משרד ראש הממשלה
מערך הסייבר הלאומי
הרשות הלאומית להגנת הסייבר

כתובת לקבלת דואר:
משרד ראש הממשלה, רח' קפלן 3, ירושלים
טלפון 03-7450892, פקס 03-7450820

8 יוני 2017

י"ד סיון תשע"ז

סימוכין: א-ה-0079

סילבוס לקורס מיישם הגנת סייבר

שם הקורס: קורס מיישם הגנת סייבר

משך הקורס: 300 שעות

דרישות קדם: אין

קוד קורס:

עדכון: יוני 2017

1. הקדמה

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.

מהות הקורס הינה העשרת ידע המיישם בהבנת תחום הסייבר, תפישות סייבר, ידע בחוקים ובתקנות הרלוונטיות, סביבות טכנולוגיות, מוצרי אבטחת מידע, תהליכי אבטחה שגרתיים, תהליך טיפול באירוע ואתיקה מקצועית.

הקורס ירחיב וירענן את הידע למועמדים, ויעזור להם להתמקד בלימוד לקראת הבחינה.

2. קהל היעד

קהל היעד הינו אנשי סייבר בגירים, בעלי אזרחות ישראלית, ללא עבר פלילי אשר חפצים לעבור את בחינת האסדרה.

3. מטרות הקורס

א. הכרה והבנת הגנת סייבר מרמת הידע הבסיסי (מבוא להגנת הסייבר) ועד לרמת היכרות טכנולוגית מעמיקה.
ב. הכנה לקראת ביצוע בחינת ההסמכה.

בסיום הקורס הלומד אמור להכיר את השפה ולהבין את מורכבות נושא אבטחת מידע ככלל וסייבר בכלל.

כתובת לקבלת דואר:
משרד ראש הממשלה, רח' קפלן 3, ירושלים
טלפון 03-7450892, פקס 03-7450820

4. תכנים

4.1. תכני הקורס

הקורס מורכב מ-24 תתי קורסים:

#	נושא	מהות הקורס	שעות לימוד עיוני	מעשי
1	מבוא לאבטחת מידע והגנת הסייבר		16	
2	תקני אבטחת מידע וניהול סיכונים		8	2
3	מבנה מחשב		2	
4	יסודות מערכות הפעלה		12	4
5	יסודות תקשורת מחשבים – א'		4	
6	יסודות תקשורת מחשבים – ב'		12	12
7	הגנת גישה בתקשורת ואינטרנט		20	10
8	בידול והפרדת רשתות תקשורת		4	4
9	היבטי אבטחת מידע בציודי תקשורת (הקשחה) ואבטחת מידע		8	8
10	הצפנה ואימות		12	4
11	בקרת גישה		10	4
12	היבטי אבטחת מידע במערכות הפעלה והקשחות שרתים		20	20
13	היבטי אבטחת מידע במסדי נתונים		8	3
14	תוכנות זדוניות וזיהוי אנומליות		12	6
15	דלף מידע		4	2
16	ניהול ורישום אירועי אבטחת מידע (Audit)		6	2
17	טיפול באירועי אבטחת מידע		6	4
18	מחשוב ענן, שירותי אירוח, וירטואליזיה		4	
19	שינוע מידע מ/אל הארגון		2	
20	המשכיות עסקית (BCP/DRP)		4	4
21	אבטחה אפליקטיבית		8	
22	מתודולוגית ביצוע ניסיונות חוסן (תשתית ואפליקציה)		8	10
23	חוק ואתיקה		8	1
24	אבטחה פיסית		2	
	סיכום		**200**	**100**
	סה"כ שעות קורס מומלצות		**300**	

כתובת לקבלת דואר:
משרד ראש הממשלה, רח' קפלן 3, ירושלים
טלפון 03-7450892, פקס 03-7450820

4.2. פירוט תכני הקורס

4.2.1. מבוא לאבטחת מידע והגנת הסייבר

תת קורס ראשון בסדרת הקורסים מתמקד בהכרת מונחי יסוד ובניית השפה בה העוסקים בתחום מדברים, כותבים ודנים.

בסיום הקורס הלומד אמור להכיר את השפה להבין את מורכבות נושא אבטחת מידע ככלל וסייבר בכלל.

משך לימוד הנושא – 16 שעות לימוד.

דרישות קדם: אין.

אסטרטגית לימוד: פרזנטציה

שיטות הערכה: מבחני הכנה.

<u>תכני הקורס</u>

- 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 לרבות תקיפת מחשב מרחוק, מתוך הארגון, חדירה פיזית למתחמי מחשב.
- Social Engineering, תקיפות משולבות, שימוש במייל, הפניה לאתרים נושאי תוכנה זדונית.
- סוגי פגיעות במערכות / במידע לרבות בהיבטי זמינות, אמינות, שלמות וסודיות.
- השלכות ומשמעויות הפגיעה מבחינה כלכלית , מוניטין ומשמעויות 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.

ביבליוגרפיה:

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. Last accessed 16.06.2016

A. 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.

4.2.2. תקני אבטחת מידע וניהול סיכונים

תת הקורס עוסק בתיאור תקני האבטחה וה-Best practices, המקובלים בתחום אבטחת המידע והסייבר. יסודות סקר סיכונים, סוגי סקרים, כיצד מתבצע סקר סיכונים ומה מטרותיו, הפעילויות להקטנת הסיכון, מושגים של סיכון, סיכון שיורי.

בסיום תת הקורס על הלומד להכיר את התקנים, וה-Best practices, להבין מה הסיבה והיתרון המתקבל מקיומם, כיצד הם משפרים את ההגנה על הארגון, מהם חסרונותיהם, וההבדלים בין הסטנדרטים. עליו להבין את מושגי הסיכון ואת תהליך וביצוע סקר סיכונים וכן את הפעילות להקטנת סיכונים.

משך לימוד הנושא – 8 שעות לימוד.

דרישות קדם: אין.

אסטרטגית לימוד: פרזנטציה

שיטות הערכה: מבחני הכנה

תכני הקורס

- הסטנדרטים המקובלים של ISO27K, סטנדרטים של סקרי סיכונים.
- מתודולוגיות לביצוע סקרי סיכונים.
- השלבים השונים של סקר סיכונים.
- היעדים של סקרי סיכונים.

- סוגים – כמותי איכותי משולב.
- נושא הסקרים – אפליקציות, תשתיות, למערכות האבטחה, שילוב סקרים.

ביבליוגרפיה:

http://www.isaca.org/journal/archives/2010/volume-
. Last accessed 1/pages/performing-a-security-risk-assessment1.aspx
13.06.2016.
http://searchsecurity.techtarget.com/magazineContent/Information-
. Last accessed 13.06.2016.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. Last accessed 13.06.2016.

OWASP, https://www.owasp.org/index.php/OWASP_Risk_Rating_Methodology. Last accessed 13.06.2016.
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. Last accessed 13.06.2016

NIST, "Guide for Conducting Risk assessments". NIST Special Publication 800-30. Available online.
http://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-
. Last accessed 13.06.201630r1.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 certification: 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.

4.2.3. מבנה מחשב

תת הקורס מיועד להכיר לתלמידים יסודות מבנה מחשב בהיבטי של חומרה, מבנה סכמתי, תפקידי הרכיבים וכן מתקפות ידועות על חלק מהרכיבים (דוגמא מתקפה על ה-BIOS).

בסיום הקורס הלומד אמור להכיר את רכיבי החומרה העיקריים ואת תפקידם. בנוסף אמור הלומד להכיר מספר תקיפות ומאפייני תקיפות מול הרכיבים הרלוונטיים.

משך לימוד הנושא – 2 שעות לימוד.

דרישות קדם: אין.

אסטרטגית לימוד: פרזנטציה

שיטות הערכה: מבחני הכנה.

<u>תכני הקורס</u>

- הכרת חלקי מחשב, לדוגמא: RAM, ROM, ALU, CPU לרבות ריבוי ליבות, GPU, אמצעי אחסון, BIOS,
- UEFI (Unified extensible firmware interface).
- תפקיד כל רכיב, מבנה סכמתי, אופני הקישור בין הרכיבים – BUS, הקישור בין כל הרכיבים
- מתקפות ידועות על חלק מהרכיבים (דוגמא מתקפה על ה- BIOS).

ביבליוגרפיה:

הערה: לעניין מבנה חומרת המחשב מצורפים מספר הפניות. יחד עם זאת אין בכוונתנו לספק לכך הפניה ספציפית מפני שהנושא הוא כוללני ואינו נידרש ברמה אקדמית.

לעניין מתקפות יש מספר הפניות ייעודיות.

Computer Organization and architecture (10th Edition). William Stallings. ISBN-13: 978-0134101613

Modern Operating systems. Andrew S. Tanenbaum and Herbert Boss. ISBN-13: 978-1292061429

http://resources.infosecinstitute.com/hardware-attacks-backdoors-and-electronic-component-qualification/. Last accessed 15.06.2016 << >>

BASIC STRUCTURE OF COMPUTERS, lecture notes. Available online.

.http://www.iare.ac.in/sites/default/files/lecture_notes/Lecture%20notes_0.pdf

Last accessed 15.06.2016

Franklin, M. "Computer Architecture and Organization: From Software to Hardware". Pearson Education, 2012. Available online.

http://ece.umd.edu/~manoj/350/notes/book.pdf. Last accessed 15.06.2016.

Known attacks on computer hardware

"Summary of Attacks against BIOS and Secure Boot – Defcon presentation". Available online. https://www.defcon.org/images/defcon-22/dc-22-presentations/Bulygin-Bazhaniul-Furtak-Loucaides/DEFCON-22-Bulygin-Bazhaniul-Furtak-Loucaides-Summary-of-attacks-against-BIOS-UPDATED.pdf. Last accessed 15.06.2016

"Attacking and Defending BIOS in 2015 – Intel Security". Available online. http://www.intelsecurity.com/advanced-threat-research/content/AttackingAndDefendingBIOS-RECon2015.pdf. Last accessed 15.06.2016

Gruhn, Michael, and Tim Muller. "On the practicability of cold boot attacks." In Availability, Reliability and Security (ARES), 2013 Eighth International Conference on, pp. 390-397. IEEE, 2013.

Kovah, Xeno, Corey Kallenberg, John Butterworth, and Sam Cornwell. "SENTER Sandman: Using Intel TXT to Attack BIOSes." (2015).

Kallenberg, Corey, and Xeno Kovah. "BIOS Necromancy: Utilizing "Dead Code" for BIOS Attacks." (2015).

Bauer, Johannes, Michael Gruhn, and Felix C. Freiling. "Lest we forget: Cold-boot attacks on scrambled DDR3 memory." Digital Investigation 16 (2016): S65-S74.

Schiffman, Joshua, and David Kaplan. "The SMM Rootkit Revisited: Fun with USB." In Availability, Reliability and Security (ARES), 2014 Ninth International Conference on, pp. 279-286. IEEE, 2014.

Bhunia, Swarup, Michael S. Hsiao, Mainak Banga, and Sriram Narasimhan. "Hardware Trojan attacks: threat analysis and countermeasures." Proceedings of the IEEE 102, no. 8 (2014): 1229-1247.

. http://www.theregister.co.uk/2011/09/14/bios_rootkit_discovered/

4.2.4. יסודות מערכות הפעלה

תת הקורס מיועד להכיר לתלמידים יסודות מבנה מערכות הפעלה, ארכיטקטורה, אופן הקישור בין החומרה לתוכנה.

בסיום הקורס הלומד אמור להכיר את רכיבי מערכת ההפעלה, הארכיטקטורה הבסיסית וההבדלים בין מערכות ההפעלה השונות.

משך לימוד הנושא – 12 שעות לימוד.

דרישות קדם: לימוד נושא מבנה המחשב.

אסטרטגית לימוד: פרזנטציה, תרגול מעשי.

שיטות הערכה: מבחני הכנה.

<u>תכני הקורס</u>

- ארכיטקטורה בסיסית של מערכות הפעלה. היכרות עם הרכיבים המרכזיים (דוגמא DLL של Win) של מערכות ההפעלה הבאות: Unix, Win, Android, VM.
- כיצד מערכת ההפעלה נפרסת בזיכרון המחשב. מימוש Virtual memory.
- אופן הקישור בין התוכנה לחומרה (לדוגמא HAL של אנדרואיד).
- הבדלים בין מערכות הפעלה השונות.

ביבליוגרפיה:

Computer Organization and architecture. William Stallings. ISBN-13: 978-0134101613

Operating Systems: Internals and Design Principles. William Stallings. ISBN-13: 978-0133805918

Modern Operating systems. Andrew S. Tanenbaum and Herbert Boss. ISBN-13: 978-1292061429

. Karim Yahgmour. ISBN:978-1-4493-0828-5.Embedded Android

Android Hacker's Handbook: Joshua J. Drake, Zach Lanier, Collin Mulliner, Pau Oliva Fora, Stephen A. Ridley, Georg Wicherski: 9781118608647: Amazon.com: Books. (Internal of android from the security point of view).

4.2.5. יסודות תקשורת מחשבים - א

הקורס מיועד להכיר לתלמידים את יסודות תקשורת המחשבים. שכבות בתקשורת, סוגי רשתות תקשורת וההבדלים ביניהן, ציוד תקשורת תפקידו והשכבה בה פועל.

בסיום הקורס על הלומד לדעת את סוגי רשתות התקשורת, הבדלים, ומימושים שלהן.

משך לימוד הנושא – 4 שעות לימוד.

דרישות קדם: לימוד נושא מבנה המחשב.

אסטרטגית לימוד: פרזנטציה, תרגול מעשי.

שיטות הערכה: מבחני הכנה.

תכני הקורס

- מודל 7 השכבות (OSI),
- רכיבי תקשורת – Router, switch.
- סוגי רשתות: WAN/LAN, Wireless, רשתות של Bluetooth.

ביבליוגרפיה:

Data and Computer Communications (Eighth Edition). William Stallings. Available online. https://abmpk.files.wordpress.com/2013/04/data-and-computer-comm-8e-william-stallings.pdf. Last accessed 16.06.2016

Wireless Communication and Networks. William Stallings. ISBN: 0-13-191835-4.

Computer Networks. Andrew S. Tanenbaum and David J. Wetherall. ISBN-13: 978-0-13-212695-3

TCP/IP tutorial and Technical Overview – IBM Redbooks. L Parziale. ISBN 0738494682 Available online. https://www.redbooks.ibm.com/redbooks/pdfs/gg243376.pdf. Last accessed 16.06.2016

4.2.6. יסודות תקשורת מחשבים - ב

הקורס מתמקד בפרוטוקולי התקשורת המרכזיים, שימושם והיבטי אבטחה של כל פרוטוקול. אין חובה לדעת את נבכי ה-RFC של כל פרוטוקול.

בנוסף הלומד יתבקש ללמוד את הקשרים בין הפרוטוקול לציוד התקשורת, והשכבות בהן הפרוטוקול פועל וחולשות שהתפרסמו.

בסיום הקורס על הלומד לדעת את סוגי הפרוטוקולים השונים, לציין את תפקידם, היבטי אבטחת מידע וחולשות מרכזיות, מי מפעיל איזה פרוטוקול.

משך לימוד הנושא – 12 שעות לימוד.

דרישות קדם: לימוד נושא מבנה המחשב.

אסטרטגית לימוד: פרזנטציה, תרגול מעשי.

שיטות הערכה: מבחני הכנה.

<u>תכני הקורס</u>

- תיאור הפרוטוקולים, שימושים והיבטי אבטחה – חולשות שהתפרסמו. אין חובה לדעת את נבכי הפרוטוקול כפי המופיע ב- RFC. חולו
- פרוטוקולים: TCP/IP, UDP, FTP, HTTP , SNTP, RIP, SIP, SNMP, ICMP, DNS, RADIUS, ARP.

ביבליוגרפיה:

Data and Computer Communications (Eighth Edition). William Stallings. Available online. https://abmpk.files.wordpress.com/2013/04/data-and-computer-comm-8e-william-stallings.pdf. Last accessed 16.06.2016

Wireless Communication and Networks. William Stallings. ISBN: 0-13-191835-4.

Computer Networks. Andrew S. Tanenbaum and David J. Wetherall. ISBN-13: 978-0-13-212695-3

TCP/IP tutorial and Technical Overview – IBM Redbooks. L Parziale. ISBN 0738494682 Available online. https://www.redbooks.ibm.com/redbooks/pdfs/gg243376.pdf. Last accessed 16.06.2016

Regarding attacks:

Nalavade, Kamini, and B. B. Meshram. "Denial of Service on TCP/IP Security Protocols: Vulnerabilities, Tools and Countermeasures." published in International Journal of Data and Network Security (IJDNS) in Jan (2014).

Washbourne, Logan. "A survey of P2P Network security." arXiv preprint arXiv: 1504.01358 (2015).

Computer security principles and practice. William Stalling and Lawrie Brown. Third edition. ISBN: 978-1-292-06617-2. (Use the relevant sections in the book).

4.2.7. הגנת גישה בתקשורת ואינטרנט

הקורס מתמקד במנגנוני ההגנה של רשתות המחשבים שבארגון, מוצרי אבטחה, גישה מרחוק למשאבי הארגון וההגנה על דרכי גישה אלו. היבטי אבטחה בעת קישור הארגון לאינטרנט. מנגנוני אבטחה ופרוטוקולים אפליקטיביים של השכבות הגבוהות במודל OSI. בקורס ידונו הפרוטוקולים המרכזיים, שימושם והיבטי אבטחה של הפרוטוקולים.

בסיום הקורס על הלומד לדעת את מנגנוני ההגנה המתאימים לכל דרך גישה למשאבי הארגון. היבטי אבטחת מידע וחולשות מרכזיות. הבעייתיות שבקישור הרשת הארגונית כולה/ או חלקה לאינטרנט, מנגנוני הגנה, סוגי הפרוטוקולים השונים המשמשים לקישור אפליקטיבי, לציין את תפקידם, היבטי אבטחת מידע וחולשות מרכזיות, מי מפעיל איזה פרוטוקול.

משך לימוד הנושא – 20 שעות לימוד.

דרישות קדם: לימוד נושא מבנה המחשב, יסודות תקשורת מחשבים א ו-ב, הצפנה ואימות

אסטרטגית לימוד: פרזנטציה, תרגול מעשי.

שיטות הערכה: מבחני הכנה.

<u>תכני הקורס</u>

- 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,
- מוצרי אבטחה,
- בנית DMZ, (נושא זה למעשה מבצע שימוש ביידע קודם של הנושאים שנלמדו.
- תיאור הפרוטוקולים האפליקטיביים, HTML5, HTML3, WebRTC, שימושים והיבטי אבטחה – חולשות שהתפרסמו. אין חובה לדעת את נבכי הפרוטוקול כפי שמופיע ב-RFC.

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

ביבליוגרפיה:

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).

4.2.8. בידול והפרדת רשתות תקשורת

הקורס מתמקד במנגנונים ומוצרים שעניינם הפרדת רשתות. אם רשתות פנים ארגוניות ואם של הרשת הארגונית כלפי העולם החיצון.

בסיום הקורס על הלומד לדעת את מנגנוני הבידול המתאים, יתרונות חסרונות. היבטי אבטחת מידע וחולשות מרכזיות. כיצד יש להקשיח את רשת התקשורת מפני מתקפות מבחוץ.

משך לימוד הנושא – 4 שעות לימוד.

דרישות קדם: לימוד נושא מבנה המחשב.

אסטרטגית לימוד: פרזנטציה, תרגול מעשי.

שיטות הערכה: מבחני הכנה.

<u>תכני הקורס</u>

- מדוע נדרש הבידול, 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 דוגמת Firewall, מחשבי Proxy, Mail relay, Content filtering, מוצרי Air Gap.
- הקשחת רשת התקשורת הארגונית

ביבליוגרפיה:

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).

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).

4.2.9. הצפנה ואימות

הקורס מתמקד ביסודות ההצפנה ופרוטוקולי אימות. בנוסף ילמדו פרוטוקולי התקשורת המשמשים לאימות משתמשים שימושם והיבטי אבטחה של כל פרוטוקול ופרוטוקול. אין חובה לדעת את נבכי ה-RFC של כל פרוטוקול ופרוטוקול.

בנוסף הלומד יתבקש ללמוד את הקשרים בין הפרוטוקול לציוד התקשורת, והשכבות בהן הפרוטוקול פועל.

בסיום הקורס על הלומד לדעת את סוגי הפרוטוקולים השונים, לציין את תפקידם, היבטי אבטחת מידע וחולשות מרכזיות, מי מפעיל איזה פרוטוקול.

משך לימוד הנושא – 12 שעות לימוד.

דרישות קדם:

אסטרטגית לימוד: פרזנטציה, תרגול מעשי.

שיטות הערכה: מבחני הכנה.

<u>תכני הקורס</u>

- הצפנה סימטרית – DES 3DES, א-סימטרית, דפי הלמן, RSA,
- אימות משתמשים באמצעות דפי הלמן.

- יסודות - Certificate Authority, לאימות קצוות תקשורת, זיהוי משתמשים (הנושא של זיהוי ציוד ילמד בנפרד).
- פרוטוקולי תקשורת התומכים בנושא של הצפנה ואימות דוגמת: IPSEC, SSL, SSH, HTTPS.

ביבליוגרפיה:

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.

4.2.10. היבטי אבטחת מידע במערכות הפעלה והקשחת שרתים

הקורס מיועד להכיר לתלמידים את היבטי אבטחת המידע במערכות ההפעלה השונות. להכיר ללומדים את העקרונות של הקשחת השרתים והשירותים השונים המטופלים במסגרת תהליכי ההקשחה.

בסיום הקורס על הלומד לדעת את ההיבטים המרכזיים של אבטחת מידע בכל מערכת הפעלה. חולשות מרכזיות הקימות במערכת. מתקפות ידועות. תהליכי הקשחה, התהליכים השונים והשירותים הניתנים ע"י מחשב מוקשח.

משך לימוד הנושא – 20 שעות לימוד.

דרישות קדם: לימוד נושא מבנה המחשב.

אסטרטגית לימוד: פרזנטציה, תרגול מעשי.

שיטות הערכה: מבחני הכנה.

<u>תכני הקורס</u>

- 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 שעניינו 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.

ביבליוגרפיה:

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. Last accessed 16.06.2016

4.2.11. היבטי אבטחת מידע במסדי נתונים

הקורס מיועד להכיר לתלמידים את היבטי אבטחת המידע – גישת משתמשים, הגנה על מידע נייח, במערכות מסדי נתונים וב- Storage systems וכן חולשות ואופני הגנה.

בסיום הקורס על הלומד לדעת את ההיבטים המרכזיים של אבטחת מידע במסדי נתונים כאמור לעייל, חולשות מרכזיות הקיימות במערכת, אופני ההגנה, מוצרים משלימים ומתקפות ידועות.

משך לימוד הנושא – 8 שעות לימוד.

דרישות קדם : לימוד נושא מבנה המחשב.

אסטרטגית לימוד: פרזנטציה, תרגול מעשי.

שיטות הערכה : מבחני הכנה.

תכני הקורס

- 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.
- מערכות Storage systems ואבטחת המידע בהם.

ביבליוגרפיה:

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. Last accessed 16.06.2016.

4.2.12. המשכיות עסקית (BCP/ DRP)

הקורס מיועד להכיר לתלמידים את נושא הגיבוי, השחזור והתאוששות מאסון על היבטיו וברמות השונות של גיבוי ושחזור. כמו כן יילמדו תמיכת מערכת ההפעלה בנושא ומוצרים משלימים והיבטי אבטחת מידע בנושא.

בנוסף הקורס יעסוק ב-Storage systems, חולשות ואופני הגנה.

בסיום הקורס על הלומד לדעת את ההיבטים המרכזיים של נושא הגיבוי השחזור וההתאוששות מאסון, תמיכת מערכת ההפעלה ומוצרים משלימים.

משך לימוד הנושא – 4 שעות לימוד.

דרישות קדם: לימוד נושא מבנה המחשב.

אסטרטגית לימוד: פרזנטציה, תרגול מעשי.

שיטות הערכה: מבחני הכנה.

<u>תכני הקורס</u>

- תאוריה של DRP and BCP, מתודולוגית לגיבוי ושחזור - 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. לדוגמא: 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.

ביבליוגרפיה:

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

4.2.13. תוכנות זדוניות וזיהוי אנומליות

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

בסיום הקורס על הלומד לדעת את ההיבטים המרכזיים של נושא התוכנה הזדונית והגנת הסביבה הממוחשבת מפניהם. דרכי הפצה, מניעה והתמודדות. מוצרים, קסטומיזציה של מוצרים, תפעול שותף של מוצרי ההגנה. להכיר את נושא זיהוי אנומליות בסיום הקורס על הלומד לדעת את ההיבטים המרכזיים של נושא זיהוי אנומליות, טיפול בסיסי בהתאם לנהלי הארגון ומוצרים תומכים בתחום.

משך לימוד הנושא – 12 שעות לימוד.

דרישות קדם: לימוד נושא מבנה המחשב.

אסטרטגית לימוד: פרזנטציה, תרגול מעשי.

שיטות הערכה: מבחני הכנה.

<u>תכני הקורס</u>

- תאוריה וסוגים של תוכנות זדוניות, לדוגמא: APT ,Trojan.
- 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 ובמחשבים.
- 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

ביבליוגרפיה:

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. Last accessed 17.06.2016.

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.

4.2.14. בקרת גישה

הקורס מיועד להכיר לתלמידים את נושא בקרת הגישה. הקורס מחולק לשני חלקים:

בחלק הראשון ילמדו הנושאים של בקרת גישה של משתמשים, תוכנות לרכיבים, מידע במערכות המחשב הארגוניות ורכיבים שונים ברשת הארגונית. כמו כן ייסקרו מוצרים שונים בתחום.

בחלק השני של הקורס ילמד התחום של מערכות ארגוניות לזיהוי ואימות משתמשים וחומרה.

בסיום הקורס על הלומד לדעת את ההיבטים המרכזיים של בקרת הגישה, תהליכים, התמודדות עם תקלות, וטיפול בחריגים, מערכות ארגוניות לזיהוי ואימות משתמשים.

משך לימוד הנושא – 10 שעות לימוד.

דרישות קדם: לימוד נושא מבנה המחשב.

אסטרטגית לימוד: פרזנטציה, תרגול מעשי.

שיטות הערכה: מבחני הכנה.

תכני הקורס

חלק ראשון

- זיהוי ואימות משתמשים תאוריה, חזרה קצרה על המנגנונים הקיימים במערכת ההפעלה לזיהוי ואימות משתמשים.
- המושג של Multifactor authentication.
- תוכנה/חומרה נוספת לזיהוי ואימות משתמשים דוגמת: Tokens, Smart cards, ו- Biometric devices.
- 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.

חלק שני

- הגדרה ושימוש במערכות Identity management, כלל ארגוניות לזיהוי ואימות משתמשים והרשאותיהם במערכות השונות, Credentials.
- התממשקות עם DNS לניהול משתמשים כאמור.
- 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.

ביבליוגרפיה:

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. Last accessed 17.06.2016.
SANS, "An Introduction to Identity Management.". Available online. https://www.sans.org/reading-room/whitepapers/authentication/introduction-identity-management-852. Last accessed 17.06.2016.

INFOSEC INSTITUTE, "Chapter 11 – Identity management and Access controls.". Available online. http://resources.infosecinstitute.com/identity-management/. Last accessed 17.06.2016.
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. Last Accessed 16.06.2016.
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
Last accessed 16.06.2016.
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. Last accessed 16.06.2016.

4.2.15. דלף מידע

הקורס מיועד להכיר לתלמידים את נושא דלף המידע הארגוני, הסכנות שבו, תהליכי מניעה/ צמצום/ גילוי. בנוסף ייסקרו מוצרים התומכים בהגנת המידע הארגוני מפני דלף מידע והפעולות שיש לנקוט בעת גילוי כאמור.

בסיום הקורס על הלומד לדעת את ההיבטים המרכזיים של נושא דלף המידע וכיצד ניתן לפעול למניעתו/ צמצומו/ גילוי עובדת קיום דלף מידע.

משך לימוד הנושא – 4 שעות לימוד.

דרישות קדם: לימוד נושא מבנה המחשב.

אסטרטגית לימוד: פרזנטציה, תרגול מעשי.

שיטות הערכה: מבחני הכנה.

<u>תכני הקורס</u>

- הגדרת המושג, 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 – דוגמת מוצרי content filtering

ביבליוגרפיה:

SANS Institute, "Data leakage – Threats and Mitigation", available online, https://www.sans.org/reading-room/whitepapers/awareness/data-leakage-threats- . Last accessed 13.06.2016mitigation-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. Last accessed 16.06.2016

4.2.16. ניהול ורישום של אירועי אבטחת מידע (Audit)

הקורס מיועד להכיר לתלמידים 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, וכו'. כמו כן ייסקרו מוצרים תומכים בתחום.

בסיום הקורס על הלומד לדעת את ההיבטים המרכזיים של ניהול ורישום של אירועי אבטחה אופן ההתמודדות, - מותנה בנהלי הארגון.

משך לימוד הנושא – 6 שעות לימוד.

דרישות קדם: לימוד נושא מבנה המחשב.

אסטרטגית לימוד: פרזנטציה, תרגול מעשי.

שיטות הערכה: מבחני הכנה.

<u>תכני הקורס</u>

- חלק תאורטי מהו הנושא מדוע נידרש ניהול ידני לחצי ידני,

- מוצרים SOC (security operation center) ומוצרים תומכים.
- מוצרי SIEM (security information event management).
- מוצרי NAC (network access control).
- סנסורים – התקנה וקונפיגורציה. תהליך הגדרה של חוקים במוצר, התראות שווא 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.

ביבליוגרפיה:

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. Last accessed 16.06.2016

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. Last accessed 16.06.2016.

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. Last Accessed 16.06.2016

McAffe, "Creating and maintaining a SOC.". Available online. http://www.mcafee.com/de/resources/white-papers/foundstone/wp-creating-maintaining-soc.pdf. Last Accessed 16.06.2016

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

כתובת לקבלת דואר:
משרד ראש הממשלה, רח' קפלן 3, ירושלים
טלפון 03-7450892, פקס 03-7450820

4.2.17. היבטי אבטחת מידע בציודי תקשורת הקשחתו

קורס זה הינו קורס המשך לקורס הקשחת שרתים ומיועד "להשלים את התמונה" ללומד.

הקורס מיועד להכיר לתלמידים את נושא הקשחת ציוד התקשורת, נתבים, בסביבות התקשורת השונות.

נושא הקשחת ציוד תקשורת הוא נושא טכני המחייב ידע מעמיק ביותר. קורס זה בא להכיר ללומד את העקרונות והפעולות הבסיסיות בנושא במערכות ההפעלה השונות ולהעניק לו הבנה בסיסית לגבי מה מתרחש במחשב המוקשח.

משך לימוד הנושא – 8 שעות לימוד.

דרישות קדם: לימוד נושא מבנה המחשב.

אסטרטגית לימוד: פרזנטציה, תרגול מעשי.

שיטות הערכה: מבחני הכנה.

<u>תכני הקורס</u>

- חלק תאורטי - מדוע נידרש לבצע הקשחת נתבים. עקרונות תהליך ההקשחה.
- הקשחה תלוית ציוד תקשורת (לדוגמא נתב של CISCO לאומת נתב של חברה אחרת).
- עדכון תוכנה, firmware, לציוד התקשורת.
- בדיקת קשיחות לציוד.
- מוצרים תומכים בהקשחה.
- תאום עם מוצרי אבטחה לדיווח על אנומליות.

ביבליוגרפיה:

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).

(Accessed 12.06.2016)https://www.techopedia.com/definition/24833/hardening

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. Last accessed 14.06.2016

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 (Accessed 13.06.2016)
See also: https://www.techopedia.com/definition/24833/hardening. Last accessed 12.06.2016.

4.2.18. מחשוב ענן, שירותי אירוח, וירטואליזציה

קורס זה בא להכיר בפני הלומד את עקרונות הענן ושירותי האירוח.

משך לימוד הנושא – 4 שעות לימוד.

דרישות קדם: לימוד נושא מבנה המחשב.

אסטרטגית לימוד: פרזנטציה, תרגול מעשי.

שיטות הערכה: מבחני הכנה.

<u>תכני הקורס</u>

מחשוב ענן

- הכרות, הסוגים השונים של מחשוב ענן. קבלת דיווחים מהלוגים השונים והבנתם. היבטי חוק. זיהוי אנומליות, מוצרים תומכי אבטחה של האורח והמארח.

שירותי אירוח

- הכרות, הסוגים השונים של משירותי אירוח. קבלת דיווחים מהלוגים השונים והבנתם. היבטי חוק. זיהוי אנומליות, מוצרים תומכי אבטחה של האורח והמארח.

וירטואליזציה

- הכרות, מדוע נדרשת, סביבת VM, לסוגיו, היבטי אבטחה מהיבט החוק מפני שהנושא דנן נלמד מהיבטים טכניים בעבר.

ביבליוגרפיה:

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.

כתובת לקבלת דואר:
משרד ראש הממשלה, רח' קפלן 3, ירושלים
טלפון 03-7450892, פקס 03-7450820

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

See also:

https://spaces.internet2.edu/display/2014infosecurityguide/Cloud+Computing+Security

4.2.19. שינוע מידע מהארגון ואליו

קורס זה בא להכיר בפני הלומד את העקרונות המתודולוגיות הנהוגות בנושא של שינוע מידע מהארגון ואליו באמצעים פיזיים דוגמת מצאי מידע מגנטיים ואופטיים. מטבע הדברים נושא זה הינו תלויי ארגון, המידע שבארגון והנחיות החוק.

בסיום הקורס הלומד אמור לדעת ולהכיר את היבטי אבטחת המידע והסיכונים הקיימים בעת שינוע מידע מ /אל הארגון והשיטות המקובלות להגן על מידע זה.

משך לימוד הנושא – 4 שעות לימוד.

דרישות קדם :

אסטרטגית לימוד: פרזנטציה, תרגול מעשי.

שיטות הערכה : מבחני הכנה.

תכני הקורס

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

ביבליוגרפיה:

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.". . Last http://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-88r1.pdf Accessed 16.06.2016.

4.2.20. אבטחה אפליקטיבית

קורס זה בא להכיר בפני הלומד את העקרונות המתודולוגיות הנהוגות בנושא הטמעת היבטי אבטחת מידע בתוכנה, ניהול שינויי תוכנה והיבטים של מבדקי אבטחת מידע בתוכנה. כמו כן יילמד הקשר בין איכות תוכנה לאבטחת מידע ואמינות תוכנה.

בסיום הקורס הלומד אמור להכיר את התהליכים השונים למימוש בעת מחזור החיים של פיתוח תוכנה ושינויים בתוכנה.

משך לימוד הנושא – 4 שעות לימוד.

דרישות קדם:

אסטרטגית לימוד: פרזנטציה, תרגול מעשי.

שיטות הערכה: מבחני הכנה.

<u>תכני הקורס</u>

- 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.

ביבליוגרפיה:

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

– Information security management system requirement."13ISO/IEC. "27001:20

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-. Last accessed 16.06.2016.security-process-sdlc-1846

Ramachandran, Muthu. "Software Security Requirements Engineering: State of the Art." In *Global Security, Safety and Sustainability: Tomorrows 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
Last accessed 16.06.2016.

4.2.21. מתודולוגיות ביצוע בדיקות חוסן – תשתיות ואפליקציות

קורס זה בא להכיר בפני הלומד את העקרונות המתודולוגיות הנהוגות בנושא מבדקי חוסן לתשתיות הארגון – תקשורת, אבטחת מידע, אתר אינטרנט, אפליקציות ומערכות מחשב.

בסיום הקורס הלומד אמור להכיר את הנושאים השונים תהליכי ביצוע מבדקי עמידות.

משך לימוד הנושא – 4 שעות לימוד.

דרישות קדם : אבטחה אפליקטיבית

אסטרטגית לימוד: פרזנטציה, תרגול מעשי.

שיטות הערכה : מבחני הכנה.

<u>תכני הקורס</u>

- מתודולוגיות לביצוע מבדקי עמידות.
- הרכיבים השונים של מבדקי העמידות.
- זיהוי חולשות פוטנציאליות במערכות.

- הכרות עם כלי תוכנה מקובלים בתחום.
- תהליכי דיווח המימצאים.

ביבליוגרפיה:

SANS. "Penetration Testing: Assessing Your Overall Security Before Attackers Do." https://www.sans.org/reading-room/whitepapers/analyst/penetration-testing-assessing-security-attackers-34635 . Last accessed 16.06.2016

PCI Security Standards Council. "Information Supplement - Penetration Testing Guidance.". https://www.pcisecuritystandards.org/documents/Penetration_Testing_Guidance_March_2015.pdf . Last accessed 16.06.2016

NIST. "Technical Guide to Information Security Testing and Assessment – Special publication 800-115." http://csrc.nist.gov/publications/nistpubs/800-115/SP800-115.pdf
Last accessed 16.06.2016.

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

כתובת לקבלת דואר:
משרד ראש הממשלה, רח' קפלן 3, ירושלים
טלפון 03-7450892, פקס 03-7450820

4.2.22. חוק ואתיקה

הקורס בנוי משלושה חלקים קצרים.

החלק הראשון מתמקד בהכרת חוקי מדינת ישראל העוסקים בתחומי הגנת הפרטיות ומחשבים, תקינה, החלטות ממשלה ואסדרה בנושא הגנת הסייבר.

החלק השני של הקורס יעסוק באתיקה של העוסקים במקצוע דוגמת מומחי הקשחת ציוד ובודקי עמידות מערכות.

החלק השלישי של הקורס יעסוק בחוקים בינלאומיים בנושא סייבר, הגנת הפרטיות בעולם – אירופה, ארה"ב.

בסיום הקורס הלומד אמור להכיר החוקים, התקנות וההנחיות בארץ, להבין מהיכן נובעים השינויים בהנחיות השונות, להבין את המשמעויות של פעולות שאינן עולות בקנה אחד עם החוק. להבין את מחויבותו האתית למקצוע ולמקום העבודה.

משך לימוד הנושא – 8 שעות לימוד.

דרישות קדם: אין.

אסטרטגית לימוד: פרזנטציה

שיטות הערכה: מבחני הכנה.

<u>תכני הקורס</u>

- חוקי מדינת ישראל: חוק הגנת הפרטיות, חוק המחשבים, הנחיות בנק ישראל, הנחיות הבורסה לני"ע, וכו'. החלטות ממשלה ואסדרה בנושא הגנת הסייבר.
- אתיקה מקצועית.

ביבליוגרפיה:

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).

כתובת לקבלת דואר:
משרד ראש הממשלה, רח' קפלן 3, ירושלים
טלפון 03-7450892, פקס 03-7450820

בלמ"ס

4.2.23. אבטחה פיזית

סביבת המחשב הארגונית אמורה להיות מוגנת ומאובטחת מפני חדירה פיזית, גישה ע"י בלתי מורשים או אבטחה מפני אירועי קיצון דוגמת רעידות אדמה. קורס זה מציג בפני הלומד מתודולוגיות שונות ואמצעים להגנת אתרי המחשב הפיזיים, בהם מצוי המידע הארגוני והמחשבים הארגוניים, לרבות סביבת העבודה של העובדים.

בסיום הקורס הלומד אמור להכיר את אמצעי האבטחה הפיזיים, מנגנוני הניטור והבקרה והאמצעים העומדים לרשות הארגון לטיפול באירועי קיצון.

משך לימוד הנושא – 8 שעות לימוד.

דרישות קדם: המשכיות עסקית, חוק ואתיקה.

אסטרטגית לימוד: פרזנטציה

שיטות הערכה: מבחני הכנה.

<u>תכני הקורס</u>

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

ביבליוגרפיה:

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. Last accessed 16.06.2016.

NIST. "An introduction to Computer Security – NIST special publication 800-12." csrc.nist.gov/publications/nistpubs/800-12/handbook.pdf.

4.2.24. טיפול באירועי אבטחה

בקורס זה מציג בפני הלומד את העקרונות של טיפול באירועי אבטחה. הבנת הסיטואציה של קיום מתקפה, שלבי המתקפה וכיצד לטפל באירוע. קורס זה מהווה אינטגרציה של הידע הנלמד בקורסים שונים.

בסיום הקורס הלומד אמור להבין כיצד נושאים שונים שלמד מתממשקים, ואת יסודות הטיפול באירוע אבטחה. יש לציין כי נושאים אלה הם תלויי ארגון והמידע שבארגון, ותלויי חוק.

משך לימוד הנושא – 6 שעות לימוד.

דרישות קדם: לימוד נושא מבנה המחשב.

אסטרטגית לימוד: פרזנטציה, תרגול מעשי.

שיטות הערכה: מבחני הכנה.

<u>תכני הקורס</u>

- הכרת סוגי תקיפות דוגמת: 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.

ביבליוגרפיה:

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).

כתובת לקבלת דואר:
משרד ראש הממשלה, רח' קפלן 3, ירושלים
טלפון 03-7450892, פקס 03-7450820

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