לזיהוי אנומליות בהתנהגות רשת והתנהגות מחשב, והפעולות שיש לנקוט בעת גילוי .

<u>סטנדרט ביצוע</u>

- התלמיד יתאר את ההיבטים המרכזיים של נושא התוכנה הזדונית והגנת הסביבה הממוחשבת מפניהם
- התלמיד יתאר דרכי הפצה, מניעה והתמודדות עם תוכנה זדונית
- התלמיד יתאר מוצרי הגנה, קסטומיזציה של מוצרי הגנה, ותפעול שותף של מוצרי ההגנה
- התלמיד יסביר את נושא זיהוי אנומליות, טיפול בסיסי בהתאם לנהלי הארגון ומוצרים תומכים בתחום.

<u>מוקדי תוכן ומושגים עיקריים</u>

נושא	פירוט
תאוריה וסוגים של תוכנות זדוניות	לדוגמא: Trojan, APT
תוכנה זדונית מוכוונת מטרה ויעד	
שימוש בתוכנה זדונית לתקיפה, דוגמאות לדרכי הפצה	
מוצרי אנטי וירוס, לשרתים, מחשבים אישיים, שרתי דואר, סביבת אינטרנט	התקנה, קסטומיזציה, עדכון
הבדלה בין מוצרים	

מבוססי חתימה למוצרים מבוססי התנהגות ומוצרים היברידיים.	
מתודולוגיות להתמודדות עם תוכנות זדוניות	
מהי אנומליה, כיצד מזהים אנומליה ברשתות, במחשבים	
טכניקות לזיהוי אנומליות	תלויות חוקים, תלויות זמן, תלויות משתמש, בניית פרופילים
מוצרים לזיהוי אנומליות. תהליכים ושיטות לטיפול באירוע	
מוצרי IDS (intrusion detection systems) IPS (intrusion prevention systems)	
התקנה קסטומיזציה, תפעול שוטף ובדיקת לוגים	
התראות שווא מול התראות אמת	
זיהוי אנומליה מחייבת "הרמת דגל" והפניה לדרג בכיר	

<u>הזדמנויות למידה</u>

- סרטונים

- Official (ISC)2® Guide to the CISSP® CBK®, Fourth Edition. Edited by Adam Gordon. (Use the relevant sections from the book).
- William Stalling and Lawrie Brown. "Computer security principles and practice." Third edition. ISBN: 978-1-292-06617-2. (Use the relevant sections from the book).
- Shevchenko Alisa, "malicious Code Detection Technologies – Kasparsky lab", Available online. http://latam.kaspersky.com/sites/default/files/knowledge-center/malicious%20code%20detection%20technologies.pdf. Riedel, Erik,

Mahesh Kallahalla, and Ram Swaminathan. "A Framework for Evaluating Storage System Security." In FAST, vol. 2, pp. 15-30. 2002.

- Kaur, Harjinder, Gurpreet Singh, and Jaspreet Minhas. "A review of machine learning based anomaly detection techniques." arXiv preprint arXiv:1307.7286 (2013).
- Ahmed, Mohiuddin, Abdun Naser Mahmood, and Jiankun Hu. "A survey of network anomaly detection techniques." Journal of Network and Computer Applications 60 (2016): 19-31.
- Yu, Yingbing. "A survey of anomaly intrusion detection techniques." Journal of Computing Sciences in Colleges 28, no. 1 (2012): 9-17.

<u>דרכי הערכה</u>

- התלמיד יבנה מצגות / ייצור סרטונים המסבירים מושגים מהפרק הנלמד
- מבחן עיוני / מעשי

פרק 11 – דלף מידע

<u>מטרות כלליות</u>

- התלמיד יכיר את נושא דלף המידע הארגוני, הסכנות שבו, תהליכי מניעה/ צמצום/ גילוי
- התלמיד יכיר מוצרים התומכים בהגנת המידע הארגוני מפני דלף מידע
- התלמיד יכיר את הפעולות שיש לנקוט בעת גילוי דלף מידע

<u>סטנדרט ביצוע</u>

- התלמיד יסביר את המושג דלף מידע
- התלמיד יתאר את היבטי החוק בנושא דלף מידע
- התלמיד יתאר שיטות הגנה / מניעה / צמצום של דלף מידע במסדי נתונים
- התלמיד יתאר שיטות הגנה / מניעה / צמצום של דלף מידע בהתקנים ניידים

<u>מוקדי תוכן ומושגים עיקריים</u>

נושא	פירוט
המושג דלף מידע	מהיכן יכול לדלוף, ערוצים, כיצד מזהים, אמצעים ושיטות קיימות למניעה/ צמצום התופעה, לזיהוי ואיתור
היבטי חוק בנושא דלף מידע	
הגנה / מניעה/ צמצום של דלף מידע במסדי נתונים	storage systems
הגנה / מניעה/ צמצום של דלף מידע בהתקנים ניידים דוגמת טלפונים חכמים, מחשבים ניידים.	
התקני זיכרון נתיקים	disk-on-key, דיסק נתיק

מוצרים וטכנולוגיות למניעה/ גילוי/ זיהוי	מוצרי content filtering

<u>הזדמנויות למידה</u>

- סרטונים

- SANS Institute, "Data leakage – Threats and Mitigation", available online,
- https://www.sans.org/reading-room/whitepapers/awareness/data-leakage-threats-mitigation-1931.
- Yang, Zhemin, and Min Yang. "Leakminer: Detect information leakage on android with static taint analysis." In Software Engineering (WCSE), 2012 Third World Congress on, pp. 101-104. IEEE, 2012.
- Sarmah, Arup, Arabindu Dey, and Chandan Jyoti Kumar. "Analysis and Modeling of an effective Anomaly Detection Techniques for Detecting Data Exfiltration of Network." Analysis 2, no. 5 (2014).
- Official (ISC)2® Guide to the CISSP® CBK®, Fourth Edition. Edited by Adam Gordon. (Use the relevant sections from the book).
- William Stalling and Lawrie Brown. "Computer security principles and practice." Third edition. ISBN: 978-1-292-06617-2. (Use the relevant sections from the book).
- S. Liu and R. Kuhn, “Data loss prevention,” IT Professional , vol. 12, no. 2, pp. 10–13, 2010. Available online. http://csrc.nist.gov/groups/SNS/rbac/documents/data-loss.pdf.

<u>דרכי הערכה</u>

- התלמיד יבנה מצגות / ייצור סרטונים המסבירים מושגים מהפרק הנלמד
- מבחן עיוני / מעשי

פרק 12 – ניהול ורישום אירועי אבטחת מידע (Audit)

<u>מטרות כלליות</u>

- התלמיד יכיר את נושא רישום וניהול אירועי אבטחת מידע על סוגיהם השונים (לדוגמא זיהוי ממוכן של וירוס, ניסיון חדירה למערכות הארגון, ניסיון להוציא מידע אל מחוץ לארגון ע"י בלתי מורשה – דלף מידע, וכדומה)
- התלמיד יכיר מוצרים תומכים בתחום

<u>סטנדרט ביצוע</u>

- התלמיד יתאר את ההיבטים המרכזיים של ניהול ורישום של אירועי אבטחה אופן ההתמודדות, - מותנה בנהלי הארגון

<u>מוקדי תוכן ומושגים עיקריים</u>

נושא	פירוט
ניהול ורישום של אירועי אבטחה	מהו הנושא מדוע נידרש ניהול ידני לחצי ידני
מוצרים תומכים	מוצרי SOC (security operation center) מוצרי SIEM (security information event management), מוצרי NAC (network access control)
סנסורים	התקנה וקונפיגורציה. תהליך הגדרה של חוקים במוצר, התראות שוא למול התראות אמת, מעקב, עדכון, תחזוקה. שילוב מוצרים אלו בארגון, קביעת מסלולי דיווח.
אופן התייחסות למידע התרעתי המתקבל ממקור חיצוני לארגון, ניסיון חדירה מבחוץ	
אופן ההתייחסות למידע הרתעתי המתקבל ממקור פנימי, מיתוך הארגון	

המתקבל מכל מחשב וציוד המותקן בארגון ו/או הרשאי לגשת למשאבי הארגון.	

<u>הזדמנויות למידה</u>

- סרטונים

- William Stalling and Lawrie Brown. "Computer security principles and practice." Third edition. ISBN: 978-1-292-06617-2. (Use the relevant sections from the book).
- Microsoft, "auditing Security Events - TechNet". Available online. https://technet.microsoft.com/en-us/library/cc776394(v=ws.10).aspx. Last accessed 16.06.2016
- NIST, "Guide to Computer Security log management – NIST Special Publication 800-92.", Available online. http://csrc.nist.gov/publications/nistpubs/800-92/SP800-92.pdf. SANS, "Successful SIEM and Log Management Strategies for Audit and Compliance." Available online. https://www.sans.org/reading-room/whitepapers/auditing/successful-siem-log-management-strategies-audit-compliance-33528. SANS, "Building a World-Class Security Operations Center: A Roadmap.". Available online. https://www.sans.org/reading-room/whitepapers/analyst/building-world-class-security-operations-center-roadmap-35907.
- McAffe, "Creating and maintaining a SOC.". Available online. http://www.mcafee.com/de/resources/white-papers/foundstone/wp-creating-maintaining-soc.pdf.
- EY, "Security Operation Centers - Helping You Get Ahead of Cybercrime". Available online. http://www.ey.com/Publication/vwLUAssets/EY-security-operations-centers-helping-you-get-ahead-of-cybercrime/$FILE/EY-security-operations-centers-helping-you-get-ahead-of-cybercrime.pdf. Last accessed 16.06.2016.
- Also See SANS IDFAQ https://www.sans.org/security-resources/idfaq/what-is-the-role-of-a-siem-in-detecting-events-of-interest/5/10

<u>דרכי הערכה</u>

- התלמיד יבנה מצגות / ייצור סרטונים המסבירים מושגים מהפרק הנלמד
- מבחן עיוני / מעשי

פרק 13 – טיפול באירועי אבטחת מידע

<u>מטרות כלליות</u>

- התלמיד יכיר את העקרונות של טיפול באירועי אבטחה. הבנת הסיטואציה של קיום מתקפה, שלבי המתקפה וכיצד לטפל באירוע

<u>סטנדרט ביצוע</u>

- התלמיד יסביר כיצד נושאים שונים שלמד מתממשקים, ויסודות הטיפול באירוע אבטחה
- התלמיד יתאר סוגי תקיפות
- התלמיד יסביר את הנזק הנגרם מתקיפה
- התלמיד יתאר אמצעים לזיהוי ובלימת תקיפה
- התלמיד יסביר את אופן הטיפול בתקיפות שנתגלו
- התלמיד יתאר את תהליכי השחזור
- התלמיד יתאר תהליכי דיווח לרשויות

<u>מוקדי תוכן ומושגים עיקריים</u>

נושא	פירוט
הכרת סוגי תקיפות	DoS/ DDoS, Spear Phishing, וכו
הבנת תהליך ביצוע התקיפה	שלבי המתקפה, משך המתקפה – לדוגמא: התקיפה מתחילה במשלוח דואר תמים המכיל קובץ עם תוכנה זדונית.
הבנת הנזק (impact) הנגרם מהתקיפה	
אמצעים העשויים לסייע לארגון לזיהוי קיומה של תקיפה	
אמצעים העשויים לסייע בבלימת התקיפה	
הכרות עם הנושא של התראות שווא	false positive ו- false negative.

אופן הטיפול בתקיפות שהתגלו	גישות ומוצרים
הפעלת מנגנונים בולמים ובדיקת יעילותם	
בדיקת נזקים, מימוש תהליכים פורנזיים	
תהליכי שחזור	
בדיקת הפתרון שניתן	
הפקת לקחים ברמות הארגוניות השונות	
הרחבת בסיס הידע הארגוני	
פניה דיווח לרשויות החוק	

<u>הזדמנויות למידה</u>

- סרטונים
- חוק הגנת הפרטיות התשמ"א – 1981.

- William Stalling and Lawrie Brown. "Computer security principles and practice." Third edition. ISBN: 978-1-292-06617-2. (Use the relevant sections from the book).
- Official (ISC)2® Guide to the CISSP® CBK®, Forth Edition. Edited by Adam Gordon. (Use the relevant sections from the book).
- HEISC. "Information Security Incident Management.".
- https://spaces.internet2.edu/display/2014infosecurityguide/Information+Security+Incident+Management. Last accessed 16.06.2016.
- ISO/IEC. "ISO/IEC 27035:2011 Information technology — Security techniques — Information security incident management."
- ISO/IEC. "ISO/IEC 27035-3: guidelines for incident response operations."
- ENISA. " Good Practice Guide for Incident Management - enisa - Europa.eu.". https://www.enisa.europa.eu/publications/good-practice-guide-for-incident-management/at_download/fullReport. Last accessed 16.06.2016.
- NIST. "Computer security Incident Handling Guide – Special publication 800-61 R2".
- http://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-61r2.pdf.

<u>דרכי הערכה</u>

- התלמיד יבנה מצגות / ייצור סרטונים המסבירים מושגים מהפרק הנלמד
- מבחן עיוני / מעשי

פרק 14 – מחשוב ענן, שירותי אירוח, וירטואליזיה

<u>מטרות כלליות</u>

- התלמיד יכיר את העקרונות מחשוב הענן, שירותי אירוח ווירטואליזציה

<u>סטנדרט ביצוע</u>

- התלמיד יתאר את הסוגים השונים של מחשוב ענן. קבלת דיווחים מהלוגים השונים והבנתם. היבטי חוק. זיהוי אנומליות, מוצרים תומכי אבטחה של האורח והמארח
- התלמיד יתאר את הסוגים השונים של משירותי אירוח. קבלת דיווחים מהלוגים השונים והבנתם. היבטי חוק. זיהוי אנומליות, מוצרים תומכי אבטחה של האורח והמארח
- התלמיד יתאר סביבת VM, לסוגיו, היבטי אבטחה מהיבט החוק מפני שהנושא דנן נלמד מהיבטים טכניים בעבר

<u>מוקדי תוכן ומושגים עיקריים</u>

נושא	פירוט
מחשוב ענן	
שירותי אירוח	
וירטואליזציה	

<u>הזדמנויות למידה</u>

- סרטונים

- William Stalling and Lawrie Brown. "Computer security principles and practice." Third edition. ISBN: 978-1-292-06617-2. (Use the relevant sections from the book).
- Modern Operating systems. Andrew S. Tanenbaum and Herbert Boss. ISBN-13: 978-1292061429. (Only the relevant chapters regarding virtualization and cloud computing).

- Modi, Chirag, Dhiren Patel, Bhavesh Borisaniya, Avi Patel, and Muttukrishnan Rajarajan. "A survey on security issues and solutions at different layers of Cloud computing." The Journal of Supercomputing 63, no. 2 (2013): 561-592.
- ENISA. "Cloud Computing – Benefits, Risks and Recommendations for Information Security.". https://resilience.enisa.europa.eu/cloud-security-and-resilience/publications/cloud-computing-benefits-risks-and-recommendations-for-information-security. Last Accessed 16.06.2016.
- Cloud Standards Customer Council. "Security for Cloud Computing Ten Steps to Ensure Success Version 2.0.". http://www.cloud-council.org/deliverables/CSCC-Security-for-Cloud-Computing-10-Steps-to-Ensure-Success.pdf. (2015). Last Accessed 16.06.2016.
- NIST. "Guide to Security for Full virtualization technologies." NIST Special Publication 800-125. csrc.nist.gov/publications/nistpubs/800-125/SP800-125-final.pdf.
- NIST. "Guide to General Server Security. NIST Special Publication 800-123.
- csrc.nist.gov/publications/nistpubs/800-123/SP800-123.pdf
- https://spaces.internet2.edu/display/2014infosecurityguide/Cloud+Computing+Security

<u>דרכי הערכה</u>

- התלמיד יבנה מצגות / ייצור סרטונים המסבירים מושגים מהפרק הנלמד
- מבחן עיוני / מעשי

פרק 15 – שינוע מידע מ/אל הארגון

<u>מטרות כלליות</u>

- התלמיד יכיר את העקרונות המתודולוגיות הנהוגות בנושא של שינוע מידע מ/אל הארגון באמצעים פיזיים דוגמת מצאי מידע מגנטיים ואופטיים.
- התלמיד יכיר את היבטי אבטחת המידע והסיכונים הקיימים בעת שינוע מידע מ /אל הארגון והשיטות המקובלות להגן על מידע זה

<u>סטנדרט ביצוע</u>

- התלמיד יתאר היבטי אבטחת המידע בעת הכנסת מידע לארגון באמצעות מצעי מידע מגנטיים ואופטיים
- התלמיד יתאר שינוע גיבויים
- התלמיד יתאר תחנות הלבנה ותהליכי השחרה

<u>מוקדי תוכן ומושגים עיקריים</u>

נושא	פירוט
היבטי אבטחת המידע בעת הכנסת מידע לארגון באמצעות מצעי מידע מגנטיים ואופטיים	
שינוע גיבויים	
נהלים ומתודולוגיות	
תחנות "הלבנה"	
תהליכי "השחרה"	

<u>הזדמנויות למידה</u>

- סרטונים

- EPA. "Information Security – Media Protection Procedures.". https://www.epa.gov/sites/production/files/2016-01/documents/cio_2150-p-10.2.pdf. Last Accessed 16.06.2016.
- U.S. department of Transformation. "Removable Media Security Policy.". http://www.faa.gov/documentLibrary/media/Order/1370.111.pdf. Last Accessed 16.06.2016.
- HEISC, "Guidelines for Data De-Identification or Anonymization.". https://spaces.internet2.edu/display/2014infosecurityguide/Guidelines+for+Data+De-Identification+or+Anonymization. Last Accessed 16.06.2016.
- NIST. "Guidelines for Media Sanitization – NIST Special Publication 800-88.".
- http://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-88r1.pdf. Last

<u>דרכי הערכה</u>

- התלמיד יבנה מצגות / ייצור סרטונים המסבירים מושגים מהפרק הנלמד
- מבחן עיוני / מעשי

פרק 16 – המשכיות עסקית (BCP/DRP)

<u>מטרות כלליות</u>

- התלמיד יכיר את נושא הגיבוי, השחזור והתאוששות מאסון על היבטיו וברמות השונות של גיבוי ושחזור
- התלמיד יכיר את תמיכת מערכת ההפעלה בנושא
- התלמיד יכיר מוצרים משלימים בנושא

<u>סטנדרט ביצוע</u>

- התלמיד יתאר מתודולוגיות לגיבוי ושחזור
- התלמיד יתאר שירותי מערכות הפעלה לגיבוי ושחזור
- התלמיד יתאר היבטים אירגוניים של התאוששות מאסון
- התלמיד יתאר היבטי אבטחת מידע של נושא הגיבוי והשחזור

<u>מוקדי תוכן ומושגים עיקריים</u>

נושא	פירוט
מתודולוגית לגיבוי ושחזור	תאוריה של DRP and BCP, - גיבוי מלא, חלקי, שימוש בלוגים כגיבוי
שיטות תלויות סביבה	אתרי מחשב מפוצלים, מערכות הפעלה שונות
שרותי מערכות ההפעלה לגיבוי ושחזור	
מוצרים חיצוניים משלימים	
היבטים אירגוניים של התאוששות מאסון	
היבטי אבטחת מידע של נושא הגיבוי והשחזור	הרשאות יתר למשתמשים המבצעים פעולות אלו, היכולת לעיין במידע שאינם מורשים לו.

מוצרי Storage systems	אופני הגנה על המידע האגור בהם, גיבוי והתאוששות ואופני הגנה במוצרים אלו.

<u>הזדמנויות למידה</u>

- סרטונים

- Official (ISC)2® Guide to the ISSAP® CBK®, Fourth Edition. Edited by Adam Gordon. (Use the relevant sections from the book).
- Official (ISC)2® Guide to the CISSP® CBK®, Fourth Edition. Edited by Adam Gordon. (Use the relevant sections from the book).
- William Stalling and Lawrie Brown. "Computer security principles and practice." Third edition. ISBN: 978-1-292-06617-2. (Use the relevant sections from the book).
- NIST, "Guide for Cybersecurity Event Recovery – Draft NIST Special Publication 800-184." Available online. http://csrc.nist.gov/publications/drafts/800-184/sp800_184_draft.pdf. Last Accessed 17.06.2016

<u>דרכי הערכה</u>

- התלמיד יבנה מצגות / ייצור סרטונים המסבירים מושגים מהפרק הנלמד
- מבחן עיוני/מעשי

פרק 17 – אבטחה אפליקטיבית

<u>מטרות כלליות</u>

- התלמיד יכיר את העקרונות המתודולוגיות הנהוגות בנושא הטמעת היבטי אבטחת מידע בתוכנה, ניהול שינויי תוכנה והיבטים של מבדקי אבטחת מידע בתוכנה. הקשר בין איכות תוכנה לאבטחת מידע ואמינות תוכנה
- התלמיד יכיר את התהליכים השונים למימוש בעת מחזור החיים של פיתוח תוכנה ושינויים בתוכנה

<u>סטנדרט ביצוע</u>

- התלמיד יתאר את הסיכונים העומדים בפני מערכת התוכנה/ אפליקציה
- התלמיד יסביר את דרישות אבטחת מידע ממערכת התוכנה/ אפליקציה
- התלמיד יתאר הפעילויות השונות, בהיבטי אבטחת מידע, שיש לבצע בכל שלב של מחזור חיי פיתוח התוכנה/ אפליקציה
- התלמיד יתאר מבדקי אבטחת מידע

<u>מוקדי תוכן ומושגים עיקריים</u>

נושא	פירוט
זיהוי הסיכונים העומדים בפני מערכת התוכנה/ אפליקציה	
קביעת דרישות אבטחת מידע ממערכת התוכנה/ אפליקציה	
הפעילויות השונות, בהיבטי אבטחת מידע, שיש לבצע בכל שלב של מחזור חיי פיתוח	

התוכנה/ אפליקציה.	
הוספת Control Gates לאיכות תוכנה ולאבטחת מידע	
מבדקי אבטחת מידע, Testing	

הזדמנויות למידה

- סרטונים
- NIST. "Security Considerations in the Information System Development Life Cycle – Special publication 800-64 R2.".
- http://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-64r2.pdf
- ISO/IEC. "27001:2013 – Information security management system requirement."
- Official (ISC)2® Guide to the CSSLP® CBK®,. Edited by Mano Paul. (Use the relevant sections from the book).
- SANS. " Software Engineering – Security as a Process in the SDLC.".
- https://www.sans.org/reading-room/whitepapers/securecode/software-engineering-security-process-sdlc-1846. Last accessed 16.06.2016.
- Ramachandran, Muthu. "Software Security Requirements Engineering: State of the Art." In Global Security, Safety and Sustainability: Tomorrow's Challenges of Cyber Security, pp. 313-322. Springer International Publishing, 2015.
- Stuttard, Dafydd and Pinto, Marcus, The Web Application Hacker's Handbook: Finding and Exploiting Security Flaws, 2011
- Gupta, Bhushan B. "Web Application Security–What You Need to Know." (2015).
- William Stalling and Lawrie Brown. "Computer security principles and practice." Third edition. ISBN: 978-1-292-06617-2. (Use the relevant sections from the book).
- NIST. "Technical Guide to Information Security Testing and Assessment – Special publication 800-115." http://csrc.nist.gov/publications/nistpubs/800-115/SP800-115.pdf

דרכי הערכה

- התלמיד יבנה מצגות / ייצור סרטונים המסבירים מושגים מהפרק הנלמד
- מבחן עיוני

פרק 18 – מתודולוגית ביצוע ניסיונות חוסן (תשתית ואפליקציה)

<u>מטרות כלליות</u>

- התלמיד יכיר את העקרונות המתודולוגיות הנהוגות בנושא מבדקי חוסן לתשתיות הארגון – תקשורת, אבטחת מידע, אתר אינטרנט, ואפליקציות ומערכות מחשב

<u>סטנדרט ביצוע</u>

- התלמיד יתאר מתודולוגיות לביצוע מבדקי עמידות
- התלמיד יתאר את הרכיבים השונים של מבדקי העמידות
- התלמיד יתאר זיהוי חולשות פוטנציאליות במערכות
- התלמיד יתאר כלי תוכנה המקובלים בתחום
- התלמיד תהליכי דיווח הממצאים

<u>מוקדי תוכן ומושגים עיקריים</u>

נושא	פירוט
מתודולוגיות לביצוע מבדקי עמידות	
הרכיבים השונים של מבדקי העמידות	
זיהוי חולשות פוטנציאליות במערכות	
כלי תוכנה מקובלים בתחום	
תהליכי דיווח הממצאים	

<u>הזדמנויות למידה</u>

- סרטונים

- SANS. "Penetration Testing: Assessing Your Overall Security Before Attackers Do."
- https://www.sans.org/reading-room/whitepapers/analyst/penetration-testing-assessing-security-attackers-34635
- PCI Security Standards Council. "Information Supplement - Penetration Testing Guidance.".
- https://www.pcisecuritystandards.org/documents/Penetration_Testing_Guidance_March_2015.pdf.
- NIST. "Technical Guide to Information Security Testing and Assessment – Special publication 800-115." http://csrc.nist.gov/publications/nistpubs/800-115/SP800-115.pdf
- Official (ISC)2® Guide to the CISSP® CBK®, Fourth Edition. Edited by Adam Gordon. (Use the relevant sections from the book).

<u>דרכי הערכה</u>

- התלמיד יבנה מצגות / ייצור סרטונים המסבירים מושגים מהפרק הנלמד
- מבחן עיוני / מעשי

פרק 19 – חוק ואתיקה

<u>מטרות כלליות</u>

- התלמיד יכיר את חוקי מדינת ישראל העוסקים בתחומי הגנת הפרטיות ומחשבים, תקינה, החלטות ממשלה ואסדרה בנושא הגנת הסייבר
- התלמיד יכיר את נושא האתיקה של העוסקים במקצוע דוגמת מומחי הקשחת ציוד ובודקי עמידות מערכות.
- התלמיד יכיר את החוקים הבינלאומיים בנושא סייבר, הגנת הפרטיות בעולם – אירופה, ארה"ב .

<u>סטנדרט ביצוע</u>

- התלמיד יתאר את חוקי מדינת ישראל העוסקים בתחומי הגנת הפרטיות ומחשבים, תקינה, החלטות ממשלה ואסדרה בנושא הגנת הסייבר
- התלמיד יסביר את המשמעויות של פעולות שאינן עולות בקנה אחד עם החוק
- התלמיד יתאר את נושא האתיקה המקצועית בתחום

<u>מוקדי תוכן ומושגים עיקריים</u>

נושא	פירוט
חוקי מדינת ישראל	חוק הגנת הפרטיות, חוק המחשבים, הנחיות בנק ישראל, הנחיות הבורסה לני"ע, וכדומה. החלטות ממשלה ואסדרה בנושא הגנת הסייבר
אתיקה מקצועית	

<u>הזדמנויות למידה</u>

- סרטונים
- חוק הגנת הפרטיות התשמ"א – 1981.
- חוק המחשבים תשנ"ה – 1995.
- תקנות הגנת הפרטיות.
- William Stalling and Lawrie Brown. "Computer security principles and practice." Third edition. ISBN: 978-1-292-06617-2. (Use the relevant sections from the book).

- Official (ISC)2® Guide to the CISSP® CBK®, Fourth Edition. Edited by Adam Gordon. (Use the relevant sections from the book).
- J. Tiller. The Ethical Hack: A Framework for Business Value Penetration Testing (New York: Auerbach Publications, 2004).

<u>דרכי הערכה</u>
- התלמיד יבנה מצגות / ייצור סרטונים המסבירים מושגים מהפרק הנלמד
- מבחן עיוני / מעשי

פרק 20 – אבטחה פיזית

<u>מטרות כלליות</u>
- התלמיד יכיר מתודולוגיות שונות ואמצעים להגנת אתרי המחשב הפיזיים, בהם מצוי המידע הארגוני והמחשבים הארגוניים, לרבות סביבת העבודה של העובדים
- התלמיד יכיר את אמצעי האבטחה הפיזיים, מנגנוני הניטור והבקרה והאמצעים העומדים לרשות הארגון לטיפול באירועי קיצון

<u>סטנדרט ביצוע</u>
- התלמיד יתאר הנחיות החוק בדבר אבטחת סביבת המחשוב
- התלמיד יסביר על מה מגנים
- התלמיד יתאר אמצעי אבטחה וניטור למניעת גישה ע"י בלתי מורשים
- התלמיד יתאר אמצעים לטיפול בפני אירועי קיצון שונים

<u>מוקדי תוכן ומושגים עיקריים</u>

נושא	פירוט
הנחיות החוק בדבר אבטחת סביבת המחשוב	
אמצעי אבטחה וניטור למניעת גישה ע"י בלתי מורשים	
אמצעים לטיפול בפני אירועי קיצון שונים	דוגמת הפסקת חשמל, רעידת אדמה, מלחמה

<u>הזדמנויות למידה</u>
- סרטונים
- חוק הגנת הפרטיות התשמ"א – 1981.
- William Stalling and Lawrie Brown. "Computer security principles and practice." Third edition. ISBN: 978-1-292-06617-2. (Use the relevant sections from the book).

- Official (ISC)2® Guide to the ISSAP® CBK®, Second Edition. Edited by Adam Gordon. (Use the relevant sections from the book).
- Security Solutions Magazine. "The Relationship between Physical Security and Information Security." http://www.securitysolutionsmagazine.biz/2013/05/27/the-relationship-between-physical-security-and-information-security/. May 27, 2013. NIST. "An introduction to Computer Security – NIST special publication 800-12."
- csrc.nist.gov/publications/nistpubs/800-12/handbook.pdf.

<u>דרכי הערכה</u>

- התלמיד יבנה מצגות / ייצור סרטונים המסבירים מושגים מהפרק הנלמד
- מבחן עיוני / מעשי

פרק 21 – התנסות מעשית התומכת את הידע התאורטי

<u>מטרות כלליות</u>

- התלמיד יכיר

<u>סטנדרט ביצוע</u>

- התלמיד יתאר

נושא	פירוט

<u>הזדמנויות למידה</u>

<u>דרכי הערכה</u>

- התלמיד יבנה מצגות / ייצור סרטונים המסבירים מושגים מהפרק הנלמד
- מבחן עיוני /מעשי